

# Installation and Configuration Guide

Version 4.1



# Installation and Configuration Guide

Version 4.1

Note:

Before using this information and the product it supports, read the information in "Notices" on page 641.

This edition applies to version 4, release 1, modification 0 of IBM Tivoli Storage Productivity Center (product numbers 5608-WB1, 5608-WB2, 5608-WB3, 5608-WC0, 5608-WC3, and 5608-WC4) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright International Business Machines Corporation 2009. US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

## Contents

Who should read this guide
Publications
IBM Tivoli Storage Productivity Center
publications
IBM Tivoli Storage Productivity Center for
Replication publications
IBM System Storage Productivity Center
publications
IBM System Storage DS3000 publications xi
IBM System Storage DS4000 and DS5000
publications
IBM System Storage DS6000 publications XII
IBM System Storage DS Open Application
Programming Interface publications
IBM System Storage SAN Volume Controller
nublications
IBM XIV Storage System publications
IBM DB2 Database for Linux, UNIX, and
Windows publications
IBM International Technical Support
Organization publications
Translations
Accessing publications online
Ordering publications
Providing feedback about publications xv
Contacting IBM Support Center
Reporting a problem
Conventions used in this guide
New for IBM Tivoli Storage
Reductivity Contex Version 4.1
Productivity Center Version 4.1 XIX
Observed Discussions for the IDM Theself
Chapter I. Planning for the IBM Tivoli
Storage Productivity Center family 1
Planning to install the IBM Tivoli Storage
Planning to install the IBM Tivoli Storage Productivity Center family
Planning to install the IBM Tivoli Storage Productivity Center family
Planning to install the IBM Tivoli Storage Productivity Center family
Planning to install the IBM Tivoli Storage Productivity Center family
Planning to install the IBM Tivoli Storage Productivity Center family
Planning to install the IBM Tivoli Storage         Productivity Center family.       2         Hardware requirements for the IBM Tivoli Storage         Productivity Center family.       2         Software requirements       4         Running IBM Tivoli Storage Productivity Center       4         in a 64-bit environment       15         General planning       15
Planning to install the IBM Tivoli Storage         Productivity Center family.       2         Hardware requirements for the IBM Tivoli Storage         Productivity Center family.       2         Software requirements       4         Running IBM Tivoli Storage Productivity Center       15         General planning       15         IBM Tivoli Storage Productivity Center packages       15
Planning to install the IBM Tivoli Storage Productivity Center family
Planning to install the IBM Tivoli Storage Productivity Center family
Planning to install the IBM Tivoli Storage         Productivity Center family.       2         Hardware requirements for the IBM Tivoli Storage         Productivity Center family.       2         Software requirements       2         Software requirements       4         Running IBM Tivoli Storage Productivity Center       15         General planning       15         IBM Tivoli Storage Productivity Center packages       15         General configuration guidelines       17         Planning for IBM Tivoli Storage Productivity       17         Planning for IBM Tivoli Storage Productivity       18
Planning to install the IBM Tivoli Storage Productivity Center family
Planning to install the IBM Tivoli Storage Productivity Center family
Planning to install the IBM Tivoli StorageProductivity Center family.2Hardware requirements for the IBM Tivoli StorageProductivity Center family.2Software requirements2Software requirements4Running IBM Tivoli Storage Productivity Centerin a 64-bit environment15General planning15General configuration guidelines17Planning for IBM Tivoli Storage ProductivityCenter authorization18TCP/IP ports used by the IBM Tivoli StorageProductivity Center family19Planning for User IDs and user rights22
Planning to install the IBM Tivoli StorageProductivity Center family.2Hardware requirements for the IBM Tivoli StorageProductivity Center family.2Software requirements2Software requirements4Running IBM Tivoli Storage Productivity Centerin a 64-bit environment15General planning15IBM Tivoli Storage Productivity Center packages15General configuration guidelines17Planning for IBM Tivoli Storage ProductivityCenter authorization18TCP/IP ports used by the IBM Tivoli StorageProductivity Center family19Planning for User IDs and user rights22Supported subsystems, devices, file systems,
Planning to install the IBM Tivoli StorageProductivity Center family.2Hardware requirements for the IBM Tivoli StorageProductivity Center family.2Software requirements2Software requirements4Running IBM Tivoli Storage Productivity Centerin a 64-bit environment15General planning15IBM Tivoli Storage Productivity Center packages15General configuration guidelines17Planning for IBM Tivoli Storage ProductivityCenter authorization18TCP/IP ports used by the IBM Tivoli StorageProductivity Center family19Planning for User IDs and user rights22Supported subsystems, devices, file systems,26
Planning to install the IBM Tivoli Storage         Productivity Center family.       2         Hardware requirements for the IBM Tivoli Storage         Productivity Center family.       2         Software requirements for the IBM Tivoli Storage         Productivity Center family.       2         Software requirements       4         Running IBM Tivoli Storage Productivity Center       4         in a 64-bit environment       15         General planning       15         IBM Tivoli Storage Productivity Center packages       15         General configuration guidelines       17         Planning for IBM Tivoli Storage Productivity         Center authorization       18         TCP/IP ports used by the IBM Tivoli Storage         Productivity Center family       19         Planning for User IDs and user rights       22         Supported subsystems, devices, file systems, databases       26         Planning for subsystem device drivers       30

Planning for Storage Resource agents.	. 32
support	22
Diagna for Internet Ducto cal Varian (	. 33
Planning for LDAP support	. 34
Planning for LDAP support	. 41
Planning for the single sign-on feature	. 42
Planning for IBM Tivoli Storage Productivity	
Center for Replication	. 44
Planning for enterprise-rollup reports	. 46
Planning for the SAN configuration tools	. 47
Planning for the SAN planning tools	. 49
Planning for the Storage Optimizer	. 51
Planning for Data Path Explorer view	. 53
Planning for the Agent Manager	. 54
Hardware requirements	. 54
Software requirements.	. 55
Common agents	. 55
Estimating the size of the registry database.	. 55
Security considerations	. 56
TCP/IP ports used by the Agent Manager	. 59
Using version 1.2.2 Common agents	60
Planning for the Data Manager	. 00
Planning for the Data Manager	. 00
Planning for the Data agents	. 01
Planning for the Data agents on Solaris	. 01
Planning for Disk Manager configuration	. 62
Planning for the Disk Manager.	. 63
Planning for the IBM CIM agents	. 64
Planning for the TagmaStore CIM agents	. 66
Planning for Disk Manager configuration	. 67
Planning for DS8000 performance	. 69
Planning for the SAN Volume Controller	. 69
Planning for the IBM XIV Storage System	. 71
Planning for Tivoli Storage Enterprise Storage	
Server FlashCopy reports	. 73
Storage capacity of volumes	. 73
Planning for the Fabric Manager	. 73
Planning for SMI-S support	. 75
Collecting data with the Fabric Manager	. 77
CIM agent for the Fabric Manager	. 79
In-hand Fabric agent	79
Out-of-band Fabric agent	80
Planning for Eabric Manager configuration	. 00 81
Planning for Fabric Manager cwitches and	. 01
directors	07
Directors	. 82
Planning for nost bus adapters (HBAs)	. 83
Planning for private switch networks.	. 84
Configuring Brocade switches	. 84
Configuring Cisco switches	. 85
Configuring McDATA switches	. 85
Configuring QLogic switches	. 87
CNT zoning considerations	. 87
Planning for performance management	. 87
Performance metrics	. 88
Performance management configuration	. 89
Tivoli Provisioning Manager 5.1 for storage	
workflows.	. 91

Microsoft Cluster Server		. 91
Microsoft Cluster Server environment		. 92
Microsoft Cluster Server support		. 92
Planning for High-Availability Cluster		
Multi-Processing		. 94
HACMP environment		. 97
NAS and NetWare support		. 98
Novell NetWare system requirements.		. 98
Network attached storage system requirements		98
Planning for NetApp device support		. 99
Planning for IBM System Storage N Series		
Gateway servers		102
Planning for VMware		103
VMware configuration		105
VMware capacity reports		105
Planning for the Virtual I/O Server		106
Support for Virtual I/O Servers		108
Planning for the universal agent		109
IBM Tivoli Storage Productivity Center installation	ı	110
Upgrading and migrating the IBM Tivoli Storage		
Productivity Center family		111
Upgrading IBM Tivoli Storage Productivity		
Center from 3.x		113
Planning for SQL access to IBM Tivoli Storage		
Productivity Center's views.		114
Setting up a view-only user on Windows		115
Running the DB2 health monitor		116
Additional IBM Tivoli Storage Productivity Center		
publications		117
Subscribing to IBM Tivoli Storage Productivity		
Center technical support Web site		118
1 1		

#### Chapter 2. Installing the IBM Tivoli Storage Productivity Center family

Storage Productivity Center family 119
Installing IBM Tivoli Storage Productivity Center
overview
Installing DB2
Preparing to install DB2
Installing DB2 on Windows
Installing DB2 on UNIX or Linux - GUI install 124
Installing DB2 on AIX - Command line 126
Verifying that DB2 is installed correctly 129
Configuring DB2, AIX, and Linux for IPv6-only
environment
Installing the Agent Manager
Installing the Agent Manager using a 32-bit DB2
instance - GUI install
Installing the Agent Manager using a 32-bit DB2
instance - Console install
Installing the Agent Manager using a 64-bit DB2
instance - GUI install
Installing the Agent Manager using a 64-bit DB2
instance - Console install
Installing the IBM Tivoli Storage Productivity
Center family
Preparing for installation
Preparing to install Storage Resource agents
remotely on Windows 2008 and Windows Vista . 167
Starting the installation program
Using typical installation

Installing the Two Site or	Th	ree	Site	e B	usi	nes	s	
Continuity license								. 197
Using custom installation								. 198
Installing the agents								. 241
Installing IBM Tivoli Stora	ge	Pro	odu	icti	vity	7		
Center in silent mode.	٠.							. 262
Installing the Language Pack								. 263

## Chapter 3. Configuring IBM Tivoli

Storage Productivity Center	267
Configuration overview	. 267
Configuration Utility	. 272
Configuration utility tasks	. 272
Configuration nodes	. 277
Role-to-Group Mappings	. 279
License keys.	. 281
Alert disposition	. 287
Log-File Retention.	. 288
Quota and Constraint e-mail Address Rules .	. 289
Scan/Probe Agent Administration	. 289
Manual NAS/NetWare Server Entry	. 290
Agent Manager Registration	. 294
History Aggregator	. 295
Storage Resource agent deployments	. 295
Data/Storage Resource Agent Upgrades	. 311
NetWare Tree Logins	. 311
Resource History Retention.	. 311
Removed Resource Retention	. 312
Resource History Retention for Databases	. 313
Removed Resource Retention for Databases .	. 313
Configuration History Settings	. 314
Configuration: Device server specific	. 314
Configuring switches.	. 314
Configuring the inactive zonesets for a fabric	
data source	. 316
Excluding devices from Fabric agent scans .	. 316
Configuration guidelines for agent placement	317
Managing a SAN without agents	. 317
Setting timeout values for the Device server .	. 318
Service Location Protocol (SLP) configuration	
recommendations	. 319
Configuring the Data server for a Windows	
domain	. 320
Granting local administrative privileges to a	
domain account	. 321
Configuring IP addressing	. 322
Configuring IBM Tivoli Storage Productivity	
Center with multiple IP addresses	. 322
Changing the HOSTS file	. 323
Configuring Java Web Start to start the IBM Tivoli	
Storage Productivity Center GUI	. 323
Configuring tracing	. 328
Configuring the DB2 JDBC driver	. 329
Configuration guidelines for 500 or more agents	329
Using a master image to set up Common agent	
machines	. 330
Configuring IBM Tivoli Storage Productivity	
Center for batch reports on UNIX or Linux	. 331
Configuring LUN provisioning for Sun Solaris .	. 332

Assigning Tivoli Storage Enterprise Storage

Server, DS6000, or DS8000 LUNs to Sun Solaris	
HBAs	332
Modifying the HBA configuration file	333
Setting Persistent Name Binding for QLA2200	
and QLA2300 HBAs using scfx	333
Modifying the SCSI disk configuration file .	334
Checking for Tivoli Storage Enterprise Storage	
Server, DS6000, or DS8000 multipaths in	
VxDMP	335
How to import a Storage Resource agent's	
authentication information	336
Configuring Tivoli Storage Productivity Center for	
DS8000 LDAP support	336
Configuring multiple Tivoli Storage Productivity	
Center servers with a single DS8000 R4.2	340
Disabling Tivoli Storage Productivity Center or	
Tivoli Storage Productivity Center for Replication	341

## Chapter 4. Upgrading and migrating the IBM Tivoli Storage Productivity

Center family	345
Migrating TotalStorage Productivity Center 3.x to	
Tivoli Storage Productivity Center 4.1	347
Migrating IBM Tivoli Storage Productivity Center	
for Replication from V3. <i>x</i> to V4.1.	348
Upgrading to DB2 9.5	349
Migrating the database repository	349
Migrating the database repository for Windows	350
Migrating the database repository for AIX.	355
Migrating the database repository for Linux .	357
Upgrading Agent Manager.	360
Preparing for an upgrade	361
Upgrading IBM Tivoli Storage Productivity Center	
(excluding agents).	363
Upgrading the remote database	368
Upgrading the IBM Tivoli Storage Productivity	
Center agents	369
Upgrading Storage Resource agents manually	369
Upgrading the Data agents.	370
Upgrading the Fabric agents	372
Upgrading the Fabric agents remotely	373
Migrating a Storage Resource agent to a Data agent	374
Upgrading the CIM agent for storage subsystems	375
Upgrading the SAN Volume Controller CIM agents	376
Upgrading the SAN Volume Controller CIM	
agents directly	376
Adding a SAN Volume Controller CIM agent on	
a different master console	376
Configuring IBM System Storage N Series Gateway	
servers	377

## Chapter 5. Uninstalling the IBM Tivoli Storage Productivity Center family

Storage Productivity Center family 383
Uninstalling the IBM Tivoli Storage Productivity
Center family using the uninstallation program 383
Uninstalling IBM Tivoli Storage Productivity
Center for Replication with InstallShield
Uninstalling IBM Tivoli Storage Productivity
Center for Replication manually

Uninstalling IBM Tivoli Storage Productivity	
Center for Replication manually on Windows . 38	8
Uninstalling IBM Tivoli Storage Productivity	
Center for Replication manually on AIX and	
Linux	8
Uninstalling the agents	9
Deleting or uninstalling an agent using the GUI 38	9
Uninstalling the Storage Resource agent	
manually	0
Uninstalling the Data agents or Fabric agents	
locally	0
Uninstalling the Data agents or Fabric agents	
remotely	1
Uninstalling agents on a Virtual I/O Server 39	3
Uninstalling the Language Pack	3
Uninstalling the Agent Manager	4
Uninstalling DB2	5
Uninstalling DB2 on UNIX or Linux	5

## Chapter 6. Administering IBM Tivoli

Storage Productivity Center		399
Administering DB2		399
Backing up the IBM Tivoli Storage Productivity		
Center database		399
Starting the Control Center		400
Using the command line on UNIX and Linux		400
Manually starting DB2 running on Windows		400
Manually stopping DB2 running on Windows		401
Monitoring DB2		401
Administering Tivoli Integrated Portal		402
Changing the user authentication method		402
Changing the LTPA token expiration for		
single-sign on		410
Managing Agent Manager		411
Getting started		411
Starting the Agent Manager		414
Stopping the Agent Manager		415
Configuring Agent Manager to use different		
ports		415
How to change port 80		416
Packaging the Agent Manager log files		419
Determining the version of Agent Manager .		420
Backup and recovery		420
Changing agent registration properties		423
Managing resource manager authorization .		424
Configuring how long agent configuration		
information is saved		427
Changing the maximum heap size for Agent		
Manager		428
Multiple Agent Managers in your enterprise .	•	429
Reusing an existing Agent Manager		429
Administering data sources		430
Checking the health of your agents		430
Manually changing the Windows service logon		
for the agent		430
CIM agents		430
Data agents and Storage Resource agents		437
In-band Fabric agents		450
Out-of-band Fabric agents		451
IBM Tivoli Storage Productivity Center Servers		453
VMware data source	•	458

Administering agents on the Virtual I/O Server	461
Adding a IBM Tivoli Storage Productivity Center	
user group name to IBM Tivoli Storage	
Productivity Center for Replication	462
Accessing the IBM Tivoli Storage Productivity	
Center for Replication GUI.	463
Backing up and recovering IBM Tivoli Storage	
Productivity Center for Replication	463
Starting and stopping the IBM Tivoli Storage	100
Productivity Center services	464
Stopping the IBM Tiveli Stopping Productivity	101
Conter consists	161
	404
Starting the IBM Tivoli Storage Productivity	
Center services	465
Starting and stopping the IBM Tivoli Integrated	
Portal server	466
Starting and stopping the Tivoli Storage	
Productivity Center GUI.	467
Starting the Tivoli Storage Productivity Center	
GUI	467
Stopping the Tivoli Storage Productivity Center	107
CIII	470
Charling IDM Timeli Charles Dreductionity Conten	470
Checking Ibivi Tivoli Storage Productivity Center	470
status	470
Checking the IBM Tivoli Storage Productivity	
Center version	471
Checking the status of the Data Server	471
Checking the status of the Device server	471
Checking the status of agents	471
Increasing memory allocation	472
Increasing the memory allocation for the Data	
server	472
server	472
server	472
server	472 474
server	472 474 474
server	472 474 474
server	472 474 474 474
server	472 474 474 474 475
server	472 474 474 474 475 475
server	472 474 474 474 475 475
server	<ul> <li>472</li> <li>474</li> <li>474</li> <li>475</li> <li>475</li> <li>475</li> </ul>
server	472 474 474 474 475 475 475
server	<ul> <li>472</li> <li>474</li> <li>474</li> <li>474</li> <li>475</li> <li>475</li> <li>475</li> <li>475</li> <li>476</li> </ul>
server	<ul> <li>472</li> <li>474</li> <li>474</li> <li>475</li> <li>475</li> <li>475</li> <li>475</li> <li>476</li> <li>476</li> <li>476</li> </ul>
server	472 474 474 475 475 475 475 476 476
server	472 474 474 475 475 475 475 476 476 477
server	472 474 474 475 475 475 475 476 476 476 476
server	472 474 474 475 475 475 475 476 476 476 477
<ul> <li>server</li></ul>	472 474 474 475 475 475 475 476 476 476 477 479
server	472 474 474 475 475 475 475 476 476 477 479
server	472 474 474 475 475 475 475 476 477 479 481
server	472 474 474 475 475 475 475 476 477 479 481
server	472 474 474 475 475 475 475 476 477 479 481 481
<ul> <li>server</li></ul>	472 474 474 475 475 475 475 476 477 479 481 481 481
server	472 474 474 475 475 475 475 476 477 479 481 481 481
<ul> <li>server</li></ul>	472 474 474 475 475 475 475 476 477 479 481 481 481 481
server	472 474 474 475 475 475 475 476 477 479 481 481 481 481 483 484
server	472 474 474 475 475 475 475 476 477 479 481 481 481 481 481 483
server	472 474 474 475 475 475 475 476 477 479 481 481 481 481 481 483
server	472 474 474 475 475 475 475 476 477 479 481 481 481 481 481 483 484 485 487
<ul> <li>server</li></ul>	472 474 474 475 475 475 475 476 477 479 481 481 481 481 481 483 484 485 487
<ul> <li>server</li></ul>	472 474 474 475 475 475 475 476 476 477 479 481 481 481 481 481 481 483 484

Checking for a fully qualified host name for	
AIX systems	. 487
Checking for a fully qualified host name for	
	. 488
Checking for a fully qualified host name for	
Solaris systems	. 488
Granting local administrative privileges to a	
domain account	. 489
Importing SSL certificates for VMware	. 489
Repository Copy tool	. 490
Exporting repository data	. 491
Importing repository data	. 492
Service tool: collecting information	. 493
Running the Service tool for the servers	. 494
Running the Service tool for the agents	. 494
Chapter 7. Troubleshooting	497
Configuration files	. 497
server.config file	. 498
scheduler.config file	. 499
TPCD.config file	. 500
agent.config file	. 500
Log files	. 501
Default log file locations	. 501
Agent Manager log files	. 503
Troubleshooting descriptions and solutions	. 505
General troubleshooting	. 505
IBM Tivoli Storage Productivity Center for	
Replication	. 528
DB2 and database troubleshooting	. 529
Agent Manager	. 535
Installation and uninstallation troubleshooting	540
Upgrading troubleshooting	. 565
Memory, space and performance	
troubleshooting.	. 569
DS4000 and FAStT troubleshooting	. 575
DS6000, DS8000, and Tivoli Storage Enterprise	
Storage Server troubleshooting	. 578
SAN Volume Controller troubleshooting	. 582
Storage Optimizer.	. 585
N Series Gateway servers troubleshooting.	. 586
XIV Storage System troubleshooting	. 587
Tape troubleshooting	. 588
Tivoli Integrated Portal troubleshooting	. 589
Independent software vendors troubleshooting	595
Miscellaneous troubleshooting.	. 601
	~~~
Chapter 8. Reference information	605
Agent Manager toolkit for administrators	. 605
Estimating tablespace allocation	. 606
DB2 user names and passwords	. 607
Valid characters for user IDs and passwords	. 607
Interop namespaces for CIM agents for switches	(00
and storage subsystems	. 608
agent.config file	. 609
server.config file	. 610
scheduler.config file	. 611
IPCD.config file	. 612
Information gathered by the agents	. 612
Zone configuration	. 615

SQL access to IDM IIVOII Storage Flocuctivity	
Center's views	. 616
Accessing views in the database repository	. 619
Options files for installing or uninstalling IBM	
Tivoli Storage Productivity Center in silent mode	. 620
setup_agents.iss options file	. 620
uninstall.iss file.	625
	. 010
Appendix A. General information for Storage Resource agents and Data agents	627

Appendix C. TCP/IP ports used by the IBM Tivoli Storage Productivity Center														
family	•	•	•	•	•	•	•	•	•	•	•	•	•	633
Appendix	D.	W	or	'k	sh	ee	t f	or	นร	ser	10	)s		
and pass	wo	rds	S	•	·	•	•	·	•	•	·	•	•	637
Notices .														641
Trademarks	•	•	•	•	•	•	•			•		•	•	. 643
Glossary	•	•	•	•	•	•	•	•	•	•	•	•	•	645
Index														651

## Preface

IBM<sup>®</sup> Tivoli<sup>®</sup> Storage Productivity Center is a storage infrastructure management software product that can centralize, automate, and simplify the management of complex and heterogeneous storage environments.

## Who should read this guide

This publication is intended for administrators or users who are installing and using IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication. It also describes the hardware and software requirements for installing the products and provides an overview of the installation procedures.

Administrators and installers should be familiar with the following topics:

- General procedures for installing software on Microsoft<sup>®</sup> Windows<sup>®</sup>, AIX, Linux<sup>®</sup>, HP-UX, and Solaris.
- SAN concepts
- IBM Tivoli Storage Productivity Center concepts
- IBM Tivoli Storage Productivity Center for Replication concepts
- DB2 Database for Linux, UNIX<sup>®</sup>, and Windows
- Simple Network Management Protocol (SNMP) concepts
- IBM Tivoli Enterprise Console

This installation and configuration guide includes information for the IBM Tivoli Storage Productivity Center family of products which includes the following programs:

- IBM Tivoli Storage Productivity Center
- IBM Tivoli Storage Productivity Center for Replication

## **Publications**

This section lists publications in the IBM Tivoli Storage Productivity Center library and other related publications. It also describes how to access publications online, how to order publications, and how to submit comments on publications.

The publications are available from the IBM publications center at http://www.ibm.com/shop/publications/order

### IBM Tivoli Storage Productivity Center publications

Use these publications for information about how to install, configure, and use IBM Tivoli Storage Productivity Center.

The Tivoli Storage Productivity Center publications are available from the IBM Tivoli Storage Productivity Center Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v4r1/index.jsp. Click **Tivoli Storage Productivity Center**.

For PDF documents, click **IBM Tivoli Storage Productivity Center > Printable documentation**.

Publication Title	Order Number
IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication Installation and Configuration Guide	SC27-2337
IBM Tivoli Storage Productivity Center User's Guide	SC27-2338
IBM Tivoli Storage Productivity Center Messages	SC27-2340
IBM Tivoli Storage Productivity Center Command-Line Interface Reference	SC27-2339
IBM Tivoli Storage Productivity Center Problem Determination Guide	GC27-2342
IBM Tivoli Storage Productivity Center Workflow User's Guide	SC27-2341

# IBM Tivoli Storage Productivity Center for Replication publications

Use these publications for information about how to install, configure, and use IBM Tivoli Storage Productivity Center for Replication.

The following table lists the IBM Tivoli Storage Productivity Center for Replication publications. These publications are available in the Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v4r1/index.jsp.

## Click Tivoli Storage Productivity Center for Replication > Reference > Publications.

Information for installing, upgrading, and uninstalling IBM Tivoli Storage Productivity Center for Replication is documented in the *IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication Installation and Configuration Guide.* 

Publication Title	Order Number
IBM Tivoli Storage Productivity Center for Replication for System z v4.1 Installation and Configuration Guide	SC27-2321-00
IBM Tivoli Storage Productivity Center for Replication V4.1 Command-Line Interface User's Guide	SC27-2323-00
IBM Tivoli Storage Productivity Center for Replication V4.1 Problem Determination Guide	GC27-2320-00
IBM Tivoli Storage Productivity Center for Replication V4.1 User's Guide	SC27-2322-00

## **IBM System Storage Productivity Center publications**

Use these publications for information about how to install, configure, and use IBM System Storage<sup>™</sup> Productivity Center.

These publications are available in the Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v4r1/index.jsp.

Click System Storage Productivity Center.

For PDF documents, click **System Storage Productivity Center > Printable documentation**.

Publication Title	Order Number
IBM System Storage Productivity Center Introduction and Planning Guide	SC23-8824
IBM System Storage Productivity Center Documentation CD	SCD7-1477
Read This First: Installing the IBM System Storage Productivity Center	GI11-8938
IBM System Storage Productivity Center User's Guide	SC27-2336

## **IBM System Storage DS3000 publications**

Use these publications for information about how to install, configure, and use the IBM DS3000.

To see the IBM DS3000 publications, follow these steps:

- 1. Go to http://www.ibm.com/servers/storage/support/.
- 2. Under Select your product, in the Product Family field, select Disk systems.
- 3. In the Product field, select DS3200, DS3300, or DS3400, as applicable.
- 4. Click Go.
- 5. In the Support and Download pane, click **Documentation**.
- 6. Under Documentation, click on a document title.

Publication Title	Part or Order Number
IBM System Storage DS3000 Storage Manager Version 10 Installation and Support Guide for Windows, Linux, NetWare, and VMware	46M1364
IBM System Storage DS3200 Storage Subsystem Installation, Maintenance, and User's Guide	46M1361
IBM System Storage DS3300 Storage Subsystem Installation, Maintenance, and User's Guide	46M1362
IBM System Storage DS3400 Storage Subsystem Installation, Maintenance, and User's Guide	46M1363
IBM System Storage DS3000 Storage Manager Version 10 Installation and Support Guide for AIX, Linux on POWER, and Sun Solaris	46M1365

## IBM System Storage DS4000 and DS5000 publications

Use these publications for information about how to install, configure, and use the IBM  $\text{DS4000}^{\$}$  and IBM DS5000.

To see the IBM DS4000 or IBM DS5000 publications, follow these steps:

- 1. Go to http://www.ibm.com/systems/support/storage/disk.
- 2. Under Select your product, in the Product Family field, click Disk systems.
- **3**. In the Product field, click the appropriate storage system.
- 4. Click Go.
- 5. Click Documentation.
- 6. Click a document.

Publication Title	Order Number		
IBM System StorageDS4000 Concepts Guide	GC26-7734		

Publication Title	Order Number
IBM System Storage DS4000/DS5000 Fibre Channel and Serial ATA Intermix Premium Feature Installation Overview	GC53-1137
IBM System Storage DS <sup>®</sup> Storage Manager Version 10 IBM System Storage DS Storage Manager Installation and Host Support Guide	GC53-1135
IBM System Storage DS Storage Manager Version 10.50 Copy Services User's Guide	GC53-1136
IBM System Storage DS4800 Storage Subsystem Quick Start Guide	GC27-2148
DS5100, DS5300 and EXP5000 Quick Start Guide	GC53-1134
IBM System Storage DS4800 Storage Subsystem Installation, User's, and Maintenance Guide	GC26-7845
IBM System Storage DS5100 and DS5300 Storage Subsystems Installation, User's, and Maintenance Guide	GC53-1140
IBM System Storage DS4000/DS5000 Hard Drive and Storage Expansion Enclosure Installation and Migration Guide	GC53-1139
IBM System Storage DS5000 EXP5000 Storage Expansion Enclosure Installation, User's, and Maintenance Guide	GC53-1141
IBM System Storage DS3000, DS4000, and DS5000 Command Line Interface and Script Commands Programming Guide	GC52-1275
IBM System Storage DS4000/DS5000EXP810 Storage Expansion Enclosure Installation, User's and Maintenance Guide	GC26-7798

## **IBM System Storage DS6000 publications**

Use these publications for information about how to install, configure, and use the  $DS6000^{TM}$ .

These publications are available from the DS6000 Information Center on the following Web site:

http://publib.boulder.ibm.com/infocenter/dsichelp/ds6000ic/index.jsp

Publication Title	Order Number
<i>IBM System Storage DS6000: Host Systems Attachment Guide</i> <b>Note:</b> No hardcopy is produced for this publication.	GC26-7680
IBM System Storage DS6000: Introduction and Planning Guide	GC26-7679
IBM System Storage Multipath Subsystem Device Driver User's Guide	SC30-4096
IBM System Storage DS6000 : Messages Reference	GC26-7682
IBM System Storage DS6000 Installation, Troubleshooting, and Recovery Guide	GC26-7678
IBM System Storage DS6000 Quick Start Card	GC26-7659

## **IBM System Storage DS8000 publications**

Use these publications for information about how to install, configure, and use the  $\text{DS8000}^{\$}$  system.

These publications are available from the DS8000 Information Center at http://publib.boulder.ibm.com/infocenter/dsichelp/ds8000ic/index.jsp.

Publication Title	Order Number
<i>IBM System Storage DS8000: Host Systems Attachment Guide</i> <b>Note:</b> No hardcopy is produced for this publication.	SC26-7917
IBM System Storage DS8000: Introduction and Planning Guide	GC35-0515
IBM System Storage DS8000: Command-Line Interface User's Guide	GC53-1127
IBM System Storage DS8000: Messages Reference	GC26-7914

# IBM System Storage DS Open Application Programming Interface publications

Use these publications for information about how to install, configure, and use the DS CIM agent.

These publications are available at http://www.ibm.com/servers/storage/ support/software/cimdsoapi/.

Click the **Install** tab **> Documentation**. Make sure you reference the correct document for the CIM agent version.

Publication Title	Order Number
<i>IBM System Storage DS Open Application Programming Interface 5.4.1</i> <i>and 5.4.2 Installation and Reference</i>	GC35-0516-04
<i>IBM System Storage DS Open Application Programming Interface 5.3</i> <i>Installation and Reference</i>	GC35-0516-03
<i>IBM System Storage DS Open Application Programming Interface Reference</i> for CIM agent 5.2	GC35-0516-01
IBM Tivoli Storage Productivity Center DS Open Application Programming Interface Reference for CIM agent 5.1	GC35-0493

## **IBM System Storage SAN Volume Controller publications**

Use these publications for information about how to install, configure, and use IBM System Storage SAN Volume Controller.

The following table lists the IBM System Storage SAN Volume Controller publications. These publications are available in the IBM System Storage SAN Volume Controller Information Center at http://publib.boulder.ibm.com/infocenter/svcic/v3r1m0/index.jsp.

Publication Title	Order Number
IBM System Storage SAN Volume Controller CIM Agent Developer's Reference	SC26-7904
IBM System Storage SAN Volume Controller Command-Line Interface User's Guide	SC26-7903
IBM System Storage SAN Volume Controller Software Installation and Configuration Guide	SC23-6628
IBM System Storage SAN Volume Controller Host Attachment Guide	SC26-7905
IBM System Storage SAN Volume Controller Hardware Installation Guide	GC27-2132
IBM System Storage SAN Volume Controller Planning Guide	GA32-0551
IBM System Storage SAN Volume Controller Service Guide	GC26-7901

## **IBM XIV Storage System publications**

For information about how to install, configure, and use the IBM XIV<sup>®</sup> Storage System, use the following link:

http://publib.boulder.ibm.com/infocenter/ibmxiv/r2/index.jsp

## IBM DB2 Database for Linux, UNIX, and Windows publications

Use these publications for information about how to install, configure, and use  $DB2^{\circledast}$ .

The following table lists some of the IBM DB2 Database for Linux, UNIX, and Windows product publications for Version 9.5.

For a complete list of DB2 publications, go to http://publib.boulder.ibm.com/ infocenter/db2luw/v9r5/index.jsp.

Publication Title	Order Number
IBM DB2 Version 9.5 for Linux, UNIX, and Windows, Getting started with DB2 installation and administration on Linux and Windows	GC23–5857
IBM DB2 Version 9.5 for Linux, UNIX, and Windows, Command Reference	SC23–5846
IBM DB2 Version 9.5 for Linux, UNIX, and Windows, Message Reference Volume 1	GI11–7855
IBM DB2 Version 9.5 for Linux, UNIX, and Windows, Message Reference Volume 2	GI11–7856
IBM DB2 Version 9.5 for Linux, UNIX, and Windows, Migration Guide	GC23–5859
IBM DB2 Version 9.5 for Linux, UNIX, and Windows, Troubleshooting Guide	GI11–7857

## **IBM International Technical Support Organization publications**

The IBM International Technical Support Organization (ITSO) publishes IBM Redbooks<sup>®</sup>, which are books on specialized topics.

You can order publications through your IBM representative or the IBM branch office serving your locality. You can also search for and order books of interest to you by visiting the IBM Redbooks home page at http://www.redbooks.ibm.com/ redbooks.

For information about IBM System Storage Productivity Center, see *IBM System Storage Productivity Center Deployment Guide*. Search for **SG24-7560**.

For information about IBM Tivoli Storage Productivity Center, see *TotalStorage*<sup>®</sup> *Productivity Center V3.3 Update Guide*. Search for **SG24-7490**.

### Translations

Translated publications are available within the IBM Tivoli Storage Productivity Center Information Center. The IBM Tivoli Storage Productivity Center Information Center is available in certain translated languages, and is displayed in the language that is appropriate for the Web browser locale setting. When a locale does not have a translated version, the information center is displayed in English, which is the default language. Translations of the PDFs are available when the information center is translated.

See the "Printable documentation" section of the information center for links to PDFs.

Contact your IBM Support Center for more information about the translated publications and whether these translations are available in your country.

## Accessing publications online

This topic provides information on how to access the IBM Tivoli Storage Productivity Center Information Center.

You can access publications in the IBM Tivoli Storage Productivity Center Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v4r1/ index.jsp.

The IBM Tivoli Storage Productivity Center Information Center contains the most recent version of the books in the product library in PDF or HTML formats, or both. Translated documents are also available for some products.

**Note:** If you print PDF documents on other than letter-sized paper, select the **Fit to page** check box in the **Adobe Acrobat Print** dialog. This option is available when you click **File**  $\rightarrow$  **Print**. **Fit to page** ensures that the full dimensions of a letter-sized page print on the paper that you are using.

## Ordering publications

Information is provided for the ordering of IBM publications on the Internet or by telephone.

You can order many IBM publications online at http://www.ibm.com/shop/ publications/order.

You can also order by telephone. In the United States and Canada, call 800-879-2755. In other countries, please contact your IBM service representative.

#### Providing feedback about publications

This topic provides information on where to send feedback about the publications.

If you have comments or suggestions about the product and documentation, complete the customer feedback survey at http://www.ibm.com/systems/ support/storage/software/tpc.

On the left side of the Web page, click Feedback.

### Contacting IBM Support Center

This topic provides information on how to contact IBM Support Center for information.

For support for IBM Tivoli Storage Productivity Center, you can contact IBM Support Center in one of the following ways:

• Go to the IBM Tivoli Storage Productivity Center technical support Web site at http://www.ibm.com/systems/support/storage/software/tpc/.

To receive future support notifications, go to the right and under **Stay informed**, click **Subscribe**. You will be required to enter your IBM ID and password. Once authenticated, you will be able to configure your subscription for Tivoli Storage Productivity Center technical support Web site updates.

- Customers in the United States can call 1-800-IBM-SERV (1-800-426-7378).
- International customers should go to the Tivoli Storage Productivity Center technical support Web site for customer support telephone numbers.

You can also review the *IBM Software Support Handbook*, which is available on our Web site at http://techsupport.services.ibm.com/guides/handbook.html.

The support Web site offers extensive information, including a guide to support services; frequently asked questions (FAQs); and documentation for all IBM Software products, including Redbooks and white papers. Translated documents are also available for some products.

When you contact the IBM Support Center, be prepared to provide identification information for your company so that support personnel can readily assist you. Company identification information might also be needed to access various online services available on the Web site. See "Reporting a problem."

## **Reporting a problem**

This topic provides a list of what information you should have ready when you encounter a problem.

Have the following information ready when you report a problem:

- The IBM Tivoli Storage Productivity Center version, release, modification, and service level number.
- The communication protocol (for example, TCP/IP), version, and release number that you are using.
- The activity that you were doing when the problem occurred, listing the steps that you followed before the problem occurred.
- The exact text of any error messages.

## Conventions used in this guide

This section provides information on the conventions used in this publication.

This publication uses several conventions for special terms and actions, and operating system-dependent commands and paths.

The following typeface conventions are used in this publication:

Bold

- · Lowercase and mixed-case commands that appear with text
- Command options that appear with text
- Flags that appear with text
- Graphical user interface (GUI) elements (except for titles of windows and dialogs)
- Names of keys

#### Italic

- Variables
- Values you must provide
- New terms
- Words and phrases that are emphasized
- Titles of documents

#### monospace

- Commands and command options in examples
- Flags that appear on a separate line
- Code examples and output
- Message text
- Names of files and directories
- Text strings you must type, when they appear within text
- Names of Java methods and classes
- HTML and XML tags also appear like this, in monospace type

For syntax notation, these conventions are used:

- <> (less than, greater than symbols) are used to indicate a variable value. Do not type the <> symbols.
- *#* is the prompt for the root user on UNIX platforms.
- Uppercase and lowercase characters do matter. Type in commands exactly as shown.

## New for IBM Tivoli Storage Productivity Center Version 4.1

Use this information to learn about new features and enhancements in IBM Tivoli Storage Productivity Center version 4.1. This section highlights the changes since IBM TotalStorage Productivity Center 3.3.2.

For more information about each of the features, go to the Tivoli Storage Productivity Center Information Center and search for **Planning for the IBM Tivoli Storage Productivity Center family**. For information about how to use the features, see the *IBM Tivoli Storage Productivity Center User's Guide*.

Tivoli Storage Productivity Center 4.1 adds the following new features, functions, and enhancements:

#### Name change

IBM Tivoli Storage Productivity Center V4.1 has been renamed from IBM TotalStorage Productivity Center. All user interfaces, documentation, online help, and messages have also been changed to reflect the name change.

#### Licensing changes

These are the licenses available for IBM Tivoli Storage Productivity Center:

- IBM Tivoli Storage Productivity Center Basic Edition
- IBM Tivoli Storage Productivity Center Standard Edition
- IBM Tivoli Storage Productivity Center for Disk
- IBM Tivoli Storage Productivity Center for Data

If you have an IBM TotalStorage Productivity Center for Fabric license only, you can upgrade to IBM Tivoli Storage Productivity Center Standard Edition.

If you have an IBM TotalStorage Productivity Center for Basic Edition license only, you can upgrade to IBM Tivoli Storage Productivity Center Basic Edition, IBM Tivoli Storage Productivity Center for Disk, IBM Tivoli Storage Productivity Center for Data, or IBM Tivoli Storage Productivity Center Standard Edition.

If you have an IBM TotalStorage Productivity Center for Data license only, you can upgrade to IBM Tivoli Storage Productivity Center for Data or IBM Tivoli Storage Productivity Center Standard Edition.

If you have an IBM TotalStorage Productivity Center for Disk license only, you can upgrade to IBM Tivoli Storage Productivity Center for Disk, IBM Tivoli Storage Productivity Center for Data (Disk plus Data), or IBM Tivoli Storage Productivity Center Standard Edition.

If you have an IBM TotalStorage Productivity Center Standard Edition license, you can upgrade to IBM Tivoli Storage Productivity Center Standard Edition.

#### Integration features

Tivoli Storage Productivity Center provides these integration features.

#### Integration of Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication

Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication, previously separated products, are now integrated. You can start the IBM Tivoli Storage Productivity Center for Replication user interface from within the Tivoli Storage Productivity Center user interface.

The IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication Installation and Configuration Guide also includes the installation, upgrade, and uninstallation information for IBM Tivoli Storage Productivity Center for Replication.

This integration enables you to:

- Start the IBM Tivoli Storage Productivity Center for Replication user interface from within the Tivoli Storage Productivity Center user interface.
- Use the Tivoli Storage Productivity Center GUI to set up IBM Tivoli Storage Productivity Center for Replication SNMP alerts and IBM Tivoli Enterprise Console<sup>®</sup> events.
- Provide a Tivoli Storage Productivity Center superuser role that has authority over all Tivoli Storage Productivity Center commands. IBM Tivoli Storage Productivity Center for Replication includes a replication administrator role that has authority to all IBM Tivoli Storage Productivity Center for Replication commands. IBM Tivoli Storage Productivity Center for Replication will honor the Tivoli Storage Productivity Center superuser role giving the superuser role authority over all Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication commands.

## Integration of Tivoli Storage Productivity Center and IBM Tivoli Integrated Portal

Tivoli Integrated Portal is a standards-based architecture for Web administration. Tivoli Integrated Portal enables developers to build administrative interfaces for IBM and independent software products as individual plug-ins to a common console network. The installation of Tivoli Integrated Portal is required to enable single sign-on for Tivoli Storage Productivity Center.

Single sign-on is an authentication process that enables you to enter one user ID and password to access multiple applications. Single sign-on integrates with the launch in context feature to enable you to move smoothly from one application to a specific location in a second application.

#### Launch in context feature

The launch in context feature enables you to access external applications from the Tivoli Storage Productivity Center GUI. Element managers are the most prevalent external applications that use the launch in context feature. An element manager is usually the vendor-specific software that is used to administer a particular storage device. The launch in context feature provides starting points in the Tivoli Storage Productivity Center GUI so you can click a button or select a menu item to start an element manager.

When you install Tivoli Storage Productivity Center, Tivoli Integrated Portal, and Tivoli Storage Productivity Center for Replication, the components are automatically configured to use launch in context. You can access Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication from the Tivoli Integrated Portal GUI and you can access Tivoli Storage Productivity Center for Replication from the Tivoli Storage Productivity Center GUI.

There are three levels of launch in context ability:

#### Simple launch

This level exists in TotalStorage Productivity Center 3.3.2. Tivoli Storage Productivity Center discovers basic information about the device and the management of the device.

#### Launch with parameters

You can specify additional parameters in the URL or command-line interface when starting an application. The parameters that are passed enable you to navigate to a particular panel or state of the application that was started. You can also identify objects to operate on and possibly provide values to use in the operation.

#### Launch with single sign-on

You can enhance the launch in context feature to include single sign-on. Single sign-on can be used when an external application can perform authentication against the same user repository as Tivoli Storage Productivity Center. A directory that is Lightweight Directory Access Protocol (LDAP) compliant is a common example of such a user repository.

External applications that do not include the WebSphere Application Server (WAS), require the authentication service that is provided by Tivoli Integrated Portal. For example, the element manager for IBM System Storage DS8000, DS8000 Storage Manager, uses the authentication service to handle launch in context with single sign-on from the Tivoli Storage Productivity Center GUI.

#### Single sign-on

Single sign-on is an authentication process that enables you to enter one user ID and password to access multiple applications. Single sign-on enables you to access:

- Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication from the Tivoli Integrated Portal GUI.
- Tivoli Storage Productivity Center for Replication from the Tivoli Storage Productivity Center GUI.
- External applications such as element managers from the Tivoli Storage Productivity Center GUI.

The single sign-on feature requires a centralized user and group repository, such as an LDAP-compliant directory, that all participating applications can access.

Tivoli Storage Productivity Center uses Lightweight Third Party Authentication (LTPA) tokens to pass the user information between applications. To use LTPA tokens for single sign-on, each participating application must possess the same set of keys to encode and decode the user information contained in the token. As an additional security feature, the LTPA tokens expire after a determined amount of time. When the tokens expire, you must re-enter your user ID and password information.

If you select operating system authentication, then the use of the single sign-on feature is limited. Operating system authentication does not support single sign-on for element managers, even when the element manager is installed on the same machine as Tivoli Storage Productivity Center.

#### **Storage Resource agents**

Tivoli Storage Productivity Center now supports Storage Resource agents on Microsoft Windows, AIX<sup>®</sup>, and Linux. The Storage Resource agent probe is equivalent to the information that is collected by probes using the Data agent.

The Storage Resource agents do not require the Agent Manager and can be deployed to other systems using the Tivoli Storage Productivity Center GUI on the server system.

You can use the following functions:

- Asset reports (including HBA)
- Capacity reports
- Subsystem to host storage correlation including multipathing information
- Topology and Data Path explorer functions

This support does not include file system scans, NAS discovery or topology, zoning and zone control functions or subsystem device driver configuration. You can still use the Data agent and Fabric agent for this information.

#### SQL access to Tivoli Storage Productivity Center database

Tivoli Storage Productivity Center will provide a set of DB2 views that represent key information that has been collected by monitoring jobs and stored in the database repository. A *view* is a way of describing data that exists in one or more tables within the database repository. It does not contain data but, instead, is a stored set of SQL commands that define a subset of rows and columns in the base tables.

You can use the Structured Query Language (SQL) to retrieve the information from the views and create reports using your own tools, such as Business Intelligence and Reporting Tools (BIRT) or Microsoft Excel. Other applications can also use these views to gather and import information that is collected by Tivoli Storage Productivity Center.

The following categories of views will contain information collected by Tivoli Storage Productivity Center:

#### Storage entity views

These views include information about the properties of the entity. For example, the name, capacity, freespace, and so forth for a storage subsystem.

#### Entities defined by Tivoli Storage Productivity Center

These entities include Data agents, Fabric agents, alert log, Tivoli Storage Productivity Center server, computer groups, storage subsystem groups, file system groups, storage resource groups, and so forth.

#### Aggregated views

These views provide summary information for the database history, data in a database instance, and the Data agent file system.

#### **Reporting views**

These views combine several different entities in one view for a report.

#### **Rollup** views

These views include rollup report information from the master and subordinate Tivoli Storage Productivity Center servers, Data agents and Fabric agents, host cluster data, computer group, host, database computer groups, fabric SAN assets, switch assets, storage subsystem group, storage subsystems, and Tivoli Storage Productivity Center for Databases.

#### **Storage Optimizer**

The Storage Optimizer is a tool to help you analyze your storage networks to identify hot spots or bottlenecks, plan for storage growth, improve performance, and help develop storage migration or storage consolidation plans. Using the data in the Tivoli Storage Productivity Center database, the Storage Optimizer enables you to create an analysis report and an optimization report. The analysis report analyzes your data storage environment and recommends changes to improve your environment. Based on the analysis report, the optimization report includes storage migration or storage consolidation recommendations.

This feature requires an IBM Tivoli Storage Productivity Center Standard Edition license.

#### Storage resource groups

Storage resource groups are new objects provided to help storage administrators plan, monitor, and report on the managed environment.

A storage resource group is a set of entities managed by Tivoli Storage Productivity Center. These entities can be servers, switches, storage subsystems, fabrics, storage pools, and storage volumes. Storage resource groups can be a group of heterogeneous objects and can also contain other storage resource groups without any connectivity.

Policies for provisioning (volume creation and selection, workload profiles, zoning and multipathing configuration) can be specified and associated with storage resource groups. These policies are used by the SAN Planner to populate default settings.

Storage resource groups are used primarily for planning functions but is also available with the Tivoli Storage Productivity Center Basic Edition license. With the basic license, you can create and view storage resource groups in the topology. With the Standard Edition license, the planner function is enabled and you can use storage resource groups as input.

Storage resource groups also work with these profiles:

#### Workload profiles

Describes the requirements that define the performance characteristics of newly provisioned capacity.

#### **Provisioning profiles**

Describes the requirements such as total capacity, number of

volumes, Redundant Array of Independent Disks (RAID) level, volume name prefix, multipathing options, zoning options, and so forth.

#### IBM General Parallel File System<sup>™</sup>

Tivoli Storage Productivity Center supports the monitoring of the IBM General Parallel File System (GPFS<sup>™</sup>) 3.2 on AIX. GPFS provides access to critical file data. GPFS also provides concurrent high-speed file access to applications that are running on multiple nodes of an AIX cluster, a Linux cluster, or a heterogeneous cluster of AIX and Linux nodes. In addition to providing file storage capabilities, GPFS provides storage management, information life-cycle tools, centralized administration and allows for shared access to file systems from remote GPFS clusters.

#### Installation changes

#### IBM Tivoli Storage Productivity Center for Replication

The IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication Installation and Configuration Guide also includes the installation, upgrade, and uninstallation information for IBM Tivoli Storage Productivity Center for Replication. IBM Tivoli Storage Productivity Center for Replication is now installed with IBM Tivoli Storage Productivity Center.

#### IBM DB2 Database for Linux, UNIX, and Windows

Tivoli Storage Productivity Center now supports DB2 9.5. You will be able to migrate your Tivoli Storage Productivity Center databases from DB2 9.1 or DB2 8.2 to DB2 9.5. DB2 9.5 is optional. Tivoli Storage Productivity Center still supports DB2 9.1.

#### Installation of IBM Tivoli Integrated Portal

Tivoli Storage Productivity Center now installs IBM Tivoli Integrated Portal along with Tivoli Storage Productivity Center.

#### Embedded WebSphere<sup>®</sup> 6.1 and JRE 1.5

The Device server is upgraded to run under Embedded WebSphere 6.1 (from Embedded WebSphere 6.0.2). The Data server, GUI, and CLI is upgraded to use JRE version 1.5. InstallShield uses JRE 1.5 during the installation and uninstallation process when Tivoli Storage Productivity Center is installed using the disk1 image. The image to perform local agent installations uses JRE version 1.4.2.

#### Silent installation

Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication do not support silent installation except for the Data agents and Fabric agents.

#### New device and application support

#### IBM System Storage DS8000 4.2

This release supports DS8000 4.2 with these additional items:

- Storage pool striping
- Dynamic volume expansion
- Internet Protocol Version 6 (IPv6)
- Redundant Array of Independent Disks (RAID 6)
- Variable logically partitioned mode (LPARs)
- Space-efficient FlashCopy<sup>®</sup>

#### IBM System Storage SAN Volume Controller 4.3.1

This release supports SAN Volume Controller 4.3.1 with these additional items:

- Embedded CIM agent
- 64-bit logical block address (LBA) for the back end array
- 2 TB virtual disks (VDisks) and managed disks (MDisks)

#### Microsoft SQL Server 2005 and Microsoft SQL Server 2008 databases

Tivoli Storage Productivity Center can now monitor the Microsoft SQL Server 2005 and Microsoft SQL Server 2008 databases. You must configure Microsoft SQL Server before you can monitor the database. For information about configuration, see the Information Center. Search for **Configuring Microsoft SQL Server 2005 or 2008**.

#### **EMC PowerPath**

With Tivoli Storage Productivity Center, you can now use EMC PowerPath storage systems like CLARiiON and Symmetrix. Using these storage systems, you can discover host volume information and display detailed information for the volume for capacity planning purposes. Connection reports can show the connectivity from the host to the storage subsystems.

EMC PowerPath version 4.0 or later is supported.

#### Network Appliance (NetApp)

With Tivoli Storage Productivity Center, you can use the Network Appliance SMI-S agent to support block storage devices. The SMI-S agent supports the SMI-S 1.2 array profile.

#### IBM XIV Storage System

**Important:** The XIV Storage System information provided in the Tivoli Storage Productivity Center 4.1 documentation is only for planning purposes until the supported XIV Storage System software is available. Tivoli Storage Productivity Center support is targeted for a futureXIV Storage System software release. A flash will be issued when Tivoli Storage Productivity Center support for XIV Storage System is available.

XIV Storage System will have an embedded CIM agent that Tivoli Storage Productivity Center will use to run discovery and probe jobs.

You will be able to start the XIV Storage System GUI from within Tivoli Storage Productivity Center if the GUI is installed on the same system as the Tivoli Storage Productivity Center GUI. The XIV Storage System GUI will be supported on Windows and Linux.

Both the Data agent and Storage Resource agent will support XIV Storage System.

For more information about XIV Storage System planning, see "Planning for the IBM XIV Storage System" on page 71.

#### Multipath subsystem device drivers

Tivoli Storage Productivity Center supports these subsystem device drivers (SDD):

- AIX SDD
- Windows SDD
- Windows SDD DSM

- Linux SDD
- HP SDD
- Solaris SDD
- Novell SDD (reporting only)
- AIX SDD PCM
- Linux DM\_Multipath

#### IBM System Storage N Series Gateway servers

IBM Tivoli Storage Productivity Center supports IBM System Storage N Series Gateway servers as **Other NAS**. This support allows you to monitor and report on file systems through the Windows CIFS or UNIX NFS shares that are accessible to the scan or probe jobs for the Data agent. No backend storage information such as controllers, disks, and logical volumes is collected or reported.

#### High-Availability Cluster Multi-Processing

This release provides additional support for High-Availability Cluster Multi-Processing version 5.5.

#### **Tivoli Enterprise Portal**

A Universal Agent for Tivoli Storage Productivity Center that utilizes a set of Tivoli Storage Productivity Center Web services calls to gather information and provide results files that will display enhanced information such as job status and Tivoli Storage Productivity Center status in the IBM Tivoli Integrated Portal.

#### Terminology

The Tivoli Storage Productivity Center documentation uses the term "storage subsystem" and the Tivoli Storage Productivity Center for Replication documentation uses the term "storage system". Both terms refer to the devices used for storage management.

# Chapter 1. Planning for the IBM Tivoli Storage Productivity Center family

The following sections provide information to help plan your IBM Tivoli Storage Productivity Center environment before you install the product. In a complex environment, good planning helps you avoid delays and problems in getting your system up and running.

The IBM Tivoli Storage Productivity Center family includes the following programs:

- IBM Tivoli Storage Productivity Center
- IBM Tivoli Storage Productivity Center for Replication

The Tivoli Storage Productivity Center documentation uses the term "storage subsystem" and the Tivoli Storage Productivity Center for Replication documentation uses the term "storage system". Both terms refer to the devices used for storage management.

#### For the Tivoli Storage Productivity Center for Replication user

The installation for Tivoli Storage Productivity Center for Replication has changed with this release. You must now install Tivoli Storage Productivity Center with Tivoli Storage Productivity Center for Replication.

If you do not want the options available with Tivoli Storage Productivity Center, the quickest way to install Tivoli Storage Productivity Center for Replication is to use typical installation, without Agent Manager registration.

Tivoli Storage Productivity Center for Replication uses an internal database repository and does not use DB2. However, you must still install DB2 because Tivoli Storage Productivity Center requires the use of DB2 for the database repository.

These are the general steps to install Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication:

- 1. Install DB2. See "Installing DB2" on page 121.
- 2. Install Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication. See "Installing without Agent Manager registration" on page 172. The minimum components to install (without Agent Manager and agents) would be:
  - Tivoli Integrated Portal
  - Data server
  - Device server
  - Tivoli Storage Productivity Center for Replication

For information about configuration and usage information for Tivoli Storage Productivity Center for Replication, see the Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v4r1/index.jsp. Click **Tivoli Storage Productivity Center for Replication**.

## Planning to install the IBM Tivoli Storage Productivity Center family

Before installing IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication for the first time, be familiar with your operating systems, storage devices, communication protocols, and system configurations.

## Hardware requirements for the IBM Tivoli Storage Productivity Center family

The IBM Tivoli Storage Productivity Center server can require a large amount of memory, network bandwidth, and processor resources. In many cases, the server performs best when other applications are not installed on the same system.

See Table 1 for information about the minimum hardware requirements needed for the Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication servers.

Table 1. Hardware requirements for the Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication servers

Item	Hardware requirements
Processor	For Tivoli Storage Productivity Center:
	• Intel <sup>®</sup> - Dual processor 3.2 GHz
	• pSeries <sup>®</sup> - Dual POWER5
	For Tivoli Storage Productivity Center for Replication:
	• For Windows or Linux: 1 x Intel Quad-Core Xeon <sup>®</sup> or greater
	• For AIX: System p <sup>®</sup> , IBM POWER4 <sup>™</sup> or IBM POWER5 <sup>™</sup> processor, 1 GHz
Memory	8 GB of RAM. If you have at least 4 GB but less than 8 GB of RAM, you can still install Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication. However, you will get a warning message.
	If you have less than 8 GB of RAM, you should run only Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication because of system load. For information about how to disable Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication after installation, see "Disabling Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication" on page 341. <b>Note:</b> To run Tivoli Storage Productivity Center on AIX requires at least 6 GB of RAM. If you cannot run with 6 GB of RAM, increase your paging swap space. For information about paging swap space, see the man pages mkps or chps.
Disk space	• For installations on Windows, you need 6 GB of available disk space and 500 MB in the Windows temporary directory.
	• For AIX: 10 GB of free disk space.
	• For installations on AIX or Linux, you need 2.25 GB for the /tmp directory, 3 GB for the /opt directory, 250 MB in the /home directory, and 10 KB of free space in /etc.
	<b>Note:</b> Once you have installed Tivoli Storage Productivity Center and start collecting data, you will need a large amount of disk space. The amount of data collected depends on many factors, including how many devices you have, how long you keep the data, and how frequently you collect data. Some users have experienced disk space usage of about 40 - 80 GB.

Table 1. Hardware requirements for the Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication servers (continued)

Item	Hardware requirements
Network interface card (NIC)	Multiple NIC cards are not supported on the Tivoli Storage Productivity Center server. If you do have multiple NIC cards, you must make sure that the first NIC card in the list is the one that all the agents can communicate with.
Console	A console or remote-connectivity application such as KDE, Remote Desktop, or VNC is required during installation of Tivoli Storage Productivity Center. The installation program is interactive (as opposed to silent).

See Table 2 for information about the storage system requirements for Tivoli Storage Productivity Center for Replication.

Storage system	Hardware requirements				
IBM Storage System	• Release 2 minimum firmware level 6.2.410.30 or Release 3 minimum firmware level 63.1.32.0				
D58000	Advanced Copy services licenses				
	Optional Ethernet adapters for Tivoli Storage Productivity Center for Replication				
	– Single image - feature code 1801				
	- Dual image - feature code 1802 and 1803				
IBM System	Minimum firmware level 6.2.2.64				
Storage DS6000	Advanced Copy services licenses				
IBM Enterprise	<ul> <li>Minimum firmware level 2.4.4.72</li> <li>Easture codes 240 PRC and 2240 PRC</li> </ul>				
Storage Server <sup>®</sup> (ESS) 2105-800	• reature codes 240 - r KC and 2240 - r KC				
IBM System Storage SAN Volume Controller 4.2.1	Copy services licenses				
Host adapter	One or more of the following host adapter feature codes:				
feature codes	3021 - Fibre Channel/FICON Host Adapter				
	• 3023 - Fibre Channel/FICON Host Adapter				
	3024 - 2 Gb Fibre Channel/FICON Host Adapter				
	• 3025 - 2 GbFibre Channel/FICON Host Adapter				

Table 2. Storage system requirements for Tivoli Storage Productivity Center for Replication

See Table 3 on page 4 for information about the minimum hardware requirements needed for the Tivoli Storage Productivity Center agents.

Operating System	Item	Hardware requirements
Windows and Linux on	Processor	Pentium <sup>®</sup> 400 <sup>®</sup> MHz processor, or above
<ul> <li>Intel</li> <li>UNIX</li> <li>AIX on IBM eServer<sup>™</sup> iSeries<sup>®</sup>, and IBM eServer pSeries</li> </ul>	Disk space	<ul> <li>Minimum memory and space requirements to run:</li> <li>256 MB of RAM.</li> <li>For a locally installed Data agent, the temporary space required is 100 MB. For a remotely installed Data agent, the temporary space required is 250 MB. If you also have the Fabric agent installed on the same machine, that will require an additional 100 MB.</li> </ul>
All	Network interface card (NIC)	Tivoli Storage Productivity Center supports multiple NIC cards. When you install an agent on a machine locally or remotely and the machine has more than one NIC card, the Tivoli Storage Productivity Center agent installer will determine the NIC card to use for two-way communication between the server and agent. If there are no NIC cards that can be used for two-way communication, the installer will return an error message.

Table 3. Hardware requirements for the Tivoli Storage Productivity Center agents

See Table 4 for information about the minimum hardware requirements needed for the Tivoli Storage Productivity Center GUI.

Operating system	Item	Hardware requirements
Windows	Processor	Minimum is PII 500 MHz processor, suggest PII 1 GHz processor or above
	Disk space	<ul><li> 256 MB of RAM</li><li> Approximately 100 MB of hard disk space</li></ul>
	Console	1024 x 768 console or above
UNIX	Disk space	<ul><li> 256 MB of RAM</li><li> Approximately 100 MB of hard disk space</li></ul>
	Console	1024 x 768 console or above

Table 4. Hardware requirements for the Tivoli Storage Productivity Center GUI

## Software requirements

This section describes the software that is required to install and run your system. This section includes operating systems supported, browsers supported, databases supported, and other software required such as DB2.

#### Software requirements for operating systems

This section lists the operating systems supported by the IBM Tivoli Storage Productivity Center family.

Before installing IBM Tivoli Storage Productivity Center, check the IBM Tivoli Storage Productivity Center support site for the latest platform support. Go to http://www.ibm.com/systems/support/storage/software//tpc. Click on a product. Click **Install**. Look for **TPC Version 4 Release 1 Platform Support**.

Table 5. Operating system support for Data server, Device server, agents, GUI, CLI, Agent Manager, and Tivoli Storage Productivity Center for Replication

Operating system	Data agent, Fabric agent, Storage Resource agent	Tivoli Storage Productivity Center server	Tivoli Storage Productivity Center GUI and CLI	Agent Manager	Tivoli Storage Productivity Center for Replication
IBM AIX 5.3 (32-bit) POWER4 or later	All agents with AIX 5300-01 maintenance level and APAR IY70336 (see note 1)	Yes with AIX 5300-01 maintenance level and APAR IY70336 (see note 1)	Yes	Yes	Yes
IBM AIX 5.3 (64-bit) POWER4 or later	All agents in 32-bit compatibility mode with AIX 5300-01 maintenance level and APAR IY70336 (see note 1)	Yes in 32-bit compatibility mode with AIX 5300-01 maintenance level and APAR IY70336 (see note 1)	Yes in 32-bit compatibility mode	Yes in 32-bit compatibility mode	Yes in 32-bit compatibility mode
IBM AIX 6.1 (32-bit) POWER5 or later (see note 2)	All agents	Yes	Yes	Yes	Yes
IBM AIX 6.1 (64-bit) POWER5 or later (see note 2)	All agents in 32-bit compatibility mode	Yes in 32-bit compatibility mode	Yes in 32-bit compatibility mode	Yes in 32-bit compatibility mode	Yes in 32-bit compatibility mode
Sun Solaris 9 (32-bit) • SPARC	Data agents and Fabric agents	No	No	No	No
Sun Solaris 10 (32-bit) (see note 7) • SPARC	Data agents and Fabric agents	No	No	No	No
Sun Solaris 10 (64-bit) (see note 7) • SPARC	Data agents and Fabric agents in 32–bit compatibility mode	No	No	No	No
HP-UX 11 and 11i.1 (32-bit) • PA-Risc	Data agents and Fabric agents on HP-UX 11i	No	No	No	No
HP-UX 11 and 11i.1 (64-bit) • PA-Risc	Data agents and Fabric agents in 32–bit compatibility mode	No	No	No	No

Operating system	Data agent, Fabric agent, Storage Resource agent	Tivoli Storage Productivity Center server	Tivoli Storage Productivity Center GUI and CLI	Agent Manager	Tivoli Storage Productivity Center for Replication
HP-UX 11 and 11i.2 (32-bit)	Data agents and Fabric agents	No	No	No	No
HP-UX 11 and 11i.2 (64-bit) • PA-Risc	Data agents and Fabric agents in 32–bit compatibility mode	No	No	No	No
Windows 2003 Standard Edition, Windows 2003 Standard Edition Release 2 (32-bit) • x86 • AMD	All agents	Yes	Yes	Yes	Yes
<ul> <li>Windows 2003</li> <li>Standard Edition,</li> <li>Windows 2003</li> <li>Standard Edition</li> <li>Release 2 (64-bit)</li> <li>x86</li> <li>AMD</li> <li>R2 on x346</li> <li>hardware (Intel Dual Xeon 64-bit processors)</li> </ul>	All agents in 32–bit compatibility mode	Yes in 32–bit compatibility mode	Yes in 32–bit compatibility mode	Yes in 32–bit compatibility mode	Yes in 32–bit compatibility mode
Windows 2003 Enterprise Edition, Windows 2003 Enterprise Edition Release 2 (32-bit) • x86 • AMD	All agents	Yes	Yes	Yes	Yes
Windows 2003 Enterprise Edition (64-bit) • x86 • AMD Windows 2003 Enterprise Edition	All agents in 32-bit compatibility mode	Yes in 32-bit compatibility mode	Yes in 32-bit compatibility mode	Yes in 32-bit compatibility mode	Yes in 32-bit compatibility mode

Table 5. Operating system support for Data server, Device server, agents, GUI, CLI, Agent Manager, and Tivoli Storage Productivity Center for Replication (continued)

Release 2 (64–bit)

 Intel Dual Xeon 64-bit processors

• x386

Operating contents	Data agent, Fabric agent, Storage Resource	Tivoli Storage Productivity	Tivoli Storage Productivity Center GUI and	A cont Manager	Tivoli Storage Productivity Center for Poplication
Windows 2008 Standard Edition (32-bit) (see note 4)	All agents	Yes	Yes	Yes	Yes
Windows 2008 Standard Edition (64-bit) (see note 4)	All agents in 32-bit compatibility mode	Yes in 32-bit compatibility mode	Yes in 32-bit compatibility mode	Yes in 32-bit compatibility mode	Yes in 32-bit compatibility mode
Windows 2008 Enterprise Edition (32–bit) (see note 4)	All agents	Yes	Yes	Yes	Yes
Windows 2008 Enterprise Edition (64-bit) (see note 4)	All agents in 32-bit compatibility mode	Yes in 32-bit compatibility mode	Yes in 32-bit compatibility mode	Yes in 32-bit compatibility mode	Yes in 32-bit compatibility mode
Windows XP (32-bit) • x86 • AMD	No	No	Yes	No	No
Windows Vista (32-bit) • x86 • AMD	No	No	Yes	No	No
<ul> <li>Red Hat</li> <li>Enterprise Linux</li> <li>AS Version 4.0</li> <li>(32-bit and 64-bit)</li> <li>For 32-bit:</li> <li>x86 (all agents)</li> <li>pSeries</li> <li>POWER<sup>®</sup> 5 or later (Storage Resource agents only)</li> <li>iSeries</li> <li>POWER5 or later (Storage Resource agents only)</li> <li>zSeries<sup>®</sup> (s390)</li> <li>(Storage Resource agents only)</li> </ul>	<ul> <li>All agents</li> <li>For 64-bit, in 32-bit compatibility mode</li> </ul>	Yes	Yes	Yes	Yes
64-bit on x86 only					

Table 5. Operating system support for Data server, Device server, agents, GUI, CLI, Agent Manager, and Tivoli Storage Productivity Center for Replication (continued)

Operating system	Data agent, Fabric agent, Storage Resource agent	Tivoli Storage Productivity Center server	Tivoli Storage Productivity Center GUI and CLI	Agent Manager	Tivoli Storage Productivity Center for Replication
<ul> <li>Red Hat</li> <li>Enterprise Linux</li> <li>AS 5.x (32-bit and 64-bit)</li> <li>x86</li> <li>iSeries</li> <li>POWER5 or later</li> <li>pSeries power 5 or later</li> <li>zSeries (s390)</li> <li>64-bit on x86 only</li> </ul>	<ul> <li>Storage Resource agents</li> <li>For 64-bit, in 32-bit compatibility mode</li> </ul>	Yes	Yes	Yes	Yes
SuSE Linux Enterprise Server 9 (32-bit and 64-bit) • x86 • iSeries POWER5 or later • pSeries POWER5 or later • zSeries	<ul> <li>Data agents on all platforms</li> <li>Fabric agents on x86 only</li> <li>Storage Resource agents: 32-bit on all platforms</li> <li>For 64-bit, in 32-bit compatibility mode</li> </ul>	No	No	Yes	No
SuSE Linux Enterprise Server 10 (32-bit and 64-bit ) • x86 • iSeries POWER5 or later: • pSeries POWER5 or later • zSeries (s390)	<ul> <li>Storage Resource agents</li> <li>32-bit on all platforms</li> <li>For 64-bit, in 32-bit compatibility mode</li> </ul>	No	No	No	No

Table 5. Operating system support for Data server, Device server, agents, GUI, CLI, Agent Manager, and Tivoli Storage Productivity Center for Replication (continued)
Operating system	Data agent, Fabric agent, Storage Resource agent	Tivoli Storage Productivity Center server	Tivoli Storage Productivity Center GUI and CLI	Agent Manager	Tivoli Storage Productivity Center for Replication
VMware V2.5x, 3.0.x, 3.5.x	Data agents and Storage Resource	Yes on Windows 2003 and Red Hat	No	Yes	No
• Windows 2003	agents				
• Red Hat Enterprise Linux AS 3.0					
• Red Hat Enterprise Linux AS 4.0					
• SuSE Linux 8 and 9					
AIX Virtual I/O Server 1.5.2 or later (see note 13)	All agents	No	No	No	No
HACMP <sup>™</sup> on AIX (see note 6)	All agents	No	No	No	No
• v5.3.0.4 or later					
• v5.4.0.1 or later					
• v5.5 or later					

Table 5. Operating system support for Data server, Device server, agents, GUI, CLI, Agent Manager, and Tivoli Storage Productivity Center for Replication (continued)

#### Note:

- 1. If you are running AIX 5.3, you must download the AIX 5300-01 (or later) Recommended Maintenance Level. You can download this package from: http://www-912.ibm.com/eserver/support/fixes/fixcentral/main/pseries/ aix. After you have downloaded the package, then follow these steps:
  - a. On the Fix Central page, select the following:
    - **Product family**

System p

#### Product

AIX

#### Version

Enter the appropriate version.

#### Click Go.

**Note: IPv6 support:** On the Fix Central page, in the Version field, select **5.3**. In the Fix Type field, select **Fix packs**. Click **Continue**. In the Select a Technology Level field, select **TL 5300–06**. Click **Go**. Download the appropriate service pack (5300–06 Technology Level). To check whether you have the correct level, run the command **oslevel -r**. The information returned should be "5300–06."

- b. Download the appropriate maintenance level.
- 2. AIX 6.1 requires DB2 9.1 fix pack 4 or later. For IPV6–only machines, need DB2 9.1 with fix pack 2 or later.
- **3**. AIX requires a C++ run time library level of xlC.aix50.rte.9.0.0.5 or later.

- 4. Windows 2008 requires DB2 9.1 with fix pack 5 or later.
- 5. Tivoli Storage Productivity Center supports Data agents and Fabric agents installed on HACMP nodes.
- 6. The Data agents can also run in these environments:
  - NetWare 5.1, 6.0, 6.5 (NetWare 6.5 requires service pack 3 or later)
  - VMWare ESX environment (Data agent tolerance support only; does not include VMWare logical reporting enhancements).
  - MSCS Clustering Windows 2000 Advanced Server
  - MSCS Clustering Windows 2000 Datacenter
  - MSCS Clustering Windows 2003 Advanced Server
  - MSCS Clustering Windows 2003 Datacenter
  - AIX Volume Manager
  - Veritas Volume Manager on Solaris and HP-UX
  - HP-UX Logical Volume Manager
  - Network Appliance NAS
  - AIX JFS
  - HACMP 5.3.0.4 or HACMP 5.4.0.1 or later. APAR IY87543 is required for HACMP 5.3.0.4. APAR IY87447 is required for HAMCP 5.4.0.1. Also check the HACMP version compatibility matrix on the support site at HACMP Version Compatibility Matrix.
  - Veritas File System (VxFS) for AIX
  - Veritas File System (VxFS) for Solaris
- 7. The Storage Resource agents running on Red Hat Linux requires the following package to be installed:

compat-libstdc++-296-2.96-138.i386.rpm

8. For Sun Solaris 10 (32–bit and 64–bit) only the Global Zone is supported for both the Data agent and Fabric agent. The non-global (or local) zones are not supported by Tivoli Storage Productivity Center.

If you upgrade from Solaris 9 to Solaris 10, all agents need to be reinstalled completely.

- **9**. Data agents and Fabric agents running on HP-UX must have the HP libc cumulative patch PHC\_34275 installed on those machines. To download patch PHC\_34275, go to this Web site: https://www1.itrc.hp.com/service/home/home.do.
- **10**. For Fabric agents and Data agents installed on HP-UX, an HP libc cumulative patch is required to be installed on all systems running the agents. Go to the following Web site: https://www1.itrc.hp.com/service/home/home.do . Search for and download patch PHC\_34275.
- 11. For Data agents installed on Red Hat Linux AS release 4, you must have Update 5. You must also have compat-libstdc++-33 installed.
- 12. Tivoli Storage Productivity Center does not support software RAID on Linux systems. A Data agent will not install and run on Linux systems with software RAID.
- **13.** For information about IPv6 support in Windows Server 2003 Enterprise Server, see http://support.microsoft.com/kb/325449.
- 14. Before installing Tivoli Storage Productivity Center on Red Hat Linux V5, install the 32-bit version of libXp.so.6 which is available on the Red Hat installation media: OVD>/Server/libXp-1.0.0-8.1.el5.i386.rpm.

- 15. AIX Virtual I/O Server only supports IBM Tivoli Storage Productivity Center agents installed on the same partition as the Virtual I/O server. IBM Tivoli Storage Productivity Center does not support the use of virtual storage from the Virtual I/O server on other partitions.
- **16.** Red Hat, the Red Hat "Shadow Man" logo, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.
- 17. AIX is shipped with Firefox 1.5. To upgrade to Firefox 2.0 on AIX, download Firefox from the following location http://www-03.ibm.com/systems/power/software/aix/browsers/index.html.

### Software requirements for the database repository

Use this information to understand what the software requirements are for the database repository.

Tivoli Storage Productivity Center supports DB2 as the database repository.

#### DB2 database

Tivoli Storage Productivity Center supports the following products for the repository database:

- DB2 Enterprise Server Edition version 9.1 with fix pack 2 or later.
- DB2 Enterprise Server Edition version 9.5 with fix pack 3a or later.

DB2 9.1

- Tivoli Storage Productivity Center supports DB2 V9.1 with fix pack 2 or later (32-bit). For AIX, use 64-bit. On Windows 2008, use DB2 Enterprise Server Edition version 9.1 with fix pack 5 or later.
- DB2 version 9.1 does not support Red Hat Enterprise Linux AS Version 3. Red Hat Enterprise Linux AS Version 4 (32-bit) is supported. For information about DB2 Linux support, see http://www-306.ibm.com/software/data/db2/linux/validate/.
- Tivoli Storage Productivity Center supports DB2 V9.1 with fix pack 2 on AIX and Windows in 64-bit mode.

For AIX 5.3 64-bit kernel, the minimum C++ runtime level is xlC.rte 8.0.0.4 and xlC.aix50.rte 8.0.0.8. You can check for the level by running the following command:

lslpp -al | grep xlC

Also, the Technology Level should be 5300.05 and  $SP^{TM}$  5300-04-2. You can check for this level by running the following command: oslevel -r

- DB2 version 9.1 supports i386 GNU/LINUX only when the kernel is at least 2.6.9.
- DB2 V9.1 with fix pack 2 or later supports both IPv4 and IPv6. If DB2 has to be configured to communicate over IPv6 (as in an IPv6-only scenario) then DB2 V9.1 has to be used.

#### DB2 9.5

The operating systems supported by DB2 9.5 are shown in Table 6 on page 12.

Table 6. Operating systems supported by DB2 9.5

Operating system	Requirements			
AIX Version 5.3	<ul> <li>64-bit AIX kernel</li> <li>AIX 5.3 Technology Level 6 and Service Pack 2 plus APAR IZ03063</li> </ul>			
	• Minimum C++ runtime level requires the xlC.rte 9.0.0.1 and xlC.aix50.rte 9.0.0.1 file sets. These file sets are included in the August 2007 IBM C++ Runtime Environment Components for the AIX package.			
	• Hardware: 64–bit Common Hardware Reference Platform (CHRP) architecture. See note 1.			
<ul> <li>AIX Version 6.1</li> <li>Linux (suggested platform)</li> <li>Red Hat Enterprise Linux 4 or 5 with 64-bit kernel</li> <li>SUSE Linux Enterprise</li> </ul>	<ul> <li>64-bit AIX kernel</li> <li>Minimum C++ runtime level requires the xlC.rte 9.0.0.1 and xlC.aix50.rte 9.0.0.1 file sets. These file sets are included in the October 2007 IBM C++ Runtime Environment Components for the AIX package.</li> <li>Hardware: 64-bit Common Hardware Reference Platform (CHRP) architecture. See note 1.</li> <li>In AIX 6.1, there are two types of workload partitions (WPARs): System workload partitions and application workload partitions. DB2 installation is supported only on a system workload partition.</li> <li>You must install DB2 Enterprise Server Edition for SUSE Linux Enterprise Server with 64-bit kernel.</li> </ul>			
Server 10 with 64-bit kernel Windows server platforms • Windows 2003 Standard Edition (32-bit and 64-bit) • Windows 2003 Enterprise	<ul> <li>Service Pack 1 or later.</li> <li>IBM Data Server Provider for .NET client applications and CLR server-side procedures require .NET 1.1 SP1 or .NET 2.0 runtime framework.</li> </ul>			
<ul> <li>Edition (32–bit and 64–bit)</li> <li>Windows 2003 Datacenter Edition (32–bit and 64–bit)</li> </ul>	<ul> <li>Hardware: All Intel and AMD processors capable of running the supported Windows operating systems.</li> </ul>			
Note:           1. To verify that you have a CHRP architecture system, run the lscfg command. Look for				

the following output: Model Architecture: chrp.

The Windows platform is enabled for both IPv6 and IPv4 addressing. If the Windows platform is used in IPv6-only scenarios, all communication should be done over IPv6. Also, DB2 V9.1 or DB2 V9.5 has to be installed. In this scenario, Windows still has an IPv4 stack active, even if no IPv4 address is configured.

When you install Tivoli Storage Productivity Center, a single, shared database instance is created on DB2 for the Data server and Device server. The default database name is TPCDB.

At installation time, you can specify whether the DB2 database will be system-managed space (SMS) or database-managed space (DMS). In SMS, the file system manager for the operating system allocates and manages the space where the table is stored. In DMS, the database manager controls the storage space. The administrator decides which devices to use, and DB2 manages the space on those devices.

#### Software requirements for Tivoli Common Agent Services

Tivoli Common Agent Services is required only if you are installing the Data agents and Fabric agents. Tivoli Common Agent Services uses DB2 as the database repository.

When you install a new version of Agent Manager or Common agent on your system, you will be installing version 1.3. If you are at level Agent Manager 1.2.x, it is mandatory that you upgrade to Agent Manager 1.3. For information about upgrading, see "Upgrading Agent Manager" on page 360.

If you install an agent locally through the Tivoli Storage Productivity Center installation program, and a Common agent already exists on the system, the Common agent will be upgraded from version 1.2.2 to version 1.2.3. The common agents are not upgraded to 1.3; they remain at level 1.2. The common agents 1.2 will work with Agent Manager 1.3.

When the Common agent starts for the first time, it connects to the Agent Manager to register itself. The date and time on the managed system must be within 24 hours of the date and time on the Agent Manager server for successful registration. The values are compared in coordinated universal time (UTC), so the systems can be in different time zones.

Agent Manager also requires that DB2 be installed. Tivoli Storage Productivity Center only supports Agent Manager with a locally installed DB2 database.

An IPv6 environment means that IPv6 is enabled only (no dual stack is used). Therefore, in an IPv6 environment, the Agent Manager is disabled. Agent Manager and agent communication can use IPv4 only.

#### Web browser support

IBM Tivoli Storage Productivity Center starts a Web browser when you access Web pages from items in the Help menu, launch another application using its launch-in-content feature, or start IBM Tivoli Storage Productivity Center for Replication from its user interface.

The following Web browsers are supported by Tivoli Storage Productivity Center:

AIX

• Mozilla Firefox 2.0

Linux

• Mozilla Firefox 2.0

#### Windows

- Internet Explorer 7
- Mozilla Firefox 2.0 and 3.0

If you do not have a Web browser configured for use with Tivoli Storage Productivity Center when you access a Web page from its user interface, the Configure Element Launcher window is displayed. Use this window to configure a Web browser for use with the product.

## Web browser support for Tivoli Storage Productivity Center for Replication

When you start Tivoli Storage Productivity Center for Replication from within the Tivoli Storage Productivity Center, its user interface appears in a Web browser. Depending on the configuration settings for the Web browser on your computer, Tivoli Storage Productivity Center for Replication appears within a tab of an existing browser session or it appears within a new browser session.

In Firefox, you can configure how Tivoli Storage Productivity Center for Replication appears when launched from Tivoli Storage Productivity Center. To do this, complete the following steps:

- 1. Start Firefox.
- 2. Select **Tools** > **Options** from the menu bar.
- 3. Select Tabs.
- 4. Select **a new window** to indicate that you want start Tivoli Storage Productivity Center for Replication in a new Web browser session. Select **a new tab** to indicate that you want to start Tivoli Storage Productivity Center for Replication in a new tab of an existing Web browser session.

**Note:** For Internet Explorer, Tivoli Storage Productivity Center for Replication is always started in a new Web browser session.

**Note:** If you start Tivoli Storage Productivity Center for Replication from within Tivoli Storage Productivity Center, you might be logged out of the Tivoli Storage Productivity Center for Replication user interface unexpectedly. This occurs when you use Tivoli Storage Productivity Center to start a session of Tivoli Storage Productivity Center for Replication in an Internet Explorer 7 Web browser and then open and close a wizard or secondary window in that Tivoli Storage Productivity Center for Replication.

To workaround this problem, start Tivoli Storage Productivity Center for Replication from Tivoli Storage Productivity Center using Firefox, start Tivoli Storage Productivity Center for Replication from IBM Tivoli Integrated Portal, or start Tivoli Storage Productivity Center for Replication by entering its Web address directly in a Firefox or Internet Explorer 7 Web browser.

#### Web browser support for Help menu items

Tivoli Storage Productivity Center provides a number of items in its **Help** menu that you can click to learn more about how to use the product. When you click one of these items, Tivoli Storage Productivity Center launches a Web browser and displays the appropriate Web page. You must have an internet connection on the machine where you are running the Tivoli Storage Productivity Center user interface and have a default browser configured to successfully access these Web pages.

#### Software requirements for LDAP servers

For information about the LDAP servers supported, see http://www-01.ibm.com/ support/docview.wss?rs=180&uid=swg27007642. Click on the relevant operating system and then navigate to the row labeled "LDAP Servers using Federated Repository Configuration."

# Running IBM Tivoli Storage Productivity Center in a 64-bit environment

This section provides information for running IBM Tivoli Storage Productivity Center in a 64-bit environment.

If you are running Tivoli Storage Productivity Center in a 64-bit environment, note the following:

- All Tivoli Storage Productivity Center programs running in a 64-bit environment will be run in 32-bit compatibility mode.
- The database that Tivoli Storage Productivity Center uses can be running in a 64-bit instance if DB2 v9 is used.
- The Tivoli Storage Productivity Center agents must be running in a 32-bit native mode or compatibility mode environment.
- The databases to be monitored by Tivoli Storage Productivity Center must be in a 32-bit native mode or compatibility mode environment.
- Tivoli Storage Productivity Center can monitor DB2 in 64-bit native mode on Windows and AIX as long as the DB instance is created in 32-bit mode.
- When installing Tivoli Storage Productivity Center on a 64-bit Windows machine, the default directory will appear as: C:\Program Files (x86)\IBM\TPC

This default location must be changed for the installation to be successful. The suggested installation folder name is:

C:\IBM\TPC or c:\program files\ibm\tpc

When installing DB2 on a 64-bit Windows machine, change the default installation path so that it is NOT:

```
c:\Program Files (x86)\IBM\SQLLIB or
c:\Program Files\IBM\SQLLIB
```

The Windows installer puts back the (x86) into the directory path and this prevents the Tivoli Storage Productivity Center Device Server from starting.

Once installed, the Tivoli Storage Productivity Center program will run in Windows 32-bit compatibility mode.

## General planning

Use this information to plan your IBM Tivoli Storage Productivity Center environment. Topics include general configuration guidelines, TCP/IP ports used, user IDS and user rights, and SMI-S support.

## **IBM Tivoli Storage Productivity Center packages**

This topic provides information on the IBM Tivoli Storage Productivity Center packages.

Tivoli Storage Productivity Center provides four general types of support: data management, disk management, fabric management, and tape management. The following table summarizes the support provided by each function. To obtain each function, you must install the appropriate package.

Data management functions	Disk management functions	Fabric management functions	Tape management functions
<ul> <li>Host-centric</li> <li>Discovery</li> <li>Monitoring</li> <li>File system extension</li> <li>Enterprise- wide reporting</li> <li>Application-centric</li> <li>Monitor DB2, Oracle, Sybase, SQL Server</li> <li>Discovery</li> <li>Monitoring</li> <li>Chargeback</li> </ul>	<ul> <li>For storage subsystems:</li> <li>Discovery</li> <li>Monitoring</li> <li>Configuration (for example, creating volumes)</li> <li>Performance management</li> </ul>	<ul> <li>For fabrics:</li> <li>Discovery</li> <li>Monitoring</li> <li>Configuration (for example, zoning)</li> <li>Performance management</li> </ul>	For tape libraries: • Discovery • Monitoring

Table 7. IBM Tivoli Storage Productivity Center functions

The following table provides information about the packages that contain the functions.

Table 8. Packages for the Tivoli Storage Productivity Center family

Package	Function	
IBM Tivoli Storage Productivity Center Standard Edition	Contains all the functions for data management, disk management, fabric management, and tape management, plus:	
	Analytical functions	
	<ul> <li>Data path explorer view (or context-sensitive performance analysis)</li> </ul>	
	Configuration Analysis	
	Configuration History	
	SAN Planner	
IBM Tivoli Storage Productivity Center for Data	Data management functions.	
IBM Tivoli Storage Productivity Center for Disk	Disk management including performance management functions, also tape management.	
IBM Tivoli Storage Productivity Center Basic Edition	Disk management and fabric management minus performance management functions, also tape management	
IBM Tivoli Storage Productivity Center for Replication (Two Site Business Continuity license and Three Site Business Continuity license)	IBM Tivoli Storage Productivity Center for Replication functions. When you install IBM Tivoli Storage Productivity Center for Replication, no licenses will be installed. You must install the Two Site or Three Site Business Continuity license after you install IBM Tivoli Storage Productivity Center for Replication.	

Each marketing package contains the complete Tivoli Storage Productivity Center product, and all functions are installed. However the different licenses that are shipped with each marketing package will limit the functionality available at the graphical user interface level.

## General configuration guidelines

IBM Tivoli Storage Productivity Center should be configured properly for monitoring. This section provides some guidelines for configuring Tivoli Storage Productivity Center.

For the most up-to-date information on the guidelines, go to this Web site: http://www.ibm.com/servers/storage/support/software/tpc. Select a product, then click the **Install/use** tab. Click **Best Practices** and look for the document titled "Server Sizing Charts."

The following guidelines are recommended for environments that exceed any of the following characteristics:

- 100 Data agents
- 1000 Disk volumes
- 5 Disk subsystems
- 10 Fibre channel switches
- 100 Fibre channel ports

Here are some general guidelines to follow:

#### **Database repository**

The database repository should be installed across multiple physical disks, either through operating system striping or hardware RAID to ensure adequate performance of Tivoli Storage Productivity Center operations which involve database queries. A minimum of three disks is recommended, and it is recommended that these are separate disks from the Tivoli Storage Productivity Center server's host operating system location and Tivoli Storage Productivity Center product installation directory location.

#### IBM Tivoli Storage Productivity Center Java<sup>™</sup> heap size setting

The Tivoli Storage Productivity Center Data Server and Device server Java heap size should be set to the maximum value of 1.5 GB. The Tivoli Storage Productivity Center GUI should be run on a separate machine from the server if the server heap sizes are set to 1.5 GB. It is possible to increase the heap size for the Data Server or Device server to 2 GB, but this should be done only on a system that is configured with at least 6 GB of RAM. To increase the server heap size, see "Increasing memory allocation" on page 472.

#### IBM Tivoli Storage Productivity Center server host

The Tivoli Storage Productivity Center server host should meet the following requirements:

- The Tivoli Storage Productivity Center server should have dual 3.2 GHz processors with 4 GB of RAM.
- The Tivoli Storage Productivity Center server should be a dedicated computer for Tivoli Storage Productivity Center operations and not shared with other applications.
- Paging space: On AIX, the paging space should be increased to 1 GB.

#### IBM Tivoli Storage Productivity Center GUI

For large environments, the Tivoli Storage Productivity Center GUI should be installed on a separate system from the Tivoli Storage Productivity Center server.

For a stand-alone GUI, a minimum of 2 GHz processor (single), 1 GB RAM workstation for the GUI, and up to 2 GB of RAM is required if a large server is used.

#### CIM agents

When setting up your CIM agents for managing devices, it is recommended to read the CIM agent documentation first. This documentation can provide guidelines for how many devices the CIM agent can be configured to manage. If the CIM agent documentation does not include such guidelines, it is important to keep in mind that memory consumed by the CIM agent as well as the time it takes for Tivoli Storage Productivity Center to probe a device through the CIM agent is usually affected by the number of devices that the CIM agent manages. If no guidelines are available in the disk array subsystem CIM agent documentation, it is recommended to limit three subsystems per CIM agent.

#### Storage subsystems

When probing storage subsystems that are registered with the same SMI-S Agent, do not probe more than three storage subsystems within the same probe job because the increased load on the agent would increase the likelihood of time-outs. Instead, spread the storage subsystems across multiple probe jobs with different starting times.

# Planning for IBM Tivoli Storage Productivity Center authorization

When a user ID is authenticated to IBM Tivoli Storage Productivity Center through the GUI, CLI, or APIs, group membership (either an LDAP-compliant repository group or an operating system group) determines the user's authorization level in IBM Tivoli Storage Productivity Center. This topic describes the user roles and authorization levels.

If you want to install IBM Tivoli Storage Productivity Center so that it authenticates its users against an LDAP-based repository, then you must ensure that your LDAP-based repository contains at least one group and at least one user who is a member of that group (and who also has a value in the userPassword attribute) before installation. You will use this LDAP user and LDAP group as the LDAP TPC Administrator username and LDAP TPC Administrator group values respectively during IBM Tivoli Storage Productivity Center installation. The IBM Tivoli Storage Productivity Center installation program automatically maps the LDAP TPC Administrator group value to the IBM Tivoli Storage Productivity Center Superuser role.

If you want to install IBM Tivoli Storage Productivity Center so that it authenticates its users against the operating system repository, then you do not have to create any groups or users before installation. The IBM Tivoli Storage Productivity Center installation program automatically maps the IBM Tivoli Storage Productivity Center Superuser role to the "Administrators" group (which contains the user "Administrator") on Windows, to the "system" group (which contains the user "root") on AIX, or to the "root" group (which contains the user "root") on Linux. For more information about user roles, see "Role-to-Group Mappings" on page 279.

# TCP/IP ports used by the IBM Tivoli Storage Productivity Center family

This topic lists the default ports that should be opened through the firewall when you install the IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication servers. You must disable the firewall program or open the ports to allow incoming requests to the IBM Tivoli Storage Productivity Center ports. Review these ports before installing the IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication.

## TCP/IP ports used by IBM Tivoli Storage Productivity Center

See Table 9 for the IBM Tivoli Storage Productivity Center ports.

Component	Session initiator (server perspective)	Inbound/ outbound (server perspective)	Port	Inbound/ outbound (agent perspective)	Session initiator (agent perspective)
Data server		Both	Default: 9549 (see note 1)		
Device server		Both	9550		
Common agent	Yes	Outbound	9510	Inbound	No
Agent Manager	No	Inbound	9511	Outbound	Yes
Agent Manager	Yes	Both	9512	Both	Yes
Agent Manager	No	Inbound	9513	Outbound	Yes
Common agent (no access needed)			9514	Local to server	
Common agent(no access needed)			9515	Local to server	
Agent Manager	No	Inbound	80	Outbound	Yes
Remote installation of UNIX agent	Yes	Outbound	SSH (22)	Both	No
Remote installation of Windows agent	Yes	Outbound	NetBIOS Sessions Service (139)		
Remote installation of UNIX agent	Yes	Outbound	RSH (514)	Both	No

Table 9. TCP/IP ports used by IBM Tivoli Storage Productivity Center

Component	Session initiator (server perspective)	Inbound/ outbound (server perspective)	Port	Inbound/ outbound (agent perspective)	Session initiator (agent perspective)
Remote installation of UNIX agent	Yes	Outbound	REXEC (512)	Both	No
Remote installation of UNIX agent	Yes	Inbound	601		
Remote installation of all agents	Yes	Inbound	Data Server 9549		
Device server to CIM agent	Yes	Outbound	Default: HTTP: 5988 HTTPS: 5989		
VMware VI Data Source to VirtualCenter or ESX server	Yes	Outbound	Default: HTTP: 80 HTTPS: 443		
Tivoli Integrated Portal server. See note 5.	Yes	Outbound	389		
Device server. See note 5.	Yes	Outbound	389		
IBM Tivoli Storage Productivity Center for Replication server. See note 5.	Yes	Outbound	389		

Table 9. TCP/IP ports used by IBM Tivoli Storage Productivity Center (continued)

1. Data server inbound server port plus another port that is 10 greater than the Data server port (9549). For example, if the Data server port is 9549, than another port would be 9549+10 or 9559.

- 2. If you choose to use a port other than the default port (9510) for the Common agent, make sure that the port you choose, and the ports above it, are available for use. For example, if N represents the open port you want to use, ensure that ports N+4 and N+5 are open as well.
- **3.** When you install the Data agent, you can specify a listener port for a remote probe. This is the port that the program uses to communicate back to the installation program.
- 4. You can find the port numbers used on your system by running the following command:

netstat -an

5. If you intend to install IBM Tivoli Storage Productivity Center so that it authenticates users against an LDAP-compliant repository, then the Embedded WebSphere Application Servers for Tivoli Integrated Portal, IBM Tivoli Storage Productivity Center Device server, and IBM Tivoli Storage Productivity Center for Replication need to be able to initiate an outbound connection to the LDAP-compliant repository, which typically listens on port 389.

# Other TCP/IP ports used by IBM Tivoli Storage Productivity Center

Port	Default
DB2	50000
CIM agent for SAN Volume Controller	For proxy CIM agent: 5988 (http) 5989 (https)
CIM agent for IBM TotalStorage Enterprise Storage Server (ESS)	5989
CIM agent for DS8000	6989 (for embedded CIM agent, cannot be changed) 5989 or 5988 (proxy CIM agent, can be changed)
IBM Tivoli Storage Productivity Center with DS8000 GUI	8451 8452
IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication	162 (default SNMP listening port)

Table 10. Other TCP/IP ports used by IBM Tivoli Storage Productivity Center

# TCP/IP ports used by IBM Tivoli Storage Productivity Center for Replication

Table 11 shows the ports used for incoming communication. Table 12 shows the ports used for outgoing communication.

Table 11.	TCP/IP	ports	used	by IB	M Tivo	li Storage	Productivity	Center for	Replication	for
incoming	commu	nicatio	on							

Port	Description		
3080 and 3443	A Web browser typically communicates with the IBM Tivoli Storage Productivity Center for Replication GUI using HTTP ports 3080 and 3443. These ports are configurable from the IBM Tivoli Storage Productivity Center for Replication installer during installation.		
5110	The IBM Tivoli Storage Productivity Center for Replication command line and GUI typically communicate with the IBM Tivoli Storage Productivity Center for Replication server using port 5110.		
5120IBM Tivoli Storage Productivity Center for Replication uses port 5120 for communication with other IBM Tivoli Storage Productivi Center for Replication servers for high-availability purposes.			
<b>Note:</b> If you changed ports 3080 or 3443 during the installation or made changes to the other port settings, note the values to which these settings were changed.			

Table 12. TCP/IP ports used by IBM Tivoli Storage Productivity Center for Replication for outgoing communication

Port	Description
2433	For communication with ESS.
1750	For communication with DS Storage Systems.

Table 12. TCP/IP ports used by IBM Tivoli Storage Productivity Center for Replication for outgoing communication (continued)

Port	Description
22	For communication with SAN Volume Controller devices.
Mate	

Note:

- If you changed the port configuration of your storage controller, the ports would be different.
- Your network configuration should allow for IBM Tivoli Storage Productivity Center for Replication to send outgoing TCP/IP packets to the storage controllers. It is possible when adding the storage controllers to IBM Tivoli Storage Productivity Center for Replication to set a specific port number for your storage controller.
- Since there are typically multiple applications running on a server, it is possible that port conflicts might arise if other applications attempt to use the same ports that IBM Tivoli Storage Productivity Center for Replication is using. You can find the port numbers used on your system by running the following command:

netstat -an

- If firewalls are being used in your configuration, make sure that none of these ports are being blocked. Ensure that not only is the IBM Tivoli Storage Productivity Center for Replication server granted access to reach the other components, but that the other components are granted access to reach the IBM Tivoli Storage Productivity Center for Replication server.
- If you are running Windows Server 2008, you need to configure the inbound and outbound rules for IBM Tivoli Storage Productivity Center for Replication. To create a new outbound rule, launch the New Outbound Rule Wizard from the Windows Firewall with Advanced Security menu.

## Planning for User IDs and user rights

This section provides information about the user IDs and user rights required to install IBM Tivoli Storage Productivity Center.

Before installation, create one unique Windows administrator user ID or UNIX user ID with root authority to be used for installing all Tivoli Storage Productivity Center products. To create the database schema, the user ID also needs database administrator authority. This user ID is required only to install the product and is not required to run the product.

To install Tivoli Storage Productivity Center on Windows, the user ID must belong to the administrators and DB2ADMNS group and have the user rights shown in the table below. This user ID can be for a local account or domain account.

On UNIX or Linux, the user must have root authority.

Component	User rights on Windows 2003	User rights on Windows 2008
Device server or Data Server	<ul> <li>Log on as a service</li> <li>Act as part of the operating system</li> <li>Adjust memory quotas for a process</li> <li>Create a token object</li> <li>Debug programs</li> <li>Replace a process-level token</li> </ul>	<ul> <li>Log on as a service</li> <li>Act as part of the operating system</li> <li>Adjust memory quotas for a process</li> <li>Create a token object</li> <li>Debug programs</li> <li>Replace a process-level token</li> </ul>
	<b>Note:</b> This user ID is automatically given the appropriate user rights when you install DB2.	<b>Note:</b> This user ID is automatically given the appropriate user rights when you install DB2.
Data agent or Fabric agent only	<ul><li>Act as part of the operating system</li><li>Log on as a service</li></ul>	<ul><li>Act as part of the operating system</li><li>Log on as a service</li></ul>
GUI or CLI only	None	None
Create database schema	Needs to be in DB2ADMNS group and Administrators group.	Needs to be in DB2ADMNS group and Administrators group.

Table 13. Requirements for user rights on Windows for installation

## Work sheet for user IDs and passwords

This section provides a work sheet to help you keep track of user IDs and passwords during the planning and installation of IBM Tivoli Storage Productivity Center.

Item	Description	Your input
DB2 administrator user ID and password	This user ID and password is required to install Tivoli Storage Productivity Center. On Windows, this user ID must be a member of the DB2ADMNS group and Administrators group. On UNIX, the user ID must be the instance owner of the instance you wish to use. This user ID and password is created when you install DB2.	
Certificate authority password	This password allows you to look at the certificate files if you have problems. Specified when you install the Agent Manager.	

Table 14. User IDs and passwords for Tivoli Storage Productivity Center installation

Item	Description	Your input
Common agent registration password	This is the password required by the Common agent to register with the Agent Manager. Specified when you install the Agent Manager. You must specify this password when you install the Common agent. To change the Common agent registration password, see "Changing the agent registration password" on page 481.	
Common agent service logon user ID and password	This is for Windows only and is optional. This creates a new service account for the Common agent to run under. If your enterprise has a security policy that requires long passwords, the installation can fail. This user ID and password allows you to run under a local account user name and password that meets your enterprise's security policy. This user ID and password will be created if you do not have one.	No default. If this user ID and password does not exist, these will be created at installation time.
Host authentication password	<ul> <li>This password is required for:</li> <li>the Fabric agent to communicate with the Device server</li> <li>the subordinate server when added to the master server (for enterprise-wide reporting)</li> <li>Specified when you install the Device server. You must specify this password when you install the Fabric agent.</li> </ul>	This password is created when you install the Device serverr.
NAS filer login user ID and password	This is for Windows only. This is the default user name and password used by Data agents during NAS discovery.	

Table 14. User IDs and passwords for Tivoli Storage Productivity Center installation (continued)

Item	Description	Your input
Resource manager registration user ID and password	This is the user ID and password required by the Device server and Data server to register with the Agent Manager. You must specify this user ID and password when you install the Device server or Data server. For information on how to change the user ID and password, see "Changing the registration password for a resource manager" on page 483.	The default user ID is <b>manager</b> . The default password is <b>password</b> .
WebSphere administrator user ID and password	This is the user ID and password required by the Device server to communicate with embedded WebSphere. Embedded WebSphere runs as a Windows Service. The Windows Service runs under the authority of this user ID and password. This user ID and password is only used when you install the Device server.	If this user ID and password does not exist, these will be created at installation time.
Windows Service account and password	This account and password is valid for Windows only and lets the agent run under this service account.	When you install the Tivoli Storage Productivity Center agent, you will be able to specify a domain name which validates the account and password.

Table 14. User IDs and passwords for Tivoli Storage Productivity Center installation (continued)

Item	Description	Your input
LDAP Tivoli Storage Productivity Center Administrator username and password and LDAP Tivoli Storage Productivity Center Administrator group	These values are relevant if you install Tivoli Storage Productivity Center so that it authenticates users against an LDAP-compliant repository. The username, password, and group must already exist in your LDAP-compliant repository in the "branches" specified by the "Relative Distinguished Name for usernames" and the "Relative Distinguished Name for groups" values. The user must also be a member of the group.	During the Tivoli Storage Productivity Center installation, the LDAP Tivoli Storage Productivity Center Administrator username value is used to set the WebSphere Administrative ID value for the Tivoli Integrated Portal server, the Tivoli Storage Productivity Center Device server, and the Tivoli Storage Productivity Center for Replication server. Also during the Tivoli Storage Productivity Center installation, the LDAP Tivoli Storage Productivity Center Administrator group value is mapped to the "superuser" role in Tivoli Integrated Portal, Tivoli Storage Productivity Center, and Tivoli Storage Productivity Center for Replication to allow initial access to the applications once the installation is complete.

Table 14. User IDs and passwords for Tivoli Storage Productivity Center installation (continued)

For information about valid user IDs and passwords, see "Valid characters for user IDs and passwords" on page 607

## Supported subsystems, devices, file systems, databases

This section provides information about the subsystems, tape libraries, file system formats, and databases that IBM Tivoli Storage Productivity Center supports.

#### Storage subsystems

IBM Tivoli Storage Productivity Center supports IBM and independent software vendors systems that are Storage Management Interface Specification (SMI-S) compatible. This support includes storage provisioning, as well as asset and capacity reporting. Tivoli Storage Productivity Center implements many of its disk, tape, and fabric management functions through exploitation of the SMI-S standards.

The IBM storage subsystems supported are as follows:

- IBM System Storage SAN Volume Controller
- IBM Tivoli Storage Enterprise Storage Server(Tivoli Storage Enterprise Storage Server)
- IBM Tivoli Storage Productivity Center Disk Subsystems (DS4000, DS6000, and DS8000 series)
- FAStT
- IBM XIV Storage System

• SMI-S certified subsystems. For information about SMI-S certified subsystems, see http://www.snia.org/ctp/conformingproviders#10provider.

For more information about the storage subsystems supported, hardware models, microcode levels, and relevant storage device APIs required, see this Web site: http://www.ibm.com/servers/storage/support/software/tpc. Click on Tivoli Storage Productivity Center for Data or Disk. Select the Install and Use tab. Click on the "Supported Products List" link.

#### Switches

IBM Tivoli Storage Productivity Center supports IBM and independent software vendor switches that are Storage Management Interface Specification (SMI-S) compatible.

Tivoli Storage Productivity Center supports the following switches:

- Brocade
- Cisco
- CNT
- IBM 2005, 2026, 2027, 2031, 2032, 2061, 3534
- McDATA Intrepid 10000
- McDATA Sphereon
- QLogic

For information about the specific models supported, see http://www-1.ibm.com/ support/docview.wss?rs=1134&uid=swg21249383.

#### Tape libraries

This section provides information about the tape libraries that IBM Tivoli Storage Productivity Center supports.

Tivoli Storage Productivity Center supports the following tape libraries:

- Tivoli Storage Productivity Center 3494 Tape Library The 3494 tape library can be used for data consolidation to help achieve higher performance and reduced requirements for tape drives and cartridges, environmental controls and personnel. The 3494 tape library supports WORM and standard rewritable media, providing further opportunity for consolidation.
- IBM System Storage TS3500 Tape Library (formerly Tivoli Storage Productivity Center 3584 Tape Library) The TS3500 Tape Library is designed to provide a highly scalable, automated tape library for mainframe and open systems backup and archive in midrange to enterprise environments.
- IBM System Storage TS3310 Tape Library is a modular, scalable tape library designed to grow as your needs grow.

Tivoli Storage Productivity Center supports IBM and non-IBM tape libraries through the SMI-S (CIM) agent. This assumes that the tape library supports the SMI-S 1.1. profile for tape libraries.

#### Note:

• The media changers displayed by Tivoli Storage Productivity Center for the TS3500 tape libraries are really logical partitions of the given library, and not physical accessors.

- Depending on the size of the tape library and network latency between the SMI-S agent host and the tape library, probes of the tape library might take a long time and might fail because of time-outs.
- The SMI-S agent does not display an exception to the SMI-S client such as Tivoli Storage Productivity Center when communication between the SMI-S agent and the tape library fails. Instead, empty result sets are returned. This limits Tivoli Storage Productivity Center's capabilities in detecting connection failures relating to tape libraries.
- In this release, support for the IBM 3494 Tape Libraries is limited to discovery and in-place launching of the ETL Specialist. This assumes that the SMI-S agent has been configured accordingly.
- When probing tape libraries that are registered with the same IBM SMI-S Agent for tape, do not probe more than two or three tape libraries within the same probe job because the increased load on the Agent would increase the likelihood of time outs. Instead, spread the libraries across multiple probe jobs with different start times.
- After the tape libraries are registered, and then a change is made to the IBM SMI-S Agent for Tape, a condition can occur where not all of the tape cartridges are returned to the CIM client, in this case, Tivoli Storage Productivity Center. To resolve this situation, restart the IBM SMI-S Agent for Tape; refer to the documentation for the SMI-S Agent for instructions on how to do this.

The same issue may occur if one out of a set of libraries registered with the same agent is unavailable, for example, because of a network problem. To work around this problem, unregister the affected library from the agent (or fix the communication problem).

#### **Databases for monitoring**

This section lists the databases that the Data Manager can monitor.

The Data Manager can monitor these databases:

- DB2 8.1 with fix pack 14
- DB2 8.2 with fix pack 7a
- DB2 9.1
- DB2 9.5
- Microsoft SQL Server 7.0
- Microsoft SQL Server 2000
- Microsoft SQL Server 2005

**Note:** There are some configuration steps required before you can monitor the Microsoft SQL Server 2005 database. For information about configuration, see "Configuring Microsoft SQL Server 2005 or 2008" on page 285.

• Microsoft SQL Server 2008

**Note:** There are some configuration steps required before you can monitor the Microsoft SQL Server 2008 database. For information about configuration, see "Configuring Microsoft SQL Server 2005 or 2008" on page 285.

- Oracle 8i
- Oracle 9i
- Oracle 10g
- Sybase

### **File systems**

This section lists the file systems that are supported for monitoring and reporting by IBM Tivoli Storage Productivity Center.

The Data Server supports monitoring and reporting of the following file systems:

- EXT2, EXT3
- FAT, FAT32
- GPFS file system
- HP-UX's HFS file system
- JFS, JFS2
- Network File System
- NTFS4, NTFS5
- NetWare\_FAT, NetWare\_NSS
- REISERFS
- IBM Tivoli Storage Productivity Center SAN File System
- Network Applicance's Data ONTAP V7, including flexible volumes (FlexVol). Flexvol enables you to create multiple flexible volumes on a large pool of disks.
- TMPFS
- UFS
- VXFS
- WAFL

#### Networked file systems

This section lists the networked file systems that are supported for monitoring and reporting byIBM Tivoli Storage Productivity Center.

When using the Data server, you can use the monitoring and reporting of the following networked file systems:

- IBM Tivoli Storage Productivity Center SAN File System 1.1 (Version 1 Release 1), from Windows 2000 Server and Advanced Server clients.
- IBM Tivoli Storage Productivity Center SAN File System 2.1, 2.2 from Windows 2000 Server and Advanced Server, Red Hat Enterprise Linux 3.0 Advanced Server, and Sun Solaris 9 clients.
- IBM General Parallel File System (GPFS) Version 2.3, 3.1, and 3.2 on AIX.

The IBM Tivoli Storage Productivity Center Data agent must be installed on one node within a GPFS *nodeset*. A nodeset is a collection of computers that see the same file system. If multiple agents are installed per GPFS nodeset, the first agent that sees the file system owns the file system. You cannot change the owning (or scanning) agent. If the agent is deleted, another agent takes ownership.

Because only one agent owns the file system and a file system cannot be scanned by more than one agent, there is no benefit to having more than one agent.

If more than one agent is installed, the last agent that runs a probe job takes ownership of the volume group. If a GPFS file system exists in that volume group and the agent that owns the volume group is not the agent that owns the file system, the file system information is not displayed in the volume group that is part of the asset tree. However, when the agent that owns the file system probes again, the data is corrected. There must be physical access to the GPFS disk for IBM Tivoli Storage Productivity Center to gather hardware disk information. File system information is gathered.

If the cluster manager for AIX HACMP is installed, the levels supported are shown in the following table.

Table 15. Supported software levels for an HACMP cluster type

Operating system	НАСМР
AIX 6.1 AIX 5.3	HACMP 5.5 HACMP 5.4 (with IY89869) HACMP 5.3 )with IY80002)
AIX 5.3	HACMP 5.3

#### **Volume managers**

This section lists the volume managers supported for monitoring by IBM Tivoli Storage Productivity Center.

The Data Server supports the monitoring of the following volume managers:

- Veritas Volume Manager on Sun Solaris
- Veritas Volume Manager on HP-UX
- AIX Logical Volume Manager (LVM)
- HP-UX Logical Volume Manager

Using these volume managers, you can create groups of logical volumes and disks. You can generate a variety of reports for these disk and volume groups.

### Planning for subsystem device drivers

This topic lists the multipath subsystem device drivers (SDD) that you can use with IBM Tivoli Storage Productivity Center.

The subsystem device driver (SDD) is a software solution for multiple configuration environments in supported storage devices. It resides in a host system with the native disk-device driver and provides the following functions:

- Enhanced data availability
- Dynamic input/output (I/O) load balancing across multiple paths
- Automatic path failover protection
- You can download licensed machine code at the same time that applications are running

With IBM Tivoli Storage Productivity Center, you can use these subsystem device drivers (SDD):

- AIX SDD
- Windows SDD
- Windows subsystem device driver device specific module (SDDDSM)
- Linux SDD
- HP SDD
- Solaris SDD
- Novell SDD (reporting only)
- AIX subsystem device driver path control module (SDDPCM)
- Linux DM\_Multipath

#### Note:

- 1. The AIX SDD cannot coexist with SDDPCM on the same system.
- 2. The Linux SDD driver is no longer available. Starting with Red Hat Enterprise Linux Version 5 and SUSE Linux Enterprise Server Version 10, only the DM\_Multipath is available. With DM\_Multipath, you can only use the round-robin policy for the SAN Planner.

You can use the subsystem device drivers with these devices and application:

- IBM Tivoli Storage Enterprise Storage Server (Tivoli Storage Enterprise Storage Server)
- IBM System Storage DS8000
- IBM System Storage DS6000
- IBM System Storage SAN Volume Controller

For more information about how to install, configure, and use the subsystem device drivers, see http://www.ibm.com/support/docview.wss?rs=540 &context=ST52G7&uid=ssg1S7000303.

#### Upgrading subsystem device drivers

SDD drivers cannot coexist on the same host with the SDDPCM, SDDDSM, or DM\_Multiplath drivers. You must upgrade from the existing SDD drivers to the SDDPCM or SDDDSM driver. Part of the upgrade process is to unconfigure and remove all SDD vpath devices. After the upgrade and configuration of the devices, the device names might differ from the previous names. Each device is detected by Tivoli Storage Productivity Center as a new device. For information about how to upgrade SDD, see http://www.ibm.com/support/docview.wss?rs=540 &context=ST52G7&uid=ssg1S7000303.

## Planning for EMC PowerPath Multipathing

IBM Tivoli Storage Productivity Center supports EMC PowerPath Multipathing.

EMC PowerPath Multipathing supports a wide range of servers including cluster servers connected to EMC storage systems. It tunes your storage area network and selects alternate paths for your data if necessary. It also integrates multiple path I/O capabilities, automatic load balancing, and path failover functions. For more information about EMC PowerPath Multipathing, see http://www.emc.com. Search for EMC PowerPath.

IBM Tivoli Storage Productivity Center supports basic EMC PowerPath Multipathing version 4.0 or later.

Disks provided by the EMC PowerPath driver are detected by IBM Tivoli Storage Productivity Center's Data agents and Storage Resource agents. The disks will be visible in the topology viewer and in Data Manager asset reports. The correlation of EMC PowerPath provided hdisks to EMC storage systems is supported and the relation is visible in the topology viewer. Multipathing information is not available for those disks. The data reports are accurate because they do not double-count capacities. The Data Path Explorer does not show multipathing. The SAN Planner does not support configuring multipathing on hosts using EMC PowerPath Multipathing.

## **Planning for Storage Resource agents**

Storage Resource agents are a type of agent that can collect information from computer systems (host systems) on which they are installed. Information is collected through probe jobs. These agents are designed to be more lightweight and easier to install or deploy than the Data agents.

You can do the following tasks with Storage Resource agents:

- Use Storage Resource agents to gather information by running probe jobs against the host systems on which they are installed. This function mirrors the probing capabilities of the existing Data agent and provides information to the following functions within IBM Tivoli Storage Productivity Center:
  - Asset reports (including HBA data)
  - Capacity reports (such as Data Manager > Reporting > Capacity > disk capacity, filesystem capacity, filesystem used space, filesystem free space)
  - Availability reports (such as Data Manager > Reporting > Availability > computer uptime)
  - Subsystems to host storage correlation (such as Disk Manager > Reporting > Storage Subsystems)
  - Data path explorer (not available with the IBM Tivoli Storage Productivity Center Basic Edition license)

See "Reports for Data agents and Storage Resource agents" on page 301 to view a list of reports for which Storage Resource agents collect information.See the Information Center. Search for **Reports for Data agents and Storage Resource agents** to view a list of reports for which Storage Resource agents collect information.

- Deploy or install Storage Resource agents through the user interface rather than an installation wizard. You can have only one type of agent per host that points to the same server. For example, if you install a Storage Resource agent, and then later install a Data agent on the same host that points to the same Data server, the Storage Resource agent is automatically uninstalled after the Data agent runs a successful probe job.
- List deployed Storage Resource agents in the following locations:
  - Administrative Services > Data Sources > Data/Storage Resource agents page
  - Tivoli Storage Productivity Center > Configuration Utility > Services page
  - Tivoli Storage Productivity Center > Configuration Utility > Data Manager page

Storage Resource agents are not part of the Tivoli Common Agent Services framework and do not require the Agent Manager to be installed. They do not require a JRE to be installed on the same system.

You deploy Storage Resource agents through the Tivoli Storage Productivity Center user interface. You must have administrative privileges to deploy the Storage Resource agent.

To deploy a Storage Resource agent, expand **Administrative Services** > **Configuration**. Right-click **Storage Resource Agent Deployments**. Click **Create Storage Resource Agent Deployments**. In the right pane, the Create Storage Resource agent Deployments window opens. From this window, you can enter host names from a Microsoft directory, enter host names manually, or import a host list file. You can schedule a job to add the Storage Resource agents at a time

that is convenient for you. You can also specify the type of alerts to generate if a job fails. After you enter information for the Storage Resource agent, you can optionally validate the connection to the Data server. This step helps eliminate most of the possible failure cases after you have submitted the job for Storage Resource agent deployment.

## Storage Resource agent and Data agent protocol support

When installing the Storage Resource agent or Data agent, Tivoli Storage Productivity Center uses specific protocols for connectivity between the server and agent.

When installing the Storage Resource agent or Data agent, Tivoli Storage Productivity Center uses the following protocol for connectivity between the server and agent (listed in order):

1. Secure shell protocol (SSH).

Note: Cygwin is only supported for the Storage Resource agent.

- 2. Windows server message block protocol (SMB protocol).
- 3. Remote execution protocol (REXEC).
- 4. Remote shell protocol (RSH).

At run time, the connectivity used between server and agent is dependent on the type of service is running: on-demand service (non-daemon service) or run as a service (daemon service).

#### on-demand service (non-daemon service)

In this case, connectivity between the server and agent is established using the same protocols as for installation of the agent: SSH, SMB, REXEC, or RSH.

#### run as a service (daemon service)

In this case, connectivity between the server and agent is established using the secure shell protocol. The server and agent will have their respective certificates and no additional information is needed besides the certificates and the security provided by the SSH protocol.

The information required for these protocols are as follows:

#### SSH protocol

There are two cases where you can use the SSH protocol:

- You supply the user ID and password to connect to the server using the SSH protocol. This user ID must have administrative privileges.
- You supply a user ID, certificate, and passphrase. You create the certificate and use that certificate when you connect to the agent. This certificate must be accessible from the server.

For information about how to create a certificate for SSH protocol connectivity, see "Creating a certificate for SSH protocol" on page 302. This uses Cygwin for the Storage Resource agent.

#### Windows SMB protocol

You supply the user ID and password. The user ID must have administrative privileges. You must also enable **File & Printer Sharing for Microsoft Windows** under **Network Properties** for the connected network adapter. Make sure that the Server service is running on the system.

#### **REXEC** protocol

You supply the user ID and password. The user ID must have administrative privileges. The system must be enabled for remote execution of commands.

#### RSH protocol

You supply the user ID with administrative privileges. The system must be enabled for the user to be able to run commands through the remote shell.

To enable RSH, edit the .rhosts file in the login directory of the user. This provides access for the user to connect from a remote system.

If you elect to use a Microsoft directory, you can also get a list of domain computers. You are required to enter the domain controller, user ID, password, and certificate location. After the list is displayed, you can select a list of computers on which to deploy the agent.

After the agent has been deployed, a probe job is automatically run.

The agent deployed on a Windows system has its registry information in the Windows registry. For UNIX or Linux, the registry information is stored in the following file: /etc/Tivoli/TPC/StorageResourceAgent.

For more information about setting up the environment for installing Storage Resource agents and Data agents, see Appendix A, "General information for Storage Resource agents and Data agents," on page 627.

## Planning for Internet Protocol Version 6

IBM Tivoli Storage Productivity Center supports Internet Protocol Version 6 (IPv6) for communication between its components. The key IPv6 enhancement is the expansion of IP address spaces from 32 bits (up to 15 characters in length) to 128 bits (up to 45 characters in length).

#### Overview

You can install and run Tivoli Storage Productivity Center on computers that are enabled for IPv4, IPv6, or dual stack. *Dual stack* indicates that a machine has both the IPv4 and IPv6 stacks enabled and both addresses configured. The following table shows the internal components of Tivoli Storage Productivity Center that can communicate with each other using IPv6.

Table	16.	IPv6	communication	for	internal	Tivoli	Storage	Productivity	Center compon	ents

Components in this column can communicate over IPv6 with the components in the second column	Tivoli Storage Productivity Center components
User interface	Data server
Data server	Device server database repository
Device server	database repository tpctool (command-line tool) SRMCP

Components in this column can communicate over IPv6 with the	
components in the second column	Tivoli Storage Productivity Center components
database repository	Data server
	Device server
	Repocopy tool
	Tivoli Storage Productivity Center universal agent
tpctool (command-line tool)	Device server
SRMCP	Device server
Repocopy tool	database repository
Tivoli Storage Productivity Center universal agent	database repository

Table 16. IPv6 communication for internal Tivoli Storage Productivity Center components (continued)

Tivoli Storage Productivity Center can communicate with the following external components over IPv6:

- SMI-S CIM agents
- SLP directory agents
- Out of band SNMP agents
- Storage devices (for example, the DS8000 element manager). Note that IBM XIV Storage System does not support IPv6.
- SMTP server

**Note:** These external components must be IPv6 enabled to communicate with Tivoli Storage Productivity Center using the IPv6 protocol.

Not all components and their related functions of Tivoli Storage Productivity Center are enabled for IPv6. Any functions that are not enabled for IPv6 will be unavailable through the user interface when you install Tivoli Storage Productivity Center on an IPv6-only system. See "IPv6 considerations in IBM Tivoli Storage Productivity Center" on page 37 for information about the functions that are currently not supported under IPv6 communication.

### Installation options

This section provides an overview of the installation options for installing and upgrading Tivoli Storage Productivity Center depending on the IP protocol enabled in your environment:

#### Installing Tivoli Storage Productivity Center on an IPv6-only machine

You can install Tivoli Storage Productivity Center on a system configured only for IPv6. This installation of the product can communicate with other Tivoli Storage Productivity Center servers (for rollup probes and reporting), SMIS CIM agents, out of band SNMP agents, and storage devices operating in IPv6 or dual stack mode. The product cannot communicate with storage entities located on IPv4-only systems.

If you install Tivoli Storage Productivity Center or its database repository on an IPv6-only system, you must use *DB2 Database V9.1 Fix Pack 2 or later* 

*for the Linux or UNIX* database repository. You cannot configure systems that are running Windows 2003 Server Enterprise Edition for IPv6-only.

See "Installation scenarios for Tivoli Storage Productivity Center" on page 40 for more information about this installation option. See "IPv6 considerations in IBM Tivoli Storage Productivity Center" on page 37 for information about the limitations of installing the product on IPv6-only systems.

**Installing Tivoli Storage Productivity Center on a dual stack machine** You can install Tivoli Storage Productivity Center on a dual stack system where both IPv6 and IP4 addresses are enabled. This installation of the product can communicate with Data agents, Fabric agents, other Tivoli Storage Productivity Center servers (for rollup probes and reporting), SMIS CIM agents, out of band SNMP agents, and storage devices operating in IPv6-only, dual stack mode, or IPv4-only modes. Communication with the Data agents and Fabric agents does not work in an IPv6-only environment.

See "Installation scenarios for Tivoli Storage Productivity Center" on page 40 for more information about this installation option.

**Installing Tivoli Storage Productivity Center on an IPv4-only machine** You can install Tivoli Storage Productivity Center in an IPv4-only environment. However, IPv6 communication for the Data and Device servers are disabled and you cannot enter IPv6 addresses in the user interface.

#### Upgrading Tivoli Storage Productivity Center for use with IPv6

You must upgrade to Tivoli Storage Productivity Center v3.3.2 or later if you want to enable the product to use the IPv6 protocol. You can upgrade an earlier version of Tivoli Storage Productivity Center for use on a machine that supports both IPv4 and IPv6 (dual stack). You cannot upgrade an earlier version of Tivoli Storage Productivity Center for use on a machine that is IPv6 only. If you want to use Tivoli Storage Productivity Center on an IPv6-only machine, you must perform a new install of the product on that machine.

See the Tivoli Storage Productivity Center Information Center for more information about how to install and upgrade the product. Click **Tivoli Storage Productivity Center > Installing** and **Upgrading**.

#### Using IPv6 addresses in the user interface

Support for IPv6 enables you to enter IPv6 addresses anywhere in the installation process and user interface that supports the entering of IP addresses. For example, you can enter and display 128-bit IP address spaces on the following panels in the user interface:

#### Logon panel

Enter the host name (or IPv6 address) and port number of an Tivoli Storage Productivity Center server to which you want to connect. See the Logon panel for more information about logging in to Tivoli Storage Productivity Center and using an IPv6 address for the server name.

#### Administrative Services > Data Sources > CIMOM agents

Specify IPv4 or IPv6 addresses for the CIMOMs that are located on an IPv6 or dual stack machine.

#### Administrative Services > Discovery > CIMOM Discovery

Specify IPv6 addresses when you run a discovery with SLP DA running on an IPv6-only or dual stack machine.

#### Administrative Services > Data Sources > Out of Band Fabric Agents

Specify IPv6 addresses for the Out of Band Fabric agents that are located on an IPv6 or dual stack machine.

## Administrative Services > Data Sources > Tivoli Storage Productivity Center Servers

Specify the names or IPv6 addresses of other Tivoli Storage Productivity Center servers that you want to add as subordinate servers for rollup probes and reports.

#### Administrative Services > Discovery > Out of Band Fabric Discovery

Specify a range of IPv6 addresses for an SNMP discovery on an IPv6-only or dual stack machine against IPv6-enabled target machines.

#### Administrative Services > Configuration > Alert Disposition

If the Tivoli Storage Productivity Center servers are running on an IPv6-only or dual stack machine enter the following information:

- Specify an IPv6 address for the target machine of SNMP traps that are generated as a result of triggered alerts.
- Specify an IPv6 address for a mail server that will receive emails notifications that are generated as a result of triggered alerts.

#### IBM Tivoli Storage Productivity Center > Configuration Utility > Element Manager tab

Use an IPv4 or IPv6 address when you specify the URL for an external tool that you want to start from Tivoli Storage Productivity Center.

#### IPv6 considerations in IBM Tivoli Storage Productivity Center

IBM Tivoli Storage Productivity Center provides limited support of some functions when using IPv6 communication.

Keep in mind the following considerations when installing the product on machines configured for IPv6 only:

## Using DB2 Database V9.1 Fix Pack 2 or later for the Linux and UNIX database repository

If you install Tivoli Storage Productivity Center or its database repository on an IPv6-only computer, you must use *DB2 Database for Linux, UNIX, and Windows V9.1 Fix Pack 2 or later* for the database repository. See the Tivoli Storage Productivity Center Information Center for information on how to install and configure DB2 to use the IPv6 protocol. You cannot configure a computer that is running Windows 2003 Server Enterprise Edition for IPv6-only.

#### Using the AIX operating system

For IPv6 support, you must install level TL 5300–06.

#### Starting the Tivoli Storage Productivity Center user interface using Java Web

- **Start** You cannot use Java Web Start to start the Tivoli Storage Productivity Center user interface on a Windows system if both of the following conditions are true:
  - An IPv6 address or a hostname that resolves to an IPv6 address is specified as the target host in the Java Web Start URL.
  - Java Runtime Environment (JRE) is installed on the same system as the Tivoli Storage Productivity Center user interface.

#### Using the Brocade API when adding an out of band fabric agent

You cannot use the advanced Brocade API functions with switches because it does not support IPv6. Use a CIM agent for managing a switch or enable the IPv4 protocol on the switch. On an IPv6-only machine, the **Enable Advanced Brocade Discovery** check box on the panel is disabled.

## Using IPv6 communication between master and subordinate servers (for Rollup reporting)

If the master server is located on an IPv6-only computer, it can communicate with existing subordinate servers under the following conditions: the subordinate servers are upgraded to Tivoli Storage Productivity Center v3.3.2 or higher and the IPv6 protocol is enabled on the computers where they are located.

#### Defining Tivoli Enterprise Console events as triggered actions

You cannot use Tivoli Enterprise Console (TEC) events as triggered actions when defining alerts for Tivoli Storage Productivity Center jobs.

#### Selecting files for archive and backup

You cannot select files for Tivoli Storage Manager archive and delete jobs. For example, you cannot use the alerting function of a constraint to automatically invoke a Tivoli Storage Manager archive or backup job to run against the files that violate that constraint.

## Using Data agents and Fabric agents to collect information about the storage in your environment

Data and Fabric agents cannot communicate with Data and Device servers that have been enabled for IPv6 and are installed on IPv6-only machines. However, Data and Fabric agents that are located on IPv4 machines can communicate with Data and Device servers that are installed on machines that have both IPv4 and IPv6 stacks (dual stack) enabled.

Because of this limitation, the following functions are not available in an IPv6-only environment:

- The Agent Manager is disabled under IPv6 communication. Agent Manager and agent communication can use IPv4 only. The Agent Manager is a network service that provides authentication and authorization. It also processes queries about its registry of configuration information about the agents and management applications, and provides an agent recovery service which is a network service for error logging for agents that cannot communicate with other Agent Manager services.
- You cannot use Data Manager for Chargeback to charge for storage information. The agents that collect charge back information do not communicate over IPv6.
- You cannot use Data Manager for Databases to monitor relational databases. The agents that collect relational database information do not communicate over IPv6.
- You cannot monitor NetWare and NetApp devices. The agents that collect information about these devices do not communicate over IPv6.
- You cannot monitor VMware ESX servers and Virtual Centers (hypervisors) because they are not IPv6 enabled.
- You cannot monitor HACMP and MSCS clusters.

In IPv6-only environments, Tivoli Storage Productivity Center will gather data about devices managed by:

- SMI-S CIM (Common Information Model ) agents (for example, Brocade CIM agents, DS8000 CIM agents, SAN Volume Controller CIM agents v4.3.0.x)
- Out of Band Fabric SNMP agents
- SLP (Service Location Protocol ) directory agents
- IPv6-enabled Tivoli Storage Productivity Center servers for rollup probes and reporting

**Note:** These management components must be IPv6 enabled to communicate with Tivoli Storage Productivity Center using the IPv6 protocol.

#### Installing Tivoli Storage Productivity Center

You can install Tivoli Storage Productivity Center on both IPv6 and IPv4 machines.

- You can enter IP addresses of machines in IPv6 format. The preferred IPv6 address representation is written as eight groups of four hexadecimal digits: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx;xxxx, where each x is a hexadecimal digit representing 4 bits. For example: 2001:DB8:0000:1234:0000:0000:5678:ABCD. You can also specify IPv6 addresses using shortened formats that omit leading zeros: 2001:DB8:01:234:00:5678:ABCD or use double colons: 2001:DB8:0000:1234::5678:ABCD in place of a series of zeros. Only one "::" is allowed per IPv6 address. You can use IPv6 addresses if the machine where Tivoli Storage Productivity Center is installed is IPv6 or dual stack (IPv4 and IPv6) enabled.
- If IPv4 is not available, the check boxes for **Register with Agent Manager** and **Agents** are not enabled on the **Select the type of installation you want to run** panel.
- The installation program will use IPv4 protocol for agent installation and communication. You cannot install agents and Agent Manager on an IPv6-only machine.
- The installation program uses IPv6 protocol for configuration and communication tasks that are related to the Device server, Data server, GUI, and CLI on IPv6-only machines.
- The installation program uses IPv4 protocol for configuration and communication tasks that are related to the Device server, Data server, GUI, and CLI on systems that are enabled for these systems:
  - Both IPv4 and IPv6 (dual stack)
  - IPv4-only systems
- You must upgrade to Tivoli Storage Productivity Center v3.3.2 or later if you want to enable the product to use the IPv6 protocol. You can upgrade an earlier version of Tivoli Storage Productivity Center for use on a machine that supports both IPv4 and IPv6 (dual stack). You cannot upgrade an earlier version of Tivoli Storage Productivity Center for use on a machine that is IPv6 only. If you want to use Tivoli Storage Productivity Center on an IPv6-only machine, you must perform a new install of the product on that machine.

#### Gathering data from IBM XIV Storage System

XIV Storage System does not support IPv6.

### Installation scenarios for Tivoli Storage Productivity Center

You can install IBM Tivoli Storage Productivity Center on computers configured for IPv4, IPv6, or dual stack protocol. Depending on the protocol enabled on the target computer, you can perform different tasks during and after the installation of the product.

#### IPv6-only installation scenario

These scenarios illustrate some of the general steps you might perform when installing the product on computers with different protocols.

In this scenario, install Tivoli Storage Productivity Center on a computer configured for IPv6-only. Agent Manager, Data agents, and Fabric agents are disabled because they do not communicate over IPv6. See IPv6 considerations in Tivoli Storage Productivity Center for information about what functions are not available when installing the product on a computer configured for IPv6-only.

- 1. Use either of the following methods when installing Tivoli Storage Productivity Center components:
  - **Method 1:** Install the graphical user interface (GUI), CLI, Data server, Device server, and database repository components on a local, IPv6-only configured computer.
  - **Method 2:** Install the database repository on a remote IPv6-only computer, and the GUI, CLI, Data server, and Device server on a local, IPv6-only computer.

If you want to connect to a remote database repository using the IPv6 protocol, you must use DB2 Database V9.1 Fix Pack 2 or later for the database repository.

- 2. Run the user interface from an IPv6-only or dual stack configured computer. You cannot run the user interface from a computer configured for IPv4-only.
- **3.** Configure communication to other Tivoli Storage Productivity Center servers (for rollup probes and reporting), SMI-S CIM agents, out-of-band Fabric agents, and storage devices operating in IPv6 or dual stack mode. You cannot configure communication from Tivoli Storage Productivity Center that is installed on an IPv6-only system to storage entities on IPv4-only systems.
- 4. Launch element managers on IPv6-only computers from the Topology viewer, the Configuration Utility, and other points in the Tivoli Storage Productivity Center GUI.

#### IPv6 and IPv4 (dual stack) installation scenario

In this scenario, install Tivoli Storage Productivity Center on a computer where both IPv4 and IPv6 are configured:

- 1. Use any of the following methods when installing Tivoli Storage Productivity Center components:
  - **Method 1:** Install the GUI, CLI, Data server, Device server, and database repository components on a local, dual stack computer.
  - **Method 2:** Install the database repository on a remote IPv4-only computer, and the GUI, CLI, Data server, and Device server on a local, dual stack computer.
  - **Method 3:** Install the database repository on a remote IPv6-only computer, and the GUI, CLI, Data server, and Device server on a local, dual stack computer. You must use the *DB2 Database V9.1 Fix Pack 2 or later for the Linux or UNIX* for the database repository. This database is IPv6 enabled and is used for the database repository.

- 2. Register with the Agent Manager running on a computer in IPv4 or dual stack mode.
- **3**. Install Data and Fabric agents remotely on computers that are running IPv4 or dual stack mode.
- 4. Run the user interface from an IPv4-only, IPv6-only, or dual stack computer.
- 5. Configure communication to other Tivoli Storage Productivity Center servers (for rollup probes and reporting), SMI-S CIM agents, out-of-band Fabric agents, and storage devices operating in IPv4, IPv6, or dual stack modes.
- 6. Start element managers on IPv6-only, IPv4-only, and dual stack computers from the Topology viewer, the Configuration Utility, and other points in the Tivoli Storage Productivity Center GUI.

## Planning for LDAP support

This section provides information about planning for LDAP support.

The Lightweight Directory Access Protocol (LDAP) is an application protocol for querying and modifying directory services running over TCP/IP. A directory is a set of objects with similar attributes organized in a logical and hierarchical manner. An LDAP directory tree often reflects various political, geographic, and organizational boundaries, depending on the model chosen. The directory might contain entries representing people, organizational units, printers, documents, groups of people, or anything else that represents a given tree entry (or multiple entries).

If you want to install IBM Tivoli Storage Productivity Center so that it uses an LDAP-compliant directory for user authentication and group authorization, then you need to know the following information regarding your directory configuration:

- What is the fully-qualified domain name of the system that is running your LDAP-compliant directory?
- What network port does your LDAP-compliant directory listen to for communications?
- Does your LDAP-compliant directory allow for anonymous binding when performing user and group searches? If the answer to this question is no, then what are the Bind Distinguished Name and Password for your LDAP-compliant directory?

**Note:** If you want the ability to create or modify LDAP users and groups from the IBM Tivoli Integrated Portal administrative panel, then the Bind Distinguished Name and Password are required.

- What is the Relative Distinguished Name for the IBM Tivoli Storage Productivity Center users in your LDAP-compliant directory? All IBM Tivoli Storage Productivity Center users must have the same Relative Distinguished Name (all IBM Tivoli Storage Productivity Center users must be in the same branch of the LDAP directory tree).
- What is the Relative Distinguished Name for the IBM Tivoli Storage Productivity Center groups in your LDAP-compliant directory? All IBM Tivoli Storage Productivity Center groups must have the same Relative Distinguished Name (all IBM Tivoli Storage Productivity Center groups must be in the same branch of the LDAP directory tree. IBM Tivoli Storage Productivity Center groups do not have to be in the same branch of the LDAP directory tree as the IBM Tivoli Storage Productivity Center users.

- What is the Naming Attribute for the IBM Tivoli Storage Productivity Center users in your LDAP-compliant directory? All IBM Tivoli Storage Productivity Center users must use the same naming attribute.
- What is the Naming Attribute for the IBM Tivoli Storage Productivity Center groups in your LDAP-compliant directory? All IBM Tivoli Storage Productivity Center groups must use the same naming attribute

If you want to install IBM Tivoli Storage Productivity Center so that it uses an LDAP-compliant directory for user authentication and group authorization, then you need to be aware of the following restrictions:

- If you want to install IBM Tivoli Storage Productivity Center on a Windows platform and have IBM Tivoli Storage Productivity Center authenticate its users against an LDAP-based repository, then the LDAP TPC Administrator username value must *not* contain a space in it. This is because of WebSphere Application Server APAR PK77578. The WASService.exe fails when the WAS Admin ID contains a space or blank character; stopserver.bat does not stop the server1 service.
- If you want to install IBM Tivoli Storage Productivity Center so that it authenticates its users against an LDAP-based repository, you must first ensure that *all* of the LDAP attributes (for example, uid, cn, ou, o, and c) are configured to be case-insensitive within the LDAP-based repository. These attributes are used in the user and group Distinguished Names or as the user or group naming attribute.

## Planning for the single sign-on feature

*Single sign-on* is an authentication process that enables you to enter one user ID and password to access multiple applications. For example, you can access IBM Tivoli Integrated Portal and then access Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication from Tivoli Integrated Portal using a single user ID and password. Single sign-on integrates with the launch in context feature to enable you to move smoothly from one application to a functionally-related location in a second application.

### How single sign-on works

A single sign-on environment requires a centralized authentication repository that is accessed by all applications within the environment. The user's ID and other authentication information are passed between applications using Lightweight Third-Party Authentication (LTPA) tokens. LTPA is the security technology that is used in the IBM WebSphere Application Server for passing the user authentication information between applications. To use the LTPA tokens, each application must have the same set of public keys to encrypt the user's information. The authenticating service uses the corresponding private keys to decrypt the user's information for authentication. As an additional security mechanism, LTPA tokens expire after a determined amount of time. By default, the tokens expire after twenty-four hours. You can change the LTPA token expiration time using the Tivoli Integrated Portal user interface.

Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication use their respective IBM WebSphere Application Server instances to authenticate LTPA tokens. However, other applications, such as the IBM System Storage DS8000 element manager and other element managers that do not run within an IBM WebSphere Application Server instance use the authentication service that is provided with Tivoli Integrated Portal. The authentication service client is typically embedded in these other applications and the client communicates with the authentication service server in Tivoli Integrated Portal for all authentication requests.

#### Use of LTPA tokens with single sign-on

Tivoli Storage Productivity Center uses Lightweight Third Party Authentication (LTPA) tokens, which were developed by IBM's WebSphere and Lotus organizations, for passing the user information between applications. To use LTPA tokens for single sign-on, each participating application must possess the same set of keys to encode and decode the user information contained in the token. As an additional security feature, the LTPA tokens expire after 24 hours by default (you can change the expiration time using the Tivoli Integrated Portal graphical user interface (GUI). After the LTPA token expires, the user ID and password information must be re-entered to continue accessing the participating applications.

Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication use their respective IBM WebSphere Application Server instances to authenticate LTPA tokens. However, other applications, such as the IBM System Storage DS8000 element manager and other element managers that do not run within an IBM WebSphere Application Server instance use the authentication service that is provided with Tivoli Integrated Portal. The authentication service client is typically embedded in these other applications and the client communicates with the authentication service server in Tivoli Integrated Portal for all authentication requests.

## Selecting the user authentication method to use with single sign-on

During the installation of Tivoli Storage Productivity Center, you can specify whether to use LDAP or the operating system as the authentication and authorization repository (see the following description of each authentication type). If you do not specify LDAP, then Tivoli Storage Productivity Center uses the operating system (OS) users and groups on the server whereTivoli Storage Productivity Center is installed for authentication and authorization.

#### **OS** Authentication

This method authenticates the user against the users defined for the local operating system (OS).

#### LDAP/Active Directory

This method authenticates the user against a Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory repository.

If OS authentication is selected, the use of the single sign-on feature is limited. OS authentication does not support single sign-on for element managers, even when the element manager is installed on the same computer as Tivoli Storage Productivity Center. LDAP or Microsoft Active Directory authentication supports single sign-on for element managers regardless of where they are installed.

You can change the user authentication method using the Tivoli Integrated Portal GUI.

During installation, you can specify that Tivoli Storage Productivity Center use an existing Tivoli Integrated Portal instance rather than the instance that is installed with Tivoli Storage Productivity Center. In this case, Tivoli Storage Productivity Center uses the authentication repository that is used by Tivoli Integrated Portal (LDAP or the operating system). However, if the existing Tivoli Integrated Portal

instance uses a file-based authentication repository, you cannot use the existing Tivoli Integrated Portal instance. You must install a new Tivoli Integrated Portal instance when you install Tivoli Storage Productivity Center.

#### Additional considerations

- If you install Tivoli Storage Productivity Center so that users are authenticated against an LDAP-based repository, you must first ensure that all of the LDAP attributes (for example, uid, cn, ou, o, and c) used in the user and group distinguished names or as the user or group naming attribute, are configured to be case-insensitive within the LDAP-based repository. For example, in IBM Tivoli Directory Server version 6, you can adjust the attribute case-sensitivity through the Equality Matching Rule for each attribute. By default, the Equality Matching Rule for most attributes in IBM Tivoli Directory Server is "caseIgnoreMatch." Both of these settings are usable for integration with Tivoli Storage Productivity Center.
- The single sign-on feature is not available for the IBM XIV Storage System element manager, XIV Storage Manager.
- The single sign-on feature is not supported by the Tivoli Storage Productivity Center command-line interface (CLI).

#### **Related concepts**

"Changing the user authentication method" on page 402

The IBM Tivoli Storage Productivity Center installation program enables you to select a user authentication method that is used by Tivoli Storage Productivity Center, IBM Tivoli Storage Productivity Center for Replication, and IBM Tivoli Integrated Portal. You can choose to authenticate users against the users defined for the local operating system or to authenticate users against the users defined in a Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory repository. You can change the user authentication method after installation using Tivoli Integrated Portal.

#### **Related tasks**

"Changing the LTPA token expiration for single-sign on" on page 410 A single sign-on environment requires a centralized authentication repository that is accessed by all applications within the environment. The user's authentication information is passed between applications using Lightweight Third-Party Authentication (LTPA) tokens. You can change the expiration time for the LTPA tokens using IBM Tivoli Integrated Portal.

# Planning for IBM Tivoli Storage Productivity Center for Replication

IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication, previously separated products, are now integrated. You will be able to launch IBM Tivoli Storage Productivity Center for Replication from the IBM Tivoli Storage Productivity Center user interface.

#### Integration highlights

This integration enables you to:

- Start the IBM Tivoli Storage Productivity Center for Replication GUI from within the IBM Tivoli Storage Productivity Center GUI.
- Use the IBM Tivoli Storage Productivity Center GUI to set up IBM Tivoli Storage Productivity Center for Replication SNMP alerts and Tivoli Enterprise Console events.
• Provide a IBM Tivoli Storage Productivity Center super user role that has authority over all IBM Tivoli Storage Productivity Center commands. IBM Tivoli Storage Productivity Center for Replication has a replication administrator role that has authority to all IBM Tivoli Storage Productivity Center for Replication commands. IBM Tivoli Storage Productivity Center for Replication will honor the IBM Tivoli Storage Productivity Center super user role giving the super user role authority over all IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication commands.

For more information about IBM Tivoli Storage Productivity Center for Replication, see http://publib.boulder.ibm.com/infocenter/tivihelp/v4r1/index.jsp. Click **Tivoli Storage Productivity Center for Replication > Getting started > Concepts**.

### Alerts

IBM Tivoli Storage Productivity Center will display the alerts issued by IBM Tivoli Storage Productivity Center for Replication SNMP traps for replication events. The SNMP traps displayed are:

- · Session state change
- Path state change
- Configuration change
- Suspending-event notification
- Communication failure
- Management Server state change

### **User interface**

There is a new node added to the navigation tree for IBM Tivoli Storage Productivity Center for Replication: **Replication Manager**. Subnodes under this major node will be **Alerting** and **Replication Management**.

From the **Replication Management** node, you will be able to manage and view information aboutIBM Tivoli Storage Productivity Center for Replication:

- Health overview
- Session
- Path Manager
- Storage subsystems
- Management servers

A **Replication Manager** tab has also been added to the Configuration Utility that provides the same information.

From the Alerting node, you will be able to manage alerts for IBM Tivoli Storage Productivity Center for Replication.

### **Disaster recovery**

When you install IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication, you can specify to use LDAP authentication or OS authentication.

When planning for disaster recovery, the IBM Tivoli Storage Productivity Center for Replication server must be accessible in the event of a disaster. Even if there is a IBM Tivoli Storage Productivity Center for Replication standby server for recovery purposes, the server still requires authentication. If you use LDAP authentication, the LDAP services must be available in the event of a disaster. You can set up the LDAP environment so that you have clustered servers for this purpose.

## Planning for enterprise-rollup reports

This topic provides information about planning for enterprise-rollup reports.

IBM Tivoli Storage Productivity Center now enables you to use a single interface to generate reports based on data collected by multiple Tivoli Storage Productivity Center servers. You will be able to perform the following:

• View the storage information that is gathered by other servers from a single Tivoli Storage Productivity Center user interface using new enterprise-wide rollup reports. These rollup reports enable you to have a network-wide perspective of storage usage in an environment where multiple Tivoli Storage Productivity Center servers are deployed and collecting storage metrics.

Note: Performance-related reports are not rolled up.

• Partition a large number of agents across multiple Data servers. This will alleviate performance issues when running aggregation reports and scan jobs for multiple agents on one Data server.

To enable rollup reporting, you must select one Tivoli Storage Productivity Center server to act as the "master" server that gathers enterprise-wide data for reports. You can then associate other Tivoli Storage Productivity Center servers to that master server as "subordinate" servers. These subordinate servers provide data to the master server about the entities they manage.

It is possible set up a rollup-reporting environment where fragmentation occurs. Fragmentation occurs when related entities are being monitored by different subordinate Tivoli Storage Productivity Center servers. For more information, see *IBM Tivoli Storage Productivity Center User's Guide*.

**Note:** Keep in mind the following information when working with master and subordinate servers:

- The master and subordinate servers can change over time.
- A master server can also manage entities just like any other server and report on these entities.
- Subordinate servers should not have more than 1200 unique data sources. This includes Data agents, Fabric agents (in-band and out-of-band), CIM agents, and VM agents.
- You must have Tivoli Storage Productivity Center superuser or Tivoli Storage Productivity Center administrator authority to perform administrative operations such as adding a subordinate server to the master server list to monitor.
- When you add a subordinate server to the master server list, you must provide the host authentication password of the subordinate server to the master server. The host authentication password is checked each time the master server is probed. This host authentication password is entered when installing Tivoli Storage Productivity Center. Contact your system administrator or the person who installed Tivoli Storage Productivity Center to determine this password.

### Planning for enterprise-rollup reports configuration

This topic provides information about planning for enterprise-rollup reports configuration.

Follow these general steps to get enterprise-wide rollup reports:

- 1. Run discoveries, probes, and scans on the master server to gather information about locally managed entities.
- Register the subordinate server with the master server. Click on Administrative Services > Data Sources > IBM Tivoli Storage Productivity Center Servers. Click Add Tivoli Storage Productivity Center Server. Enter information for the subordinate server including the host authentication password. The host authentication password is checked each time the master server is probed.
- **3**. Run discoveries, probes, and scans on the subordinate servers to gather information about their locally managed entities.
- 4. Define and run Tivoli Storage Productivity Center server probes from the master server to collect storage information that has been gathered by subordinate servers.
- View the information gathered by the Tivoli Storage Productivity Center server probes in rollup reports under Tivoli Storage Productivity Center > Rollup Reports.

## Planning for the SAN configuration tools

This topic provides information on planning for the SAN configuration tools.

System administrators can identify potential problems with storage area network (SAN) configurations by using the Configuration Analysis and Configuration History tools.

#### **Configuration Analysis**

This tool allows the system administrators to check whether existing configurations violate defined best practices and policies. The user selects a set of best practices (policies) and specifies the name of a target SAN (or zone set) through the GUI, and then the tool checks to see whether the selected best practices are being violated in the specified SAN. The policy violations are displayed as IBM Tivoli Storage Productivity Center alerts. The topology viewer will display these policy violations and the affected SAN entities involved in each violation.

#### **Configuration History**

This tool displays the changes that have occurred in the SAN environment over a period of time. Using this tool, the user can periodically or on-demand take snapshots of the SAN configuration managed by Tivoli Storage Productivity Center. Using the configuration history viewer, which is a slight variation of the topology viewer, the user can select any two snapshots and view the changes (whether the SAN entities were added, removed, or modified) that have occurred in the SAN environment between those two time periods when snapshots were taken.

To create and schedule jobs using these tools, you must have Tivoli Storage Productivity Center superuser or Tivoli Storage Productivity Center administrator authority.

You must have the IBM Tivoli Storage Productivity Center Standard Edition license to use these tools.

### **Planning for Configuration Analysis**

This topic provides information on planning for the Configuration Analysis tool.

When you set up the Configuration Analysis tool for policy checking, you define the scope to perform the checking:

- All Fabrics
- One Fabric
- One Zoneset

The Configuration Analysis tool can check for these policies (the policies supported depend on the scope you select). For more information on each policy and how to use the Configuration Analysis tool, see *IBM Tivoli Storage Productivity Center User's Guide*.

Zone and fabric related requirements:

- Each connected computer and storage subsystem port must be in at least one zone in the specified zone set.
- Each host bus adapter (HBA) accesses storage subsystem ports or tape ports, but not both.
- Each volume can be accessed only by computers running the same type and version of operating system.
- Each zone must contain only HBAs from a single vendor.
- Each zone must contain only a single model of storage subsystem.
- Each zone is part of a zone set.
- Each host must be zoned so that it can access all of its assigned volumes.
- Each fabric can have up to (x) zones.
- Each zone can have up to (x) zone members.

Model, firmware, and software requirements:

- Each computer has only HBAs of the same model and firmware version.
- For each host type and operating system, every HBA of a given model must have the same firmware version.
- Every SAN switch of a given model must have the same firmware version.
- Do not manage the same SAN Volume Controller cluster with SAN Volume Controller CIM agents of different release versions. For example, if you have a cluster named "Einstein" you can manage Einstein with two SAN Volume Controller CIM agents on 4.2.0, or with two SAN Volume Controller CIM agents on 4.3.1. Do not attempt to manage Einstein or any other SAN Volume Controller cluster with one SAN Volume Controller CIM agent on 4.2.0 and the other SAN Volume Controller CIM agent on 4.3.1.

For SAN Volume Controller 4.3.1, the CIM agent is embedded in the hardware.

• Every storage subsystem of a given model must have the same firmware version.

To use the Configuration Analysis tool, follow these general steps:

- 1. You must have run discovery and probe jobs for the computers, fabrics, switches, storage, and other objects you want information about.
- 2. Make sure that the Device server and Data server are up and running.
- **3**. Go to **Tivoli Storage Productivity Center > Analytics > Configuration Analysis** and specify the scope that the policies apply to. Also select the policies to check.
- 4. Click the button to run the validation checking just once. Or, you can schedule the job to run at specific time intervals.

5. After the configuration analysis job has run, you can use the alert overlay within the topology viewer to see the detailed information for policy violations encountered during that job run.

### Planning for the Configuration History tool

This topic provides information on planning for the Configuration History tool.

The Configuration History view is a variation of the topology viewer. The Configuration History view shows the current configuration as well as what the configuration looked like in the past. Use the snapshot selection panel in the Configuration History page to view changes that occurred in your storage environment between two or more points in time. After you define the configuration history settings, the system takes snapshots of your configuration so that you can compare the configuration at different points in time. The comparison can help you analyze system performance, as well as enhance the quality of provisioning and planning tasks. The Configuration History tool does *not* show the *current* configuration.

To use the Configuration History tool, follow these general steps:

- 1. You must have run discovery and probe jobs for the computers, fabrics, switches, storage, and other objects of interest. For computers, you must also have run scan jobs.
- 2. Make sure that the Device server and Data Server are up and running.
- **3**. In the GUI, go to **Administrative Services** > **Configuration** > **Configuration History Settings**. Enable the periodic scheduling of configuration history snapshot creation or create some on-demand configuration history snapshots.
- 4. In the GUI, go to **IBM Tivoli Storage Productivity Center > Analytics > Configuration History** for the following:
  - Computers
  - Fabrics
  - Switches
  - Storage
  - Other

A Configuration History topology view is displayed of the item you selected.

- 5. Select the time range for the snapshots and click **Apply**.
- 6. You will be able to view the SAN configuration changes in the configuration history view for the two time periods you selected.

For more information about how to use this tool, see *IBM Tivoli Storage Productivity Center User's Guide*.

## Planning for the SAN planning tools

This topic provides information on planning for the SAN planning tools.

The SAN planning tools consist of the following:

#### Volume Planner

The Volume Planner helps administrators plan for the provisioning of subsystem storage based on capacity, storage controller type, number of volumes, volume size, performance requirements, RAID level, performance utilization, and capacity utilization. The Volume Planner generates a plan that presents the storage controllers and storage pools that can satisfy the request. If the user explicitly specifies the storage pool and controller information, then the Volume Planner checks to see whether the input performance and capacity requirements can be satisfied. For provisioning of storage, you must use all three planners together (Volume Planner, Path Planner, and Zone Planner).

The Volume Planner was formerly known as the Volume Performance Advisor. This support is being enhanced as follows:

- Support is being added for DS8000 and DS6000 controllers. Formerly, support was only available for the Tivoli Storage Enterprise Storage Server800. You will be able to consider a combination of the supported storage controllers when performing planning operations to find suitable storage space.
- Support is being added to support new policies. The current policies supported are:
  - Use of unassigned volumes
  - Performance profile
  - Volume number and size range

The following additional policies will be supported:

- Controller type preference
- Whether the storage request can be satisfied by multiple controller types
- RAID level

#### Path Planner

The Path Planner enables system administrators to plan and implement storage provisioning for hosts and storage subsystems with multipath support in fabrics managed by IBM Tivoli Storage Productivity Center. Planning the provisioning of storage to hosts with multipath drivers requires knowing which storage subsystems are supported by the host multipath driver and the supported multipath nodes that are both the driver and storage subsystem support. Planning the paths between the hosts and storage controller requires designing paths between hosts and storage subsystems that are implemented through zones in the fabric. For storage provisioning, you must use all three planners together (Volume Planner, Path Planner, and Zone Planner).

Multipath information is collected by the Data agent installed on all managed hosts.

Multipath aware storage provisioning adds the ability to adjust multipath settings to the standard Tivoli Storage Productivity Center storage provisioning process, enabling the checking, tuning and optimizing of multipath settings during the storage provisioning process. This aids the administrator by assisting in the multipath tuning process through the selection of these policies:

- Using the multipath setting determines whether the Path Planner will specify multiple paths between the hosts and the storage subsystem. This setting will require each host to have at least two fibre channel ports connected to the SAN.
- Using the preferred number of paths setting specifies the number of paths the user would like between each host and the storage subsystem.
- Using the multipath mode setting determines the host multipath driver option, which specifies how the driver uses the paths between the host and the storage subsystem. (For example, load balancing mode, failover mode, and so forth.)

• Using the redundant fabric setting specifies if the Path Planner will check for redundant fabrics between each host and storage subsystem, and create paths in each fabric.

Besides policies and application profiles, the Path Planner also checks the following:

- Multipath driver storage subsystem interoperability matrix
- Multipath driver load balancing types and mode settings
- · Operating systems supported by the storage subsystem

#### Zone Planner

The Zone Planner enables the administrator to plan for zoning and LUN masking configuration based on the following information: host ports, storage controller ports, zones, zone sets, switches, user zoning input, user LUN masking input, existing LUN masking or mapping. If the user specifies the exact zoning and LUN masking information, then the Zone Planner informs the user whether the user input is different from the selected input or the existing configuration.

To use the SAN planning tools, you must have Tivoli Storage Productivity Center superuser or Tivoli Storage Productivity Center administrative authority.

These are the general steps to follow to use the SAN planning tools:

- Make sure you have the IBM Subsystem Device Driver installed. If not, install it. SDD is required to get multipath information. For Windows, you need to use IBM Subsystem Device Driver version 1.5.1 or later. For information about SDD, go to this Web site: http://www-1.ibm.com/support/dlsearch.wss?rs=540 &tc=ST52G7&dc=D430.
- 2. Install and configure the SMI-S agents (CIM agents) for the subsystems and fabric to collect subsystem and fabric data. Contact your vendor for information on installing and configuring the CIM agent for the subsystem or fabric.
- 3. Install the Data agent on the systems you wish to find information about.
- 4. Run a discovery job for the CIM agents and Data agents.
- 5. Run a probe job for the subsystem, fabric, and Data agents.
- 6. Run a scan job for the Data agents.
- 7. Run a performance monitoring job for the subsystem.
- 8. You will now be able to use the SAN planning tools to help you plan for system configuration.

# Planning for the Storage Optimizer

The Storage Optimizer uses data in the IBM Tivoli Storage Productivity Center database to analyze your storage subsystems to identify performance bottlenecks, and recommend changes to improve performance. The Storage Optimizer helps you develop storage migration or storage consolidation plans, and helps you plan for the growth of your storage infrastructure.

**Note:** The Storage Optimizer does not actually perform any migrations or make any modifications to subsystem configurations. Its primary purpose is to provide you with a performance analysis and optimization recommendations that you can choose to implement at your discretion.

**Important:** Storage Optimizer does not take into account any established replication relationships or sessions. Migration recommendations should be followed with care to ensure continuity of all replication relationships.

To use the Storage Optimizer, you must have a IBM Tivoli Storage Productivity Center Standard Edition license.

The following IBM storage subsystems or applications are supported:

- DS8000
- DS6000
- DS4000
- Tivoli Storage Enterprise Storage Server
- SAN Volume Controller

**Note:** Non-IBM subsystems, including SAN Volume Controllers that use non-IBM back-end subsystems, are not supported by Storage Optimizer. Solid state drives (SSDs) are not supported at this time. Subsystems that contain solid state drives may produce unexpected results in the Storage Optimizer heat maps. Storage Optimizer analysis of subsystems containing solid state drives should be avoided until support is available.

Before running Storage Optimizer, you must set up performance monitors and collect performance monitoring data for all storage subsystems that you want Storage Optimizer to analyze. You must also collect performance monitoring data for a SAN Volume Controller's back-end subsystems in order to produce the most accurate Storage Optimizer analysis.

Storage Optimizer analyzes performance monitoring data for the time interval you specify. The analysis will be less accurate if there are any gaps in the data collection for the time interval being analyzed. It is recommended that you collect at least one week's worth of performance monitoring data before using Storage Optimizer. Providing a longer time interval for data collection will increase the accuracy of the Storage Optimizer analysis and recommendations. To create a subsystem performance monitor job, navigate to **Disk Manager > Monitoring > Subsystem Performance Monitors**. Right-click **Subsystem Performance Monitors** and choose **Create Subsystem Performance Monitor**.

You must provide the Storage Optimizer with the following input:

- Subsystem performance monitoring data that you collect for the supported storage subsystems before running the Storage Optimizer
- One or more selected storage subsystems or pools that you specify as input to the Storage Optimizer.
- Connected fabric topology and zoning information will be included in the analysis if it is available.

The Storage Optimizer provides the following output:

- An analysis report that displays performance heat maps and tables that graphically illustrate the performance utilization of the storage subsystems and pools that you specified as input.
- An optimization report that provides migration and consolidation recommendations for improving performance.

The Storage Optimizer produces more accurate results if you provide both the required and optional input data requested by the Storage Optimizer, and if you collect performance monitoring data over a longer time interval before using the Storage Optimizer.

Because running the Storage Optimizer is a processor-intensive task for the IBM Tivoli Storage Productivity Center server, schedule a time to run the Storage Optimizer when processor demand on the IBM Tivoli Storage Productivity Center server is expected to be at a minimum.

When the Storage Optimizer considers potential pools as targets of a migration, it takes into consideration whether the source and target pools have the same RAID level, format (CKD or FB), and whether or not the potential target has enough available capacity.

For more information on using the Storage Optimizer, see the *IBM Tivoli Storage Productivity Center User's Guide*.

## Planning for Data Path Explorer view

This topic provides information on planning for the Data Path Explorer view in the topology viewer.

The Data Path Explorer is a new type of view in the topology viewer. Data path explorer combines several of the usual topology views into a visualization that allows users to follow connectivity from one end point in the topology view to another. Storage administrators can use this view to debug connectivity and performance problems in the storage environment. Data Path Explorer will display the different data paths (SAN access paths or I/O paths) for each host disk. This allows you to use the Data Path Explorer to check the health and performance statistics of the storage components along the I/O path.

Different agents play different roles when discovering information and what can be shown in the topology viewer. The Data Path Explorer view is also subject to those limitations as well. Different amounts of information can be shown by the Data Path Explorer view depending on the agents deployed throughout the fabric.

To display data paths from a host to a subsystem in this view, it is necessary to have the following agents installed and configured:

- · CIM agent to monitor the storage subsystem
- Data agent to monitor the host
- In-band Fabric agent to monitor the fabric. Also a CIM agent for the fabric to collect fabric performance information.

The Data Path Explorer view will not be able to display the data path from a host to a subsystem if any one of these agents is not installed and configured.

To show the host disk assignment from a given storage subsystem, it is necessary for IBM Tivoli Storage Productivity Center Data Server to have access to the subsystem's CIM agent (SMI-S agent). In the case of the subsystem, the data path is defined by the host masking or mapping information maintained by the CIM agent.

Analysis on data paths involving SAN Volume Controllers would require one or more CIM agents pointing to the SAN Volume Controller as well as the disk drives for the storage system.

To show accurate information, it is important to have the most current information from the CIM agents, Fabric agents, and Data agents. You must probe all the components within the data path (or a set of agents strategically placed throughout the fabric). To show physical fabric connectivity, you must have an in-band Fabric agent, out-of-band Fabric agent, or a CIM agent for the fabric.

To show performance overlay in the Data Path Explorer view, you must first create and run performance monitors on the switches and storage subsystems of interest. To see the overlays you must also go to the topology viewer. Right-click on the topology viewer. Click **Global Settings**. On the Settings window under Active Overlays, click the **Performance** check box.

To show the zone overlay, you need an in-band Fabric agent connected to the fabric along the data paths defined or a CIM agent for the fabric. To see the overlays you must also go to the topology viewer. Right-click on the topology viewer. Click **Global Settings** and check the **Show zone tab** check box. Click **OK**.

If you want to launch the Data Path Explorer view for a host, that host must have a Data agent running on it.

These are the general steps to follow to display the data path explorer view:

- Install and configure the SMI-S agents (CIM agents) for the subsystems (including SAN Volume Controllers) and fabric to collect subsystem and fabric data. Contact your vendor for information on installing and configuring the CIM agent for the subsystem or fabric.
- 2. Install and configure the in-band Fabric agent, or out-of-band Fabric agent to monitor a given fabric.
- 3. Install the Data agent on the hosts.
- 4. Run a discovery job for the CIM agents and Data agents.
- 5. Run a probe job for the subsystem, fabric, and Data agents.
- **6**. Run a performance monitoring job for the subsystem and switches if you want to see performance information.
- 7. You will now be able to see the data paths from a host to a storage subsystem in the Data Path Explorer view.

## Planning for the Agent Manager

This section provides planning information for the Agent Manager.

#### Note:

- The Agent Manager is disabled for IPv6 communication. Agent Manager and agent communication use IPv4 only.
- You need the Data agent and Agent Manager installed to run IBM Tivoli Storage Productivity Center batch reports.

### Hardware requirements

This topic provides information about the hardware requirements for Agent Manager.

The Agent Manager with embedded WebSphere uses approximately 150 MB of disk space. An additional 100 MB of temporary disk space is used during the installation. On Windows systems, the temporary space must be on the C: drive, even if you are installing to a different drive.

This space estimate does not include space required for the RDBMS server software or the registry database. Consult your database software documentation for those space requirements. Use the formulas in "Estimating the size of the registry database" to determine how much hard drive space the database will require. Although you do not explicitly configure the size of the database, you must make sure that sufficient space is available. For local DB2, the database is on the Agent Manager server in an operating system-specific location.

## Software requirements

This section provides information about the software requirements for the Agent Manager.

The Agent Manager can be installed on the following operating systems:

- AIX 5.3 (32 and 64-bit kernel)
- Windows Server 2003 Standard Edition (32-bit kernel)
- Windows Server 2003 Enterprise Edition (32-bit kernel)
- Windows 2003 Datacenter Edition (32-bit kernel)
- Red Hat Enterprise Linux AS Version 3.0 for xSeries®

You can use the **Typical** installation of this product. You do not need to install the following additional functions:

- Data warehousing
- Satellite administration capability

#### Note:

- DB2 is installed on the same computer as Agent Manager.
- Do not use the Cloudscape<sup>®</sup> database when installing the Agent Manager.
- The Agent Manager can be installed on a separate computer from IBM Tivoli Storage Productivity Center.

## Common agents

This topic describes the version of Common agents supported by IBM Tivoli Storage Productivity Center.

IBM Tivoli Storage Productivity Center supports Common agents at version 1.2.x only.

If you are using an Agent Manager that is used by another product, for example Tivoli Provisioning Manager, note the information below. Tivoli Provisioning Manager supports Agent Manager 1.3 and Common agents 1.3. Tivoli Storage Productivity Center currently does not support Common agents 1.3. If you want to use the Agent Manager 1.3 provided by Tivoli Provisioning Manager, make sure that the Tivoli Storage Productivity Center servers are registered with the Agent Manager 1.3. You must use the Common agent 1.2.x that is shipped with the Tivoli Storage Productivity Center installation package. If a Common agent 1.3 installation exists on the server where Tivoli Storage Productivity Center agents are to be installed, a separate installation of a supported Common agent 1.2.x must be installed and configured so that the ports will not conflict with the pre-existing Common agent 1.3 installation.

## Estimating the size of the registry database

Before you install the Agent Manager, make sure that the computer system that hosts the registry has sufficient file system space. The guidelines in this section help you calculate the amount of space you will need for the registry. The following factors are important when estimating the size of your registry database:

- The number of agents in your deployment
- The length of time that configuration updates are saved

By default, only the most recent configuration information is saved. However, you can configure the registry to save all updates or to delete updates after a specified number of hours.

• The length of rows in the agent tables

Some rows in the registry contain variable length data. For example, one column in the row for an agent error contains the message text, which can be up to 2,000 characters but is typically shorter. The calculations below include an average row size, as determined by examining the database during testing, as well as the maximum row size. The effect of row size is greater as you retain configuration updates for a longer time.

The following table estimates the size of a registry containing information about one hundred, one thousand, and ten thousand agents. It shows the database size in megabytes (MB) for both average and maximum row sizes, and shows the impact of increasing the retention period for configuration updates from the default of keeping a single update to 7 days and 14 days. In this estimate, the registry receives four configuration updates per day. This includes one daily update plus three event-driven updates.

	Retain most recent only		Retain for 7 days		Retain for 14 days	
Number of agents	Average rows	Maximum row	Average rows	Maximum row	Average rows	Maximum row
100	55 MB	70 MB	69 MB	91 MB	86 MB	115 MB
1000	96 MB	246 MB	240 MB	455 MB	408 MB	699 MB
10000	511 MB	2009 MB	1951 MB	4102 MB	3631 MB	6543 MB

Table 17. The estimated size of a registry with varying numbers of agents, configuration update retention times, and row size

Aside from configuration update and error information, is not automatically deleted from the registry. This means that the size of your deployment increases over time. For example, the registry contains the information for all agents, even after they have been removed from service. You can delete agents that are no longer active, using tools in the Agent Manager toolkit. For more information about the toolkit, see "Agent Manager toolkit for administrators" on page 605.

Although your initial estimate typically deals with a single manager application, consider whether you will add additional system management products that use the Tivoli Common Agent Services infrastructure. This can help you select a server whose storage can scale up to handle the increased storage needed to record additional bundles and agents managed by another application.

### Security considerations

This topic provides information about security considerations for the Agent Manager.

Note the following:

authority needed to access the registry database For a DB2 registry, you must configure the Agent Manager server so that it uses the instance owner to access the registry database. The Agent Manager applications do not run correctly if you use a different DB2 user, even if that user has the same authorization privileges as the instance owner.

#### authority needed to install the Agent Manager

To install the Agent Manager, you must log in as a user with the following authority:

- On Windows systems, you must have administrator authority.
- On AIX, Linux, and Solaris systems, you must have root authority. After installing the Agent Manager, you can configure it to run as a user other than **root**.

Only the user who installs the Agent Manager has access to the directory that contains the certificates.

#### controlling access to the Agent Manager

Only registered agents and resource managers can access Agent Manager services (other than the agent recovery service). Registration requires a password, and separate passwords are used to control registration by agents and resource managers. After an agent or resource manager registers, it can access only the Agent Manager functions that are appropriate to its type (agent or resource manager).

#### controlling access by resource managers

A resource manager has access to sensitive information about your environment and has the authority to install and run programs on agent systems. Therefore, it is important to make sure that only authorized resource managers can register with the Agent Manager. The person installing a resource manager must provide a user ID and password of a user that is authorized to register the type of resource manager being installed.

The resource manager access is controlled using the Authorization.xml file in the <Agent\_Manager\_install\_dir>\config directory. This file contains a list of users that are authorized to register a resource manager, an encrypted version of the user's password, and the type of resource manager each user is authorized to register.

When the Agent Manager is installed, a single user is defined. This default user, named **manager**, has the authority to register all resource managers. The default password for the user manager is **password**. You should change the password after installing the Agent Manager. You can optionally configure more granular control, down to a separate user ID and password for each type of resource manager. See "Managing resource manager authorization" on page 424.

The registration password for a resource manager can be changed at any time. The new password takes effect as soon as the Agent Manager server is restarted. For more information about changing resource manager registration passwords, see "Changing the registration password for a resource manager" on page 483.

The Agent Manager protects resource-manager registration against attacks that attempt to find a valid password through exhaustive search, by limiting the number of unsuccessful login attempts that can be made by a user in a fixed time period. This makes it impractical for an attacker to try a large number of user ID and password combinations. You set the threshold for unsuccessful attempts to register. After a configurable number of unsuccessful attempts, the user is locked out for a configurable time period.

#### controlling access by agents

A person who installs the agent must provide the agent registration password, which is used to determine whether the agent is allowed to register. You set the agent registration password when you install the Agent Manager. After installation, you can change the password using the **EncryptAMProps** command. This command is described in "Changing the agent registration password" on page 481.

#### controlling access to keys and certificates

To make sure that the Agent Manager certificates cannot be copied or modified by unauthorized users or applications, the directory that contains the security files (<Agent\_Manager\_install\_dir>\certs) has restricted permissions. Only the user who installed the Agent Manager can access that directory.

For additional security, the following certificate authority files in the directory are locked with a password called the *certificate authority password*:

- CARootKeyRing.jks
- CARootKey.pwd
- agentManagerKeys.jks

The certificate authority password is set during the installation of the Agent Manager. You can specify a password or let the installation program generate a random password for internal use. You need to specify the value for the certificate authority password only if you need to open the truststore files to examine the certificates that they contain.

The \certs directory also contains the certificate authority truststore file (agentTrust.jks), which contains the signer certificate for the certificate authority. This file is locked with the agent registration password.

#### deploying the certificate authority truststore file

You want to be sure that the Agent Manager that accepts the registration of an agent or resource manager is authorized to do so. The agent or resource manager checks for you by comparing the certificate presented to it by the Agent Manager with a certificate from a trusted source, which is the signer certificate of the certificate authority provided by the Agent Manager. This certificate is in the agentTrust.jks truststore file in the <Agent\_Manager\_install\_dir>\certs directory on the Agent Manager server. Your role is to decide on the level of security that is required in

server. Your role is to decide on the level of security that is required in your environment, and to chose the appropriate method for providing the agent or resource manager installation program with a copy of the truststore file.

To access the truststore file on the Agent Manager server, you must be logged in as the user who installed the Agent Manager. Be sure that only authorized users can access the copy of the truststore file.

The truststore file is automatically copied to the agent and resource manager directories when you install or upgrade the agent or resource manager.

The Agent Manager provides a demonstration certificate to facilitate the rapid deployment of a test environment or demonstration environment. The demonstration certificate and its password are publicly available.

Anyone who has a demonstration certificate can participate in your deployment. Using the demonstration certificate does not provide the level of security required by a typical production environment. In a production environment, let the Agent Manager installation program generate a certificate that is unique to your Agent Manager installation.

If you choose to use the demonstration certificate, you must specify that as an option during the installation of the Agent Manager. Then, when you install each agent or resource manager, specify the demonstration certificate, which is the agentTrust.jks file in the \certs directory on the installation media.

# TCP/IP ports used by the Agent Manager

This topic describes the ports used by the Agent Manager.

The following table lists the TCP/IP ports used by the Agent Manager component. You can change any of the port numbers except for port 80, which is used by the agent recovery service.

Port	Use	Connection security
9511	<ul><li>Registering agents</li><li>Registering resource managers</li></ul>	Secure SSL
9512	<ul> <li>Providing configuration updates</li> <li>Renewing and revoking certificates</li> <li>Querying the registry for agent information</li> <li>Requesting ID resets</li> </ul>	Secure SSL with client authentication
9513	<ul> <li>Requesting updates to the certificate revocation list</li> <li>Requesting Agent Manager information</li> <li>Downloading the truststore file</li> <li>Alternate port for the agent recovery service</li> </ul>	This is a public port and is unsecure
80	Recovery service (optional)	Unsecure

Table 18. TCP/IP ports used by the Agent Manager

If there is a firewall between the Agent Manager and the common agents and resource managers in your deployment, configure your firewall for the following situations:

- Allow inbound traffic to the Common agent on the Common agent port. By default, this is port 9510.
- Allow inbound traffic to the Agent Manager on all of the Agent Manager ports. By default, this includes ports 9511, 9512, and 9513.
- Allow inbound traffic to the Agent Manager on the ports used by the agent recovery service. This is port 80 and 9513 and the configurable unsecure port of the Agent Manager, which is port 9513 by default.

If there is a firewall between the common agents and the Agent Manager server, you must allow inbound traffic on ports 80 and 9513 to the agent recovery service. Opening these ports allow common agents to report registration problems. If you

configure Agent Manager to use a port other than 9513 for the public port, open that port as well, so that common agents can report communication problems after their initial registration. Opening the backup port is especially important if you disable the Agent Manager use of port 80.

## Using version 1.2.2 Common agents

This topic provides information on running version 1.2.2 Common agents.

Agents that run Data Manager and Fabric Manager version 1.2.2 of the Common agent software can connect to and register with an Agent Manager server that is running version 1.2.2 or 1.2.3 of the Agent Manager software.

IBM Tivoli Storage Productivity Center ships Tivoli Common Agent Services version 1.2.3.

## Planning for the Data Manager

This section provides planning information for the Data Manager.

Data Manager is a comprehensive file and capacity management solution for heterogeneous storage environments. Data Manager includes enterprise-wide reporting and monitoring, policy-based management and automated capacity provisioning for Direct Attached Storage (DAS), network attached storage (NAS), and SAN environments.

Data Manager helps you improve storage utilization, plan for future capacity, and ensure availability by providing storage on demand for file systems. Use Data Manager to perform the following functions:

- Discover and monitor disks, partitions, shared directories, and servers.
- Monitor and report on capacity and utilization across platforms to help you identify trends and prevent problems.
- Provides a wide variety of standardized reports about file systems and storage infrastructure to track usage and availability.
- Provide file analysis across platforms to help you identify and reclaim space used by non-essential files.
- Provide policy-based management and automated capacity provisioning for file systems when user-defined thresholds are reached.

Using these functions, Data Manager helps you lower storage costs by:

- Improving storage utilization.
- Enabling intelligent capacity planning.
- Helping you manage more storage with the same staff.
- Supporting application availability through computer uptime reporting and application database monitoring.

Information collected by Data Manager helps you understand what is really going on with data on your servers and in your storage environment. You can view when files are created, accessed, and modified, and by what group or user. This type of information helps system administrators map storage resources to the consumers of the resource.

In addition to understanding the current consumption and usage of data within the enterprise, Data Manager tracks the information over time. Not only does this historical view of storage consumption and utilization show usage trends over time, the system administrator can also see a projected use of storage in the future. System administrators can prepare for the need to purchase additional capacity in a planned proactive manner rather than reacting to out-of-space emergencies.

Use the Data Manager policy functions to help you evaluate and control the usage and status of your enterprise storage management assets. Because Data Manager is policy-based, it has autonomic self-healing capabilities that can detect potential problems and automatically make adjustments based on the policies and actions you have established. Use the capability to provision storage based upon storage policies to expand a file system, and to allocate storage to a volume (LUN).

## Planning for the Data agents

The Data agents collect information from the machine or host they are installed on. The agents collect asset information, file and file system attributes, and any other information needed from the computer system. Data agents can also gather information on database managers installed on the server, Novell NDS tree information, and NAS device information. You can create ping, probe, and scan jobs to run against the servers that have Data agents installed. This topic provides planning information for installing the Data agents.

The Data agents are installed on all the computer systems that you want IBM Tivoli Storage Productivity Center to manage.

Data agents can only be remotely installed by running the Tivoli Storage Productivity Center agent installation program from the Tivoli Storage Productivity Center server machine. This will install both the Common agent and the Data agent.

You can remotely install Data agents using the **Add Agents from MS Directory** or **Manually Enter Agents** button or install them locally on the managed server.

## Planning for the Data agents on Solaris

You can skip automount maps (automaps) for a discovery job on Solaris. To skip automount maps, specify the **skipAutoFS=1** parameter in the server section of the TPCD.config file. The change will globally affect all Solaris Data agents managed by the same Data server.

To change the TPCD.config file, follow these steps:

- 1. Stop the Data server.
- Modify the TPCD.config file in this directory: <TPC\_Data\_Server\_home>/config

The default directories are:

Windows: C:\Program Files\IBM\TPC\data\config UNIX or Linux: /<usr or opt>/IBM/TPC/data/config

3. Modify the TPCD.config file with the **skipAutoFS=1** parameter added:

```
[server]
  threadPoolSize=3
  abbreviatedProbe=1
  maxThreads=8
  pingReceiveTimeout=10
  skipAutoFS=1 <== Set to 1 for Discovery
        on Solaris Data agent to skip AutoMounts
        process.By default, discovery will always</pre>
```

process AutoMounts on the Solaris Data agent.

```
[gui]
threadPoolSize=3
maxThreads=10
reportRowLimit=5000
keepCachedReport=120
```

Save the file.

4. Restart the Data server.

## Planning for Disk Manager configuration

This section provides information for planning Disk Manager configuration.

If you will be using a CIM agent to collect data, you need to make sure the following items are done before adding the CIM agent:

- 1. The version of CIM agent and firmware for the device is supported.
- 2. A CIM agent is installed on a different server from the IBM Tivoli Storage Productivity Center server. For some storage subsystems, the CIM agent is imbedded in the subsystem, and therefore, no separate CIM agent installation is required.
- **3**. For subsystems on a private network, be sure to have the CIM agent installed on a gateway machine so that the Tivoli Storage Productivity Center server on a different machine can communicate with the CIM agent.
- 4. The CIM agent is configured to manage the intended device.

For information about how to install and configure the CIM agent, contact your CIM agent provider.

To get Disk Manager data, you must do the following general steps:

- 1. If you are using a CIM agent to collect data, you need to do the following:
  - a. Add the CIM agent to Tivoli Storage Productivity Center.
  - b. Perform a CIMOM discovery operation for the subsystems.
- 2. Perform one or more discovery jobs. The discovery job discovers:
  - CIM agents
  - Out of Band Fabric agents
  - Netware Filers
  - Windows domain, NAS, and SAN File System
- **3**. Run a probe job for the storage subsystems and computers. A probe job collects detailed information about the configuration of the storage subsystem. A probe job needs to be run before volumes can be created on a storage subsystem or a storage subsystem can be monitored for performance management.
- 4. Run a scan job. Scan jobs are used to collect statistics on the files on the hosts where Data agents are installed. The results of the scan jobs are stored in the repository database and are used to supply the data necessary for the capacity, usage, usage violations, and backup reporting facilities.
- 5. Create alerts. Alert definitions can be created so that you will receive notification of a condition and can take the appropriate action when a certain condition occurs on a computer resource, storage device, or the fabric. Alerts can be defined by using the alerting feature of Data Manager, Disk Manager, and Fabric Manager.

If you are generating enterprise-wide reports, you will have a master Tivoli Storage Productivity Center server and one or more subordinate servers. It is recommended that each subordinate server should report on no more than 1200 unique data sources. This number includes Data agents, Fabric agents (in-band and out-of-band), CIM agents, and VMWare data sources. Once this threshold has been met, a new Tivoli Storage Productivity Center server should be deployed and all new data sources should point to the new server.

For more information about Disk Manager, see "Planning for the Disk Manager."

For more information about Fabric Manager, see "Planning for the Fabric Manager" on page 73.

## Planning for the Disk Manager

This section provides information on planning for Disk Manager.

Because IBM Tivoli Storage Productivity Center provides an abstraction for the storage subsystems managed in order to make the heterogeneous environment look more homogenous, Tivoli Storage Productivity Center uses a number of terms, which map to different things when looking at the actual storage subsystems. Most of these terms are derived from SMI-S, which already provide a common model for storage subsystems.

These terms are:

#### storage pool

A collection of storage capacity with a given set of capabilities. A pool has certain storage capabilities, which indicate the range of quality of service requirements that can be applied to objects created from the pool.

#### primordial pool

A type of storage pool. This pool might contain unformatted or unprepared capacity. This type of pool might simply contain unassigned capacity. Storage capacity is drawn from the primordial storage pool to create concrete storage pools. The primordial storage pool aggregates storage capacity that has not been assigned to a concrete storage pool. Storage volumes are allocated from concrete storage pools. For the Tivoli Storage Enterprise Storage Server, DS8000, and DS6000, the primordial pool is the disk groups or array sites which are installed in the machine but have not yet been configured into RAID arrays. Primordial pools for SAN Volume Controller are those MDisks which are available, but have not yet been configured to any MDisk Group (one primordial pool per back-end controller). The Primordial pool for the XIV Storage System is a virtual concept that represents the aggregation of system-wide unallocated storage capacity which is available but unassigned to XIV storage pools.

#### storage volumes

Allocations of storage capacity that is exposed from a system through an external interface. In SCSI terms, they are logical units.

The following table shows the mapping of the Tivoli Storage Productivity Center terms to the device specific terms.

Tivoli Storage Productivity Center terms:	Storage pool	Primordial pool	Storage volume	Disk
Device terms	01	Ĩ	0	
DS6000, DS8000, Tivoli Storage Enterprise Storage Server	Extent pool	not applicable	Volume	Disk drive module (DDM)
DS4000	Volume group	not applicable	Volume	Disk
SAN Volume Controller	MDisk group	not applicable	VDisk	MDisk
XIV Storage System	Storage pool	not applicable	Volume	Disk

Many disk arrays provide an interface for the administrator to specify which initiators can access what volumes through which target ports. The effect is that the given volume is only visible to SCSI commands that originate from the specified initiators through specific sets of target ports. There may also be a capability to select the SCSI Logical Unit Number as seen by an initiator through a specific set of ports. The ability to limit access is called *device masking*. The ability to specify the device address seen by particular initiators is called device mapping. For SCSI systems, these terms are known as LUN masking and LUN mapping. In Tivoli Storage Productivity Center, masking and mapping is handled through host assignment.

**Note: For DS6000 and DS8000:** The DS6000 and DS8000 keep track of the number of spares still available after a spare disk has been used to replace a failing disk drive in the device by marking the failing drive with an operational status of "Predictive Failure." If there are not enough spare disks left for a rank, then the disk's operational status also shows a status of "Error."

If the DS6000 or DS8000 marks a disk drive with a status of "Predictive Failure" but not "Error", then Tivoli Storage Productivity Center will show a green icon with a consolidated status of "OK" in the health overlay, and will not create an alert. The topology viewer will show the real status of the disk drive as "Predictive Error" in the Operational Status column of the tabular view. This allows you to see the changed status.

### Planning for the IBM CIM agents

The CIM agents are provided by the vendor of the storage device, fabric switch, or tape library. This topic provides planning information for the IBM CIM agents for the IBM storage subsystems.

For storage subsystems, the CIM agents are needed for storage asset information, provisioning, alerting, and performance monitoring. For tape libraries, the CIM agents are used for asset and inventory information. The CIM agents conform to the SNIA SMI-S specification to provide a communication transport between IBM Tivoli Storage Productivity Center and the managed devices.

The CIM agents can be referred to by a variety of names, such as CIMOM (CIM Object Manager) or SMIS agent. A CIM agent consists of a CIMOM and an SMIS provider for the managed device. The CIM agent can be a separate agent installation or can be imbedded in the device itself, as is the case with Cisco fabric

switches. In this case, there is no proxy agent to install and Tivoli Storage Productivity Center is configured to point to the managed device itself.

Once the CIM agent is installed and configured, Tivoli Storage Productivity Center can be configured to communicate with it.

Tivoli Storage Productivity Center supports the following:

- CIM agent 5.4 for the DS8000 DS6000 and Tivoli Storage Enterprise Storage Server storage systems.
- CIM agent 5.3 for the Tivoli Storage Enterprise Storage Server Model 800, DS6000, and DS8000 storage systems.
- CIM agent 5.2.1 for the Tivoli Storage Enterprise Storage Server Model 800, Tivoli Storage Enterprise Storage Server F20, DS6000, and DS8000 storage systems.
- CIM agent 5.1 for the Tivoli Storage Enterprise Storage Server, DS6000, and DS8000 storage systems.

The CIMOM for XIV Storage System will be embedded in the firmware and therefore will be started and ready for SLP discovery. Tivoli Storage Productivity Center support for this CIMOM is targeted for a future XIV Storage System software release. The XIV Storage System information provided in the Tivoli Storage Productivity Center 4.1 documentation is only for planning purposes until the supported XIV Storage System firmware is available. A flash will be issued when Tivoli Storage Productivity Center support for XIV Storage System is available.

#### Note:

- Do not use different DS CIM Agent releases (for example 5.1, 5.2.1, 5.3, and 5.4) to manage the same DS8000, DS6000, or Tivoli Storage Enterprise Storage Server with IBM Tivoli Storage Productivity Center. Each DS CIM Agent release reports some information in a different way so this can cause a reporting failure. Use the same release of DS CIM Agent for all CIMOMs managing the same device.
- If an Engenio Provider is being used by the Tivoli Storage Productivity Center server, then no other SMIS-enabled application should be using that Engenio Provider. This controlled environment is required to ensure that the Engenio Provider receives synchronized CIM Client requests.
- For the Tivoli Storage Enterprise Storage Server 2105, disk drive information could be displayed twice after an upgrade. The first half of the information is new and is displayed online. The second half of information is no longer detectable. The second half of information is impossible to correlate.

For more information about the CIM agents and a list of certified devices and applications, go to this Web site: http://www.ibm.com/systems/support/storage/software/tpc/. Click on a product, select the Install/use tab, and then select a topic under "Integration/Interoperability."

For information about certified SMI-S devices, see http://www.snia.org/ctp/ conformingproviders#10provider.

For information about how to install and configure the CIM agent, see http://www.ibm.com/servers/storage/support/software/cimdsoapi/.

# Planning for the TagmaStore CIM agents

The TagmaStore CIM agents are provided by Hitachi Data Systems for the TagmaStore storage subsystem. The TagmaStore CIM agent collects information from the TagmaStore storage subsystem.

IBM Tivoli Storage Productivity Center now supports the Hitachi Data Systems TagmaStore CIM Agent 5.8. This version of the CIM Agent supports only the Array Profile and not the Storage Virtualizer Profile. However, Tivoli Storage Productivity Center will support the TagmaStore as a Storage Virtualizer. Tivoli Storage Productivity Center will be able to display information for virtual disks and local disks.

Tivoli Storage Productivity Center cannot provide correlation information between the virtual storage used by TagmaStore and the volumes created on the storage due to an existing limitation of the CIM agent 5.8 from Hitachi Data Systems. However, Tivoli Storage Productivity Center reports correctly display the correlation between volumes created on the local storage and the local disks. This limitation has no impact on the topology but it does affect several reports that show the correlation:

- Data Manager > Reporting > Asset > By Storage Subsystem > <HDS\_device> > Managed Disks > LUN (will not show the relation between the disk and LUN or volume in the tree)
- Disk Manager > Reporting > Storage Subsystem > Volume to Backend Volume
- Disk Manager > Reporting > Storage Subsystem > Computer Views (because Tivoli Storage Productivity Center cannot populate the information for volumes created on the virtual disks)

All volumes are created from a storage pool that is allocated from a primordial storage pool and an imported primordial pool. A volume cannot be created over both local and virtual extents.

For LUN and volume correlation, the host machine must have the Data agent and Fabric agent installed and the TagmaStore device should be in the same SAN fabric. There should also be a zone configured in the active zoneset between the ports of the host machine and the ports of the TagmaStore device. The Fabric agent needs to be configured for the fabric to which the host is connected.

For back-end correlation, the TagmaStore device ports and back-end subsystem ports must be in the same zone and the back-end subsystem has assigned storage volumes to all ports of the TagmaStore device.

Before you can use the CIM agent 5.8, you must uninstall pre-version 5.8 CIM agents. You cannot have a mixture of CIM agent 5.8 and pre-version 5.8 CIM agents. This will cause failures.

The events returned by the CIM agent are:

- Generation of a volume
- Deletion of a volume
- Allocation of a path
- Cancellation of a path

When you delete a volume, you can only delete the latest created volume. For example, if you create five volumes, you need to delete the volumes in reverse order from the creation order.

### **General procedure**

The general steps to follow to use the TagmaStore CIM agents are:

- 1. Install Tivoli Storage Productivity Center or upgrade to 4.1.
- 2. Remove the pre-5.8 CIM agent from Tivoli Storage Productivity Center as a data source before adding the 5.8 CIM agent. You must add the CIM agent before running a discovery job.
- 3. Run a discovery job for the TagmaStore CIM agent.
- 4. Run probe jobs, scan jobs, and ping jobs for the TagmaStore CIM agent.
- 5. View the storage information gathered by the monitoring jobs through the topology viewer and reports that you can generate through the Fabric Manager, Data Manager, and Disk Manager.

### Planning for Disk Manager configuration

This section provides information for planning Disk Manager configuration.

Disk Manager data can only be collected from devices managed by a CIM agent. You need to make sure the following items are done before adding the CIM agent:

- 1. The version of CIM agent and firmware for the device is supported.
- 2. A CIM agent is installed on a different server from the IBM Tivoli Storage Productivity Center server. For some storage subsystems, the CIM agent is imbedded in the subsystem, and therefore, no separate CIM agent installation is required.
- **3**. For subsystems on a private network, be sure to have the CIM agent installed on a gateway machine so that the Tivoli Storage Productivity Center server on a different machine can communicate with the CIM agent.
- 4. The CIM agent is configured to manage the intended device.

For information about how to install and configure the CIM agent, contact your CIM agent provider.

To get storage subsystem data, you must do the following general steps:

- 1. Add the CIM agent to Tivoli Storage Productivity Center.
- 2. Run a CIMOM discovery operation for the subsystems. The CIMOM discovery operation consists of two parts:
  - Discovering the CIM agents available in the network.
  - Discovering the storage subsystems managed through these CIM agents.

The first part of the discovery is based on service location protocol (SLP). Depending on your network configuration, you have to configure Tivoli Storage Productivity Center to scan the local subnet, query a Directory Agent (DA), or do both.

**3**. Run a probe job for the subsystems. This collects detailed information about the storage subsystems known to Tivoli Storage Productivity Center. In contrast to a CIMOM discovery job, the probe interacts with the CIM agent to get information about just the storage devices configured to be probed. You can set up a probe job to gather data for just one storage subsystem, or you can set up probe jobs to collect data from more than one storage subsystem. A probe job

must be run before volumes can be created on a storage subsystem or a storage subsystem can be monitored for performance management.

Running a probe job puts additional workload on the Tivoli Storage Productivity Center server, the repository database, and the CIM agents. For probe jobs, this is especially important if multiple devices are managed by the same CIM agent and are probed concurrently. As a result, the probe completion time is impacted by the number of devices probed in parallel and the number of CIM agents involved in the probe job. This is especially important if the CIM agent machines are at the lower end of the hardware prerequisites.

To help keep the workload low, the probe jobs for the storage subsystems should be distributed over a time when Tivoli Storage Productivity Center as well as the network are not used heavily, which is typically over night time. To allow this workload distribution, there should be probe jobs for each storage subsystem, which are scheduled to run one after the other.

The following example shows how you might run your probe jobs. This environment assumes that you have four storage subsystems (SS1, SS2, SS3, and SS4), with three of them having a probe job duration of less than 30 minutes and one (SS3) taking 90 minutes to complete a probe job. You could arrange the probe jobs according to the following table:

Probe	Probe 1	Probe 2	Probe 3	Probe 4
Subsystem	SS1	SS2	SS3	SS4
Start time	0:30	1:30	2:30	4:30

If you have a probe job that collects data from more than one subsystem, then the probe job should be configured to contain only one subsystem per CIM agent. This is important because the CIM agent response time is a major contributor to the overall Tivoli Storage Productivity Center probe job duration.

The storage subsystem probe jobs collect detailed information about the configuration of the storage subsystems and the properties describing those configuration elements. The elements gathered are:

- Component computer systems (like the SAN Volume Controller nodes)
- Storage pools
- Storage volumes
- FC ports
- Disks
- Host-to-volume assignments
- Relationships among the elements (for example storage pool to storage volume relationships)

This configuration is typically not changing that much, especially because Tivoli Storage Productivity Center updates the repository database whenever you do configuration changes using the Tivoli Storage Productivity Center GUI (for example when creating a volume). Therefore, the probe jobs for the subsystems can be scheduled to occur less often than the CIMOM discovery.

If you use the device-specific CLI for configuration changes, the probe is needed in case the CIM agent does not support all needed indications to inform Tivoli Storage Productivity Center about the change.

Storage subsystems should be probed once every one or two days. Other factors influencing this interval are:

• Is the device mainly managed by Tivoli Storage Productivity Center or is an alternative tool used (for example device-specific CLI)?

- Does the CIM agent support CIM indications and how extensively are Tivoli Storage Productivity Center alerts used?
- 4. Create alerts. You can specify which alerts you want to be notified of when monitoring the storage subsystems.

Because communication between Tivoli Storage Productivity Center and the storage subsystem is based on SMI-S, CIM indications are the primary approach for getting notified about relevant events, and depending on the configuration, raise an alert for this event. CIM indications are not fully implemented in many CIM agents, but the CIM agents are constantly being improved. Tivoli Storage Productivity Center uses the probe jobs as a kind of fall-back mechanism to raise the alerts even if the event was not presented to Tivoli Storage Productivity Center by the CIM agent for the device.

This approach also has implications on how often to run the probe jobs. Normally, it is enough to run a probe job for the storage subsystems once every one or two days. If you plan to use alerts to monitor your storage subsystems, depending on the CIM indication implementation of the CIM agent, you may want to decide to have shorter probe job intervals (for example every 12 hours) to account for missing indications.

If an event is not sent as a CIM indication to Tivoli Storage Productivity Center, you will not see an alert being raised for that event until the next probe of this storage subsystem. Tivoli Storage Productivity Center does a comparison with the previous status of the device elements. Tivoli Storage Productivity Center does this to see if anything significant has changed (like an operational status changing from "OK" to "error." In this case, the alert is raised at the time of the probe, not at the time the event actually happened. This means that it might take up to one probe interval of the storage subsystem for an alert to be generated. Depending on the CIM indication support of the CIM agent used, you should consider this delay in alert generation when planning probe schedules.

Tivoli Storage Productivity Center should be configured to catch SNMP traps from subsystems, so that all notifications sent by the storage subsystems show up in Tivoli Storage Productivity Center. For information about SNMP traps, see "Planning for Fabric Manager switches and directors" on page 82.

# Planning for DS8000 performance

This section provides information about DS8000 performance.

Space-efficient volumes are not fully allocated when they are created, unlike the "normal" type of volumes. Their actual allocated space grows as the volume is used, until it has reached the full volume's size. After the full volume's size is reached, the allocated size does not change further. For performance management, this means that at any given point in time, the current size of the volume is unknown. This makes it impossible to know how the volume's segments (extents) are distributed among the various ranks in a multi-rank extent pool. It is therefore impossible to accurately compute the performance statistics for the arrays associated with a multi-rank extent pool that contains one or more space-efficient volumes.

# Planning for the SAN Volume Controller

Use this information to plan for using the SAN Volume Controller with IBM Tivoli Storage Productivity Center.

You will be able to view reports and the topology for your SAN Volume Controller environment. Use this information to understand the configuration that is required to use SAN Volume Controller with Tivoli Storage Productivity Center.

By using Tivoli Storage Productivity Center, you will be able to view SAN Volume Controller performance statistics for the following reports:

- Disk Manager > Reporting > Storage Subsystem Performance > By Storage Subsystem
- Disk Manager > Reporting > Storage Subsystem Performance > By I/O Group
- Disk Manager > Reporting > Storage Subsystem Performance > By Node

You will also be able to view the SAN Volume Controller environment through the topology viewer.

When you have hosts connected to storage subsystems which have multi-pathing enabled, you should have the multi-pathing subsystem device drivers (SDD) installed on the hosts. For more information, see the SAN Volume Controller Information Center and click the following:

- Installing > Attaching to a host running the Microsoft Windows 2000 Server and Windows Server 2003 operating systems > Configuring the Windows 2000 Server and Windows Server 2003 operating systems > Multipath support for host running the Windows 2000 Server and Windows Server 2003 operating systems or
- Installing > Attaching to a host running the Linux operating system > Configuring the Linux operating system > Multipath support for hosts running the Linux operating system

### SAN Volume Controller 4.3.1

Tivoli Storage Productivity Center supports these new features of SAN Volume Controller version 4.3.1. This is in addition to the features supported for SAN Volume Controller version 4.2.

The big advantages of SAN Volume Controller 4.3.1 are performance and reliability. Currently the proxy CIM agent architecture causes all clusters to be scanned in response to each request so the more clusters under management of a single CIM agent, the slower the Tivoli Storage Productivity Center probes. Starting with SAN Volume Controller 4.3.1, the CIM agent is embedded in the hardware. Any time you have more than a single cluster attached to a CIM agent, you should see better overall probe times with the embedded CIM agent. From a reliability point of view the embedded CIM agent is clustered so if the SAN Volume Controller node it is running on fails, it will be restarted on one of the other nodes automatically. The SAN Volume Controller processes also automatically recovers many software failures. The other advantage is that there is only one network connection for data collection so connection issues between the CIM agent and the cluster are reduced because it is a local connection.

For more information about SAN Volume Controller, go to the Information Center at http://publib.boulder.ibm.com/infocenter/svcic/v3r1m0/index.jsp.

Tivoli Storage Productivity Center supports the SAN Volume Controller version 4.3.1 CIM agent only when used with the SAN Volume Controller 4.3.1 cluster firmware version. Conversely, the new firmware should only be managed by the SAN Volume 4.3.1 CIM agent.

**Note:** Using multiple CIM agents to manage the same SAN Volume Controller cluster is not supported.

### **General procedure**

To view the reports and topology for the SAN Volume Controller environment, follow these general steps:

- 1. Configure the SAN Volume Controller console.
- 2. Log into the SAN Volume Controller console and create a user ID and password for use with Tivoli Storage Productivity Center.
- **3.** Open the Tivoli Storage Productivity Center user interface and register the CIM agent with Tivoli Storage Productivity Center.
- 4. Run a discovery job for the CIM agent.
- 5. Run a probe job for the CIM agent.
- **6.** View the reports and topology for the SAN Volume Controller environment in Tivoli Storage Productivity Center.

## Planning for the IBM XIV Storage System

Use this information to plan for using the IBM XIV Storage System with IBM Tivoli Storage Productivity Center.

**Important:** The XIV Storage System information provided in the Tivoli Storage Productivity Center 4.1 documentation is only for planning purposes until the supported XIV Storage System software is available. Tivoli Storage Productivity Center support is targeted for a future XIV Storage System software release. A flash will be issued when Tivoli Storage Productivity Center support for XIV Storage System is available.

IBM XIV Storage System is a high-end disk storage architecture designed to eliminate the complexity of administration and management of storage. The XIV Storage System system's parallelized architecture, optimal exploitation of all system components (including disks, CPUs, and switches), and unique caching architecture all translate into excellent performance.

The unique balancing of all data across system components prevents the occurrence of hot spots. With all components working under the same load, performance and reliability are exceptional.

XIV Storage System uses large capacity SATA disk drives which optimizes the use of disk capacity, resulting in outstanding power consumption without compromising performance.

XIV Storage System is designed to be scalable in storage, interfaces, cache, CPU power, and internal bandwidth. The architecture supports each aspect to grow independently, resulting in a scalable system in both capacity and performance.

XIV Storage System provides data protection and availability. All disk drives, modules, switches, and UPS units are fully redundant, ensuring high reliability and excellent performance.

The built-in thin provisioning of XIV Storage System helps reduce direct and indirect costs by allowing users to install capacity only for data actually written. You can grow your data capacity over time with minimal management effort.

For more information about XIV Storage System, see the XIV Storage System Information Center.

### **Tivoli Storage Productivity Center support**

XIV Storage System has an embedded Common Information Model (CIM) agent, which Tivoli Storage Productivity Center uses to run discovery and probe jobs. Because of the dynamic XIV architecture, where volume data is spread over all disks, no data that describes the space allocation from volumes to a specific physical disk is available.

XIV Storage System includes a graphical user interface (GUI) for configuration and administration (XIV Storage Manager). XIV Storage Manager is the element manager for XIV Storage System. XIV Storage Manager version 44 or later must be installed on the same computer as the Tivoli Storage Productivity Center GUI. If XIV Storage Manager is not installed on the same computer as the Tivoli Storage Productivity Center GUI or is configured incorrectly, an error message is displayed when you attempt to start XIV Storage Manager from Tivoli Storage Productivity Center. For more information about this message, see "Error message when starting element manager for XIV Storage System" on page 588.

### Features that are not supported for XIV Storage System

Tivoli Storage Productivity Center 4.1 does not support the following features for XIV Storage System:

- Common Information Model (CIM) indications
- Provisioning
- Performance Manager
- SAN Planner
- Storage Optimizer
- Volume Planner
- · Disk configuration
- Single sign-on and alerts and indications related to single sign-on
- Launch in context

XIV Storage System does not support IPv6.

### Considerations for data collected for XIV Storage System

The following considerations apply to values shown in the XIV Storage System and Tivoli Storage Productivity Center GUIs.

- The XIV Storage System GUI and the XIV Storage System command line interface (CLI) report sizes in GB of volumes, pools, and so forth, based on 10^9. Tivoli Storage Productivity Center reports sizes in GB based on 2^30. For example, a volume showing a size of 17 GB in the XIV Storage System GUI is reported as 16 GB in Tivoli Storage Productivity Center.
- XIV Storage System differentiates thin provisioned pools from non-thin provisioned (regular) pools and volumes in a thin provisioned pool and a non-thin provisioned pool. When hard size is equal to soft size, the pool is represented as a regular pool, otherwise the pool is represented as thin provisioned. However, the XIV Storage System CLI and CIM do not distinguish

between regular and thin provisioned pools and all pool volume names in Tivoli Storage Productivity Center are prefixed with an asterisk (\*) to indicate that the volume is thin provisioned.

# Planning for Tivoli Storage Enterprise Storage Server FlashCopy reports

Use this information to plan for displaying Tivoli Storage Enterprise Storage Server FlashCopy reports in IBM Tivoli Storage Productivity Center.

If you want to display Tivoli Storage Enterprise Storage Server FlashCopy relationships in Tivoli Storage Productivity Center, you must add the type ESSCS in addition to type Tivoli Storage Enterprise Storage Server to the CIM agent. For example:

dscimcli mkdev 10.10.10.100 -type ess -user <user\_ID>
-password <password>
dscimcli mkdev 10.10.10.100 -type esscs -user <user\_ID>
-password <password>

You must also have a specific level of microcode. For information about the microcode level, see http://www.ibm.com/systems/support/storage/software/tpc/. Click the Install/use tab. Click Tivoli Storage Productivity Center Version 4 Release 1 Supported Products List.

## Storage capacity of volumes

This section provides information about how IBM Tivoli Storage Productivity Center displays the storage capacity of volumes.

The disk storage that IBM Tivoli Storage Productivity Center supports is expressed in powers of two:

1 KB = 2 to the power of 10 bytes (1024)
1 MB = 2 to the power of 20 bytes (1 048 576)
1 GB = 2 to the power of 30 bytes (1 073 741 824)
1 TB = 2 to the power of 40 bytes (1.09951E+12)
1 PB = 2 to the power of 50 bytes (1.1259E+15)

This matches the convention of many storage subsystems but does not match the behavior of the Tivoli Storage Enterprise Storage Server family of devices. Therefore, a volume created using the Tivoli Storage Enterprise Storage Server Specialist with a size of 10 GB might be displayed by Tivoli Storage Productivity Center as 9.3 GB in size. TheDS6000 and DS8000 storage subsystem GUIs display the storage as powers of two.

## Planning for the Fabric Manager

This topic provides planning information for the Fabric Manager.

Feature	Advantages	Benefit
Automatic device discovery	Enables you to see the data path from the servers to the switches and storage systems	Easily manage your SANs from a single console
Real time monitoring and alerts	Monitors SAN events and alerts administrators of problems	Helps maintain the availability of your SAN

The main features of Fabric Manager are shown in the following table.

Feature	Advantages	Benefit
Zone control	Gives you the ability to add and remove devices from zones	Comprehensive fabric management from a single console
SAN reporting	Provides the ability to generate reports on the SAN devices	Quickly provides reports and inventories of your SAN
Enterprise scalability	Scale from SAN islands to enterprise SANs	Accommodates new and ever changing business needs
Switch performance management (1)	Provides the ability to monitor switches for performance metrics which allows for the triggering of switch threshold alerts and performance reporting. The performance reporting is at the switch and port levels and displays in the defined Switch Performance reports and in the topology viewer.	Helps you maintain high SAN availability

### Note:

1. IBM Tivoli Storage Productivity Center for Fabric provides predictive fault analytics for the SAN infrastructure through reporting, monitoring and alerting of link failure rates and error frame rates. These transient errors are indicative of potential pending SAN link failures.

Most heterogeneous fabrics, which are composed of switches from two or more vendors, are not supported. IBM Tivoli Storage Productivity Center supports heterogeneous fabrics that are comprised entirely of McDATA and Brocade switches, when CIM agents are configured for these switches. All other heterogeneous fabrics are not supported. The following are known issues which prevent Tivoli Storage Productivity Center from supporting heterogeneous fabrics (with the exception of Brocade and McDATA heterogeneous fabrics):

- If there is no Brocade out-of-band Fabric agent and no CIM Agent for a heterogeneous fabric, Tivoli Storage Productivity Center will attempt to perform zone control operations through an available in-band Fabric agent for the fabric. However, if the in-band Fabric agent detects that one or more Brocade switches are in the fabric, zone control is not allowed by Tivoli Storage Productivity Center on the fabric through the in-band Fabric agent.
- Some zone member types that can be chosen for use in zone control operations will cause zone control operations to fail in heterogeneous fabrics. This is because switch vendors only support limited zone member types in heterogeneous fabrics.
- Zone control capabilities of the fabric are assumed by Tivoli Storage Productivity Center to be the capabilities of the principal switch vendor. However, the agent used for zone control operations may be for a switch vendor that differs from the principal switch in heterogeneous fabrics. For this reason, zoning operations such as creation of "orphan" zones and use of non-alphanumeric characters in zoning entity names may fail at the switch rather than be caught by Tivoli Storage Productivity Center.
- Heterogeneous fabrics with Cisco may be shown as duplicate fabrics in the topology viewer if only CIMOM Data Sources are configured. Users should

configure out-of-band Fabric agents for both the Cisco and the non-Cisco switches. The non-Cisco switch may be represented as both a part of the physical fabric and the virtual fabric.

# **Planning for SMI-S support**

IBM Tivoli Storage Productivity Center supports the SMI-S as the single standard interface for managing SANs. You no longer need the in-band agents for zone discovery and zone control operations. Tivoli Storage Productivity Center uses the SMI-S Fabric Profile and related SubProfiles for inventory collection of SAN topology and zoning, for active configuration of zoning, and for fabric and switch alerts for the switch vendors.

This support applies to Brocade and McDATA switches for the following:

- Topology discovery
- Zoning discovery
- Zone control of zone sets and zones
- Alerts from fabric and switch events
- Launching switch or fabric element managers

The legacy interfaces (SNMP and GS-3) will still be necessary for QLogic and Cisco switches and SANs.

Brocade has acquired McDATA and therefore provides two separate SMI-S agents: one for the Brocade switches that did not come from the McDATA acquisition and one for managing switches from the McDATA SMI-S agent. This document refers to the SMI-S agents as the fabric CIM agents.

The use of legacy interfaces for discovery of topology information (SNMP and GS-3), and legacy interfaces for zone inquiry (Brocade API and GS-3) and legacy interfaces for zone control (Brocade API and GS-3) are still supported for these vendors. However, the SMI-S interface is automatically the preferred mechanism for these vendors when CIM agents are configured with Tivoli Storage Productivity Center.

Table 19 outlines the supported and preferred interfaces for topology discovery, zone inquiry and probing, and zone control.

Function	Brocade	McDATA	Cisco	QLogic
Topology discovery	Preferred: fabric CIM agent Still supported: out-of-band SNMP and in-band GS-3 agents	Preferred: fabric CIM agent Still supported: out-of-band SNMP and in-band GS-3 agents	No change: in-band GS-3 out-of-band SNMP SNMP is needed for physical infrastructure discovery.	No change: in-band GS-3 out-of-band SNMP

Table 19. Supported and preferred interfaces for fabric management

Function	Brocade	McDATA	Cisco	QLogic
Zone discovery	Preferred: fabric CIM agent	Preferred: fabric CIM agent	No change: in-band GS-3	No change: in-band GS-3
	Still supported: Brocade API	Still supported: In-band GS-3		
Zone control	Preferred: fabric CIM agent	Preferred: fabric CIM agent	No change: in-band GS-3	No change: in-band GS-3 fabric CIM agent
	Still supported: Brocade API	Still supported: in-band GS-3		
Fabric and switch alerts	Preferred: fabric CIM agent	Preferred: fabric CIM agent	No change	No change
	Still supported: Out-of-band SNMP, Brocade API, in-band GS-3	Still supported: Out-of-band SNMP, in-band GS-3		
Performance monitoring	Preferred: fabric CIM agent	Preferred: fabric CIM agent	No change: fabric CIM agent	No change: fabric CIM agent
Launch of switch and fabric element managers	Preferred: fabric CIM agent	Preferred: fabric CIM agent	No change: out-of-band SNMP, in-band GS-3	No change: out-of-band SNMP, in-band GS-3
	Still supported: Out-of-band SNMP, in-band GS-3	Still supported: Out-of-band SNMP, in-band GS-3		

Table 19. Supported and preferred interfaces for fabric management (continued)

Here are some things to note about fabric CIM agents:

- You need to install and configure the fabric CIM agents before specifying the CIM agents through Tivoli Storage Productivity Center.
- Some CIM agents are embedded in the switch (QLogic and Cisco). Other CIM agents are not embedded (McDATA and Brocade) and therefore run on a separate host machine. These CIM agents can manage one or more switches.
- For information about the CIM agents which have been tested by the Conformance Testing Program by SNIA, see http://www.snia.org/ctp/ conformingproviders.
- For information about the switches and CIM agents that IBM Tivoli Storage Productivity Center supports, see http://www.ibm.com/systems/support/ storage/software/tpc/. Click on IBM Tivoli Storage Productivity Center for Fabric. Click on the Install/use tab. Click on Tivoli Storage Productivity Center Version 4 Release 1 - Supported Products Matrix for Fabric Manager.
- There are some configuration considerations with McDATA switches. The McDATA SMIS agent can be configured to run in "proxy" mode or in "direct" mode.
  - In "proxy" mode, the SMIS agent communicates through an EFCM Server. The zoning database visible from the SMIS agent is synchronized with the

zoning database stored on the EFCM Server. For this reason, Tivoli Storage Productivity Center users should run the McDATA SMIS agent in "proxy" mode.

- In "direct" mode, the SMIS agent communicates directly with the switches and stores inactive zone sets on the SMIS agent. The zoning database from the SMIS agent is not in synchronization with the zoning database from EFCM.
- The benefits of using the fabric CIM agents instead of in-band Fabric agents are:
  - Enables probes and zone control to not occur within the data path.
  - Zone alias control is only supported by Tivoli Storage Productivity Center through the fabric CIM agents.
  - Propagation of alerts for real-time SAN events will not be degraded by the use of fabric CIM agents.
- For probes, a default "enumerations" probe algorithm is used to quickly probe all fabrics managed by a proxy CIM agent (for McDATA or Brocade), even if only a subset of the fabrics is intended to be probed. For this reason, you should set up fabric probes so that all fabrics managed by a single CIMOM are included in one probe job definition.
- Brocade fabrics that are not laid out as a "mesh", where one ISL break can segment the fabric, should be managed by both a fabric CIM agent and by an out-of-band Fabric agent (SNMP). The reason for this is that Brocade CIM agents do not automatically manage newly created fabrics in the event of a fabric segmentation.
- Note that fabric CIM agents are the preferred agent type with Tivoli Storage Productivity Center fabric support for Brocade and McDATA fabrics. You should consider using the legacy agents for redundancy, in addition to the CIM agents.
- You should use fabric CIM agents if you want to use zone alias control (for Brocade) or performance management features (for all switch vendors). The use of out-of-band Fabric agents and in-band Fabric agents can be used in addition to the fabric CIM agents. In Brocade or McDATA environments with fabric CIM agents as well as out-of-band Fabric agents and in-band Fabric agents, only the fabric CIM agent will be used for zone control. Discoveries, probes, and fabric events will use all three types of agents.

# **Collecting data with the Fabric Manager**

IBM Tivoli Storage Productivity Center uses four different types of agents to gather data about the switches. Different combinations of these agents are required to effectively enable the functions of Fabric Manager. In addition, the topology viewer is greatly affected by the proper discovery of all the managed entities in the management scope of Tivoli Storage Productivity Center.

For information about the supported agent types for switch performance management and fabric zone configuration, see the following table.

Function > Switch	Brocade	McDATA	Cisco <sup>1</sup>	QLogic
Switch Performance Monitoring	CIMOM agent	CIMOM agent	CIMOM agent	Not supported

Table 20. Supported agent types for Switch and Fabric Functions

<b>Function &gt; Switch</b>	Brocade	McDATA	Cisco <sup>1</sup>	QLogic
Zone Control	Recommended: CIMOM agent	Recommended: CIMOM agent	In-band fabric agent required in each VSAN	In-band fabric agent
	Also supported: Out-of-band fabric agent	Also supported: In-band fabric agent		
Zone Control with Zone Aliases	CIMOM agent	Not supported	Not supported	Not supported
Switch and switch port information collected	Recommended: CIMOM agent	Recommended: CIMOM agent	Recommended: CIMOM agent	Out-of-band fabric agent, In-band fabric agent
	Out-of-band fabric agent, In-band fabric agent	Out-of-band fabric agent, In-band fabric agent	Out-of-band fabric agent, In-band fabric agent	
Topology connectivity information collected	Recommended: CIMOM agent Also supported: Out-of-band fabric agent, In-band fabric agent	Recommended: CIMOM agent Also supported: Out-of-band fabric agent, In-band fabric agent	Out-of-band fabric agent, In-band fabric agent	Out-of-band fabric agent, In-band fabric agent
Zoning information collected	Recommended: CIMOM agent Also supported: Out-of-band fabric agent	Recommended: CIMOM agent Also supported: In-band fabric agent	In-band fabric agent required in each VSAN	In-band fabric agent
Tivoli Storage Productivity CenterAlerts	Recommended: CIMOM agent Also supported: Out-of-band fabric agent, In-band fabric agent	Recommended: CIMOM agent Also supported: Out-of-band fabric agent, In-band fabric agent	Out-of-band fabric agent, In-band fabric agent	Out-of-band fabric agent, In-band fabric agent
Hosts, endpoint devices, device-centric and host-centric information collected	In-band fabric agent	In-band fabric agent	In-band fabric agent	In-band fabric agent
Switch "Sensors and Events"	Out-of-band fabric agent	Out-of-band fabric agent	Out-of-band fabric agent	Out-of-band fabric agent

Table 20. Supported agent types for Switch and Fabric Functions (continued)

Notes:

• The In-band fabric agent gets the information on a VSAN basis.

• Each VSAN is viewed as an individual SAN.

• The Out-of-band fabric agent and CIMOM agent gets the physical fabric information and can correlate the VSAN information to a physical infrastructure.

• The Out-of-band fabric agent also collects some VSAN information.

# CIM agent for the Fabric Manager

For fabric switches (all switch vendors), the CIM agents are used for performance monitoring. For a subset of switch vendors, the CIM agents are also used to collect complete topology and zoning information, to receive and handle fabric events represented by "CIM Indications", and for zone control.

The CIM agents perform the following functions:

- Discovers the existence of fabrics and switches
- · Gathers switch port information needed for performance monitoring
- Gathers statistics for performance monitoring
- Gathers information about SAN topology (for Brocade and McDATA only)
- Gathers information about the zoning and allows zone control (for Brocade and McDATA only)
- Gathers event information sent by CIM Indications from the CIM agent (for Brocade and McDATA only)

The CIM agents are referred to by a variety of names, including CIMOM agent, SMI-S Provider, and so on. CIM agents are typically implemented by fabric vendors in these ways:

- One SMI-S CIM agent can manage the whole fabric. These are referred to as "Fabric CIMOMs".
- Each SMI-S CIM agent manages one switch in the fabric. These are referred to as "switch CIMOMs". A switch CIMOM may be imbedded in the switch.

For more information about the supported agent types for switch performance management and fabric zone configuration, see the IBM Tivoli Storage Productivity Center Information Center. Search for Frequently Asked Questions. Click Fabric Manager.

Some switch vendors imbed the CIM agent on the switch and others rely on a proxy CIM agent. For proxy CIM Agents, the CIMOM must be installed on a separate system and can typically be used to manage several switches. Contact your switch vendor for information on how to enable the CIM agent or install the CIMOM proxy.

# **In-band Fabric agent**

The in-band Fabric agent collects information about the SAN and sends that information to the IBM Tivoli Storage Productivity Center Device server. The in-band Fabric agent is capable of gathering topology information for the entire fabric. To gather host-level and detailed Host Bus Adapter (HBA) information, the agent must be installed on each host where that information is desired.

The in-band Fabric agent performs the following functions:

- Gathers information about the SAN by querying switches and devices for topology and identification information.
- Gathers host-level information for the local system.
- Gathers information about the HBAs installed on the local system, including make, model, and driver versions.
- Gathers information about the zoning and allows zone control (except for Brocade switches) of the fabric.
- Gathers event information detected by the HBAs and forwards it to the Device server.

Limitations to note are:

- A known limitation exists regarding zone control with downlevel in-band Fabric agents. For McDATA fabrics, Tivoli Storage Productivity Center users must use the McDATA SMIS agents, or must have all in-band Fabric agents that are attached to the fabric to be able to use Tivoli Storage Productivity Center's zone control feature. For Cisco and QLogic fabrics, users must have all in-band Fabric agents attached to the fabric in order to use Tivoli Storage Productivity Center's zone control feature.
- Can only gather host-level and HBA information on the host containing the in-band Fabric agent.
- Can only provide detailed identification for devices that are in the same zone as the in-band Fabric agent. The in-band Fabric agent will identify the device by world-wide name (WWN) if the in-band Fabric agent is NOT in the same zone as the device rather than being able to uniquely identify the device by device type (for example, host, subsystem, and so on).
- Identification of endpoint devices is reliant on the endpoint device responding to RNID or other queries.
- Can only gather a subset of the switch attributes. There are some switch attributes that can only be collected using out-of-band Fabric agents.
- If the HBA that the in-band Fabric agent uses is not in the active zone set for a fabric, events from the fabric will not be received by the in-band Fabric agent.
- Some removable media devices cannot handle command queuing causing long read or write commands to fail. To avoid this problem, see "Excluding devices from Fabric agent scans" on page 316.
- Tivoli Storage Productivity Center does not collect information on aliases through the in-band Fabric agents. Aliases are not supported by the GS-3 standard.

## **Out-of-band Fabric agent**

IBM Tivoli Storage Productivity Center uses SNMP queries to discover information about the SAN. Management Information Base (MIB) information is collected from the switches and directors by the out-of-band Fabric agent. Switches and directors are added as out-of-band Fabric agents and contacted from the Tivoli Storage Productivity Center Device server by SNMP.

The out-of-band Fabric agent performs the following functions:

- Gathers information about the fabric by querying the switch or director for topology information.
- Gathers information about the zoning and allows zone control (Brocade switch only) of the fabric.
- Gathers virtual SAN information for Cisco switches.

Limitations to note are:

- Topology information is only gathered for the switch added as an out-of-band Fabric agent. The agent will not be able to gather the topology information for any connected switches unless they are also defined as out-of-band Fabric agents. If you are performing out-of-band discovery only on a fabric with several switches, you must install an out-of-band Fabric agent for each switch in the fabric to discover the whole fabric.
- Device information is limited; most devices will be unknown with a type equal to "Other" and identified by their WWN.
- For Brocade switches, zoning information is gathered by configuring the out-of-band Fabric agent to also include the admin ID and password for the switch. (If a Brocade CIM agent is present, zoning information is gathered through the CIM agent rather than the Out-of-band Fabric agent for Brocade.)
- There must be a TCP/IP connection between the switch and the Tivoli Storage Productivity Center Device server.
- To enable events from the switch to the Device server, the switch must be configured to send SNMP traps to the Device server. The SNMP traps are synonymous to the events that are received by the in-band Fabric agent.

## Planning for Fabric Manager configuration

It is essential that you configure the main SAN devices properly before using IBM Tivoli Storage Productivity Center.

There are two main components to setting up Tivoli Storage Productivity Center:

- SAN environment setup
- Tivoli Storage Productivity Center setup

The essential elements of the SAN environment needed for Tivoli Storage Productivity Center are:

- Switches and directors
- Host Bus Adapters (HBAs)
- CIM agents for switches

These are the general steps to follow for fabric configuration:

- 1. Install and configure the SMI-S agent (CIM agent) for the switch. Contact your switch vendor for instructions on how to install and configure the SMI-S agent.
- 2. Install a Fabric agent for the switch.
- **3**. Run a CIMOM discovery job for the CIM agents. Wait for the job to complete successfully for the CIM agents.
- 4. Run a fabric probe job. Wait for the job to complete successfully for the fabric.
- 5. You will now be able to view information for the fabric and create a switch performance monitor job.

These are limitations for switches:

#### SNMP V1 protocol

Switches that are being managed out-of-band such as SNMP agents should be configured to use the SNMP V1 protocol. Some switches use SNMP V2 or V3 by default and must be reconfigured before they can work correctly with Tivoli Storage Productivity Center. Refer to the switch vendor documentation for specific configuration information.

#### HBA API for HP-UX

The HBA API for the HP-UX platform does not support the API function that is required for IBM Tivoli Storage Productivity Center for Fabric in-band agent to support the collection of SAN events through the HBA of the HP-UX host on which the Fabric in-band agent is installed. If there is no other Fabric agent (out-of-band or in-band) that is covering a particular SAN, alerts for SAN events will not be reported by Tivoli Storage Productivity Center and automatic discovery that would have normally been triggered due to reporting of such events will not occur. Users may still be able to have a Tivoli Storage Productivity Center agent report SAN events for a particular SAN and have automatic triggering of discovery if one of the following conditions is true:

- Installing a Fabric agent on another supported host (non-HP-UX platform) that is connected to the same SAN that the HP-UX Fabric agent or agents are connected to.
- Defining out-of-band agents that are configured to get SNMP traps from switches in that SAN. You should consider this option carefully because there can be performance implications for this option.

#### **Performance statistics**

Some switch vendors do not return all of the performance statistics required by Tivoli Storage Productivity Center. In these cases, some performance statistics might report as zero.

**Note:** A CIMOM discovery and fabric probe is required for all switch vendors supporting SMIS 1.1 and higher.

In the Storage Management Initiative Specification (SMI-S), a port's peak data rates are reported in the CIM\_FcPortRateStatistics class. For SMI-S Version 1.1, this class is an optional class, meaning that it might not be supported by a given vendor. This will be the case if the Tivoli Storage Productivity Center user interface shows zero values for the peak rates, even when there is non-zero traffic flowing through the port. When a vendor does support the this class, the peak data rate represents the peak value of the associated metric counter (as reported by the CIMOM used to access the device) over a recent, vendor-defined measurement window (for example, 20 milliseconds) of the Tivoli Storage Productivity Center measurement window (for example, 15 minutes).

#### Index number of a fibre channel port on a blade

Currently there is no SMI-S standard property that holds the index value number of a fibre channel port on a blade. For this reason, the Tivoli Storage Productivity Center SMIS Fabric Topology Table Mappers must have vendor-specific code for calculating the index. At this time, only Cisco and Brocade implement the Blades Subprofile, so index calculations will be done only for Cisco and Brocade.

#### Switch blade port index values

The switch blade port index values may be incorrect for Brocade switches where one of the following scenarios apply:

- When a port swap operation is performed
- When the Extended Edge PID mode has been enabled on the director. For more information about the Extended Edge PID mode, see the Brocade document *Fabric OS Administrator's Guide*.

## Planning for Fabric Manager switches and directors

For the Fabric Manager to gather and display information about switches and directors, the switches and directors must be configured correctly. The configuration varies between vendors. Incorrect switch configuration can lead to missing information and misconceptions about the IBM Tivoli Storage Productivity Center product not working properly with certain switches.

For the switch to successfully receive and respond to queries, there are some basic requirements:

• The FC Management MIB and FE MIB must be enabled on the switch.

- The switch must be configured to receive SNMPv1 queries and respond in SNMPv1. Some switches are configured to use SNMPv2 or SNMPv3 by default.
- The community string configured in IBM Tivoli Storage Productivity Center for Fabric must match one of the community strings configured on the switch with read access. Cisco switches must additionally have a community string match for write access. The default community strings in Tivoli Storage Productivity Center are "public" for read access and "private" for write access. Additional community strings can be defined on the switches, but will not be used.
- SNMP access control lists need to include the Tivoli Storage Productivity Center Device Server. Some automatically include all hosts while others exclude all hosts by default.

Another aspect of the SNMP configuration includes trap notification. SNMP traps are generated by the switch and directed to the Tivoli Storage Productivity Center Device Server as an indication that something in the fabric has changed and that a discovery should occur to identify changes. The default configuration for handling switch traps is to send them from thee switch to port 162 on the Tivoli Storage Productivity Center Device Server. For the successful generation and reception of traps, there are some configuration requirements:

- The trap destination must be set. The trap destination is typically the Tivoli Storage Productivity Center Device Server, but it can also be an intermediary SNMP manager that receives the trap and sends it to Tivoli Storage Productivity Center. This is set on the switch.
- The destination port must be set on the switch. Tivoli Storage Productivity Center listens on port 162 by default.
- The traps must be sent as SNMPv1. This is set on the switch.
- The trap severity level should be set to generate traps for change conditions. This typically means to send error level traps and anything more severe. This is set on the switch.

Configuring these settings differs between switch vendors and models. For information about configuring supported switches, see http://www.ibm.com/ developerworks. In the upper right corner, search for "configure switches." Open the article "Configure switches successfully for IBM Tivoli Storage Productivity Center for Fabric."

## Planning for host bus adapters (HBAs)

Proper installation of the HBA driver is an essential element for enabling data collection and is one of the most common problems when an agent appears to be healthy, but is not discovering any data other than the host information. Some HBA vendors will require a separate installation of the HBA API package while others include it with the driver.

For the switches to successfully receive and respond to queries, there are some basic requirements:

- The switch must support the FC-GS-3 standard interface for discovery:
  - Name server
  - Configuration server
  - Unzoned name server
- For zone control functions, the fabric zone server must be supported, except in the case of Brocade switches.

There are some basic requirements on the HBA for proper in-band Fabric agent operation:

- The HBA driver must be installed.
- The HBA API package must be installed. Some vendors include the HBA API package as part of their driver.
- HBA firmware is at a level that IBM Tivoli Storage Productivity Center supports.
- The current state of the HBA as reported by the operating system is good.
- The HBA has a good connection to the fabric.

Fabric events are automatically sent from the agent to the Tivoli Storage Productivity Center Device server. There is no need for configuration.

## Planning for private switch networks

Some switch vendors recommend a private IP network for the fibre channel switches. It is important to understand that the IBM Tivoli Storage Productivity Center Device server will not be able to communicate with the switches if they are on a private IP network. It is important to note that the out-of-band Fabric agents require a TCP/IP connection from the the Device server to the switch. Also, SNMP traps from the switches will not be able to travel directly from the switches to the the Device server.

If you are using a private switch IP network you will be reliant on in-band Fabric agents to gather your SAN information and to forward SAN events to the Device server.

Another option that is sometimes used with a private switch network is to allow the Tivoli Storage Productivity Center Device server to communicate on the private switch network using a second network interface card (NIC).

## **Configuring Brocade switches**

Use this information to configure your Brocade switches properly for use with IBM Tivoli Storage Productivity Center.

If you have a Brocade fabric and have an ISL (inter-switch link) break that causes a fabric segmentation, you must use the CIM agent as well as the out-of-band Fabric agent (SNMP) for the fabric. This is necessary because Brocade CIM agents do not automatically manage newly created fabrics in the event of a fabric segmentation.

Non-standard zones are not presented by the Brocade CIM agent. Therefore, Tivoli Storage Productivity Center will not display, delete, or remove non-standard zones.

In order to receive alerts through CIM Indications from your Brocade CIM agent correctly, the "trackchanges" setting must correctly be configured on each Brocade switch. Be sure to **telnet** into each Brocade switch and use the following CLI commands to check the settings and set the setting correctly:

trackchangesshow (to check the current "track changes setting) trackchangesset 1, 1 (to set the switch to track changes, which ensures that port disablement CIM Indications are sent)

Brocade CIM agents running on a system with multiple IP addresses must be configured correctly for the CIM agent to receive alerts from the switch. See the *Brocade SMI Agent User's Guide* section on "Enabling multi-homed support". If this is not set up correctly, the following results can occur:

- Tivoli Storage Productivity Center will not receive indications from the CIM agent.
- The CIM agent will not always have the latest zoning information for the fabric.

These are limitations for Brocade switches:

- The Brocade management application and CLI (**switchshow**) shows G-Ports as online but SNMP queries report these G\_Ports as offline. Tivoli Storage Productivity Center uses SNMP queries and will report these ports as offline. G\_Ports have a GBIC (terminator) connected to the switch port; they do not have any end device attached to these ports.
- If a Brocade switch is rebooted, in certain scenarios it may take 45 minutes or longer for the SMI-S Agent to rediscover the restarted switch. In order to avoid this problem, it is a good practice to restart the Brocade SMI-S Agent after rebooting any switch that the Brocade SMI-S Agent is managing. This will allow the SMI-S Agent to again manage the Brocade switch.

## **Configuring Cisco switches**

Cisco supports the concept of virtual SANs (VSANs). This is a method of virtualizing physical switches into multiple virtual switches and then using these virtual switches to create virtual fabrics (VSANs) within IBM Tivoli Storage Productivity Center.

Tivoli Storage Productivity Center uses the term physical infrastructure to represent the physical switches that are connected together. This physical infrastructure is what can be divided up into multiple virtual fabrics (VSANs)

When you probe the CIM agent for a Cisco switch, information collected is entered into the Tivoli Storage Productivity Center database. This information includes the representation of the Cisco fabrics and VSANs, switches, and partitioned switches.

Zone control is automatically disabled if one or more non-standard zones exist in the zoning definition.

Zoning is performed in-band with Cisco as is gathering topology information for VSANs. Information about the physical infrastructures and the VSANs contained in the physical infrastructures is obtained by using out-of-band with Cisco switches. Therefore, it is recommended that you use in-band and out-of-band Fabric agents with Cisco switches. If only in-band Fabric agents are used, Tivoli Storage Productivity Center views a VSAN as a normal fabric and there is no VSAN knowledge within the topology viewer.

It is recommended that you add each Cisco switch as an out-of-band Fabric agent and there should be at least one in-band Fabric agent per virtual fabric (VSAN). You must have at least one in-band Fabric agent in the VSAN to be able to perform zoning on the VSAN.

## **Configuring McDATA switches**

If you have a McDATA switch, ensure that the switch has the OSMS (Open Systems Management Server) feature enabled. OSMS is required for in-band discovery. If you want zone control, you must have the host control option enabled. See your McDATA documentation for information about Open Systems Management Server and how to enable different options.

If you want switch performance functionality for your McDATA switches, you will need to install a CIM agent as a proxy for McDATA because it does not have the CIM agent embedded into the switch. See the McDATA documentation for information about installing and configuring a CIM agent.

Note: On the McDATA site, the CIM agent is referred to as the SMI-S agent.

**Limitation for the McDATA switch:** If you are using a McDATA switch, the domain ID displayed by IBM Tivoli Storage Productivity Center has a different value from the one displayed by McDATA's management application. Tivoli Storage Productivity Center displays the domain ID on the Properties dialog for a selected switch or on the Zone dialog for zone control. The reason for this difference for the domain ID is because the Tivoli Storage Productivity Center API call to the McDATA switch has some additional encoded information in the high-order bits. For example, a McDATA switch with the domain ID of 1 (as displayed on McDATA's management application) is displayed as 97 (hexadecimal 61 where the 6 represents the high-order bit encoding information).

The McDATA CIM agent can be installed using direct connection mode, or use the Enterprise Fabric Connectivity Manager (orderable from McDATA).

If you use the direct connection mode, the McDATA CIM agent communicates directly with the SAN device. If you use the Enterprise Fabric Connectivity Manager, the McDATA CIM agent and device communicates only through the Enterprise Fabric Connectivity Manager.

If you use the Enterprise Fabric Connectivity Manager, these are the differences from using the direct connection mode:

- The CIM agent for McDATA always manages the same set of devices as those managed by Enterprise Fabric Connectivity Manager.
- The CIM agent for McDATA cannot add or delete a device from its list of managed devices. This must be done through the Enterprise Fabric Connectivity Manager. When Enterprise Fabric Connectivity Manager adds a device, that device is automatically added to the McDATA CIM agent. When Enterprise Fabric Connectivity Manager deletes a device, that device is automatically removed from the McDATA CIM agent.
- If Enterprise Fabric Connectivity Manager is running when the CIM agent for McDATA starts, any devices being managed by Enterprise Fabric Connectivity Manager are automatically added to the CIM agent.

**Limitation when running a CIMOM Discovery against a McDATA CIM agent:** When you run a CIMOM discovery against a McDATA CIM agent, the following switch information is collected:

- Manageable McDATA switches that exist in the fabric.
- Unmanageable switches that connect to the manageable McDATA switches. In a homogenous fabric, a McDATA switch is considered unmanageable when it is managed by an Enterprise Fabric Connectivity Manager (Proxy Mode) or a McDATA CIM agent (Direct Mode) other than the McDATA CIM agent against which you ran a CIMOM discovery. In a heterogenous fabric, unmanageable switch is either a non-McDATA switch or a McDATA switch which is managed by different Enterprise Fabric Connectivity Manager in proxy mode or different McDATA CIM agent in direct mode

You can use Tivoli Storage Productivity Center to view detailed information about the manageable McDATA switches and collect performance data about them. For unmanageable switches, you can use Tivoli Storage Productivity Center to view their WWN and port numbers which connect to manageable McDATA switches only, and you cannot collect performance data about them.

## **Configuring QLogic switches**

No special configuration is needed for QLogic switches.

**Note:** For QLogic switches, zone control is automatically disabled if one or more non-standard zones exist in the zoning definition.

## **CNT zoning considerations**

For CNT, the element manager is called the Enterprise Manager. Rather than storing the full zoning definition on the switches within a fabric, CNT switches store the full zoning definition on the CNT Enterprise Manager.

The full zone definition stored on the CNT Enterprise Manager is not just for a single fabric, but for ALL fabrics that are being managed by that Enterprise Manager. This is an extremely important point because you might have the intention of only changing the zoning definition on a single fabric, but could inadvertently change the zone definition on another fabric by modifying the wrong zone. For this reason you should manage different environments with different instances of the CNT Enterprise Manager. For example if you have a production and a test environment, you would want one instance of CNT Enterprise Manager for your production environment and one instance for your test environment. This will help to protect your production environment from inadvertent changes made to your test environment.

When performing zone control operations, the Enterprise Manager must be running or zone control within IBM Tivoli Storage Productivity Center will fail.

## Planning for performance management

IBM Tivoli Storage Productivity Center can collect performance data for devices (storage subsystems and fibre channel switches) with CIM agents that are SMI-S 1.1 compliant, and store the data in the database. Performance management is not available for IBM XIV Storage System

There are three main functions for Tivoli Storage Productivity Center performance management:

- Performance data collection (performance monitoring)
- Performance thresholds and alerts
- · Performance reports

You can define how long performance data is stored in the database. Tivoli Storage Productivity Center can set thresholds for important performance metrics. When any boundary condition is crossed, Tivoli Storage Productivity Center can notify the user through e-mail, SNMP, or other alerting mechanisms. Tivoli Storage Productivity Center can generate reports, historic trend charts, and help analyze the bottleneck of a performance congestion by drilling down to threshold violated components and the affected hosts. The combination of these functions can be used to monitor a complicated storage network environment, to predict warning signs of system fallout, and to do capacity planning as overall workload grows.

## **Performance metrics**

IBM Tivoli Storage Productivity Center can report on many different performance metrics, which indicate the particular performance characteristics of the monitored devices.

In principle, the two very important metrics for subsystems are throughput in I/O per second, and the response time in milliseconds. Throughput is measured and reported in several different ways. There is throughput of an entire box (subsystem), or of each cluster (Tivoli Storage Enterprise Storage Server) or controller (DS6000 or DS8000), or of each I/O Group (SAN Volume Controller). There are throughputs measured for each volume (or LUN), throughputs measured at the Fibre Channel interfaces (ports) on some of the storage boxes and on fibre channel switches, and throughputs measured at the RAID array after cache hits have been filtered out. Front-end I/O metrics are averages of all traffic between the servers and storage box, and account for relatively fast hits in the cache, as well as occasional cache misses that go all the way to the RAID arrays on the back-end. Back-end I/O metrics are averages of all traffic between the subsystem cache and the disks in the RAID arrays in the back-end of the subsystem. Most storage boxes give metrics for both kinds of I/O operations, front-end and back-end. Throughput and response time at the front-end is very close to the system level response time as measured from a server. Throughput and response time at the back-end is just between the server cache and disk.

**Note:** A CIMOM discovery and fabric probe is required for all switch vendors supporting SMIS 1.1 and higher.

The main front-end throughput metrics are:

- Total IO Rate (overall)
- Read IO Rate (overall)
- Write IO Rate (overall)

The corresponding front-end response time metrics are:

- Overall Response Time
- Read Response Time
- Write Response Time

The main back-end throughput metrics are:

- Total Back-end IO Rate (overall)
- Back-end Read IO Rate (overall)
- Back-end Write IO Rate (overall)

The corresponding back-end response time metrics are:

- Overall Back-end Response Time
- Back-end Read Response Time
- Back-end Write Response Time

It is desirable to track any growth or change in the rates and response times. It frequently happens that I/O rate grows over time, and that response time increases as the I/O rates increase. This relationship is what "capacity planning" is all about. As I/O rates increase, and as response times increase, you can use these trends to project when additional storage performance (as well as capacity) will be required.

Depending on the particular storage environment, it may be that throughput or response time times change drastically from hour to hour or day to day. There may be periods when the values fall outside the expected range of values. In that case, other performance metrics can be used to understand what is happening. Here are some additional metrics that can be used to make sense of throughput and response times:

- Total cache hit percentage
- Read cache hit percentage
- NVS full percentage
- Read transfer size (KB/operation)
- Write transfer size (KB/operation)

Low cache hit percentages can drive up response times, because a cache miss requires access to back-end storage. Low hit percentages will also tend to increase the utilization percentage of the back-end storage, which may adversely affect the back-end throughput and response times. High NVS full percentage (also known as write-cache delay percentage) can drive up the write response times. High transfer sizes usually indicate more of a batch workload, in which case the overall data rates are more important than the I/O rates and the response times.

All these metrics can be monitored through reports or graphs in the Tivoli Storage Productivity Center GUI. You can also monitor the thresholds for a few throughput metrics such as:

- Total I/O rate threshold
- Total back-end I/O rate threshold
- Overall back-end response time threshold

For switches, the important metrics are total port packet rate and total port data rate, which provide the traffic pattern over a particular switch port. When there are lost frames from the host to the switch port, or from the switch port to a storage device, the dumped frame rate on the port can be monitored.

The important things are:

- Monitor the throughput and response time patterns over time for your environment
- Develop an understanding of expected behaviors
- Investigate the deviations from normal patterns of behavior to get warning signs of abnormal behavior
- Generate the trend of workload changes

## Performance management configuration

Performance data can only be collected from devices managed by a CIM agent because the product uses the SMI-S interface for performance management.

You need to make sure the following items are done before adding the CIM agent:

- The version of CIM agent and firmware for the device is supported.
- A CIM agent is installed on a different server from IBM Tivoli Storage Productivity Center. For some switch vendors, the switch comes with an imbedded CIM agent, and therefore, no separate CIM agent installation is required.

- For subsystems or switches on a private network, be sure to have the CIM agent installed on a gateway machine so that the Tivoli Storage Productivity Center server on a different machine can communicate with the CIM agent.
- The CIM agent is configured to manage the intended device.

For information about how to install and configure the CIM agent, contact your CIM agent provider.

To get performance data, you must do the following general steps:

- 1. Add the CIM agent to Tivoli Storage Productivity Center.
- 2. Perform a CIMOM discovery operation for the subsystems or switches.
- **3.** Perform a probe job for the subsystems. This gets all component level information into the database. This includes getting all the instances of controllers, arrays, extents, volumes, LUN to host mappings, FC ports, and so forth. Only those subsystems for which configuration information has been collected successfully can have performance monitors run on them.
- 4. For fibre channel switches, perform a fabric probe job for the fabric the desired switch is contained in.
- 5. Create threshold alerts. A performance threshold is a mechanism by which you can specify one or more boundary values for various performance metrics, and can specify to be notified if any collected performance data violates these boundaries.

When thresholds are applied during the processing of data collection, a performance monitor for a device must be actively running for a threshold violation to be recognized. Chronologically, you would need to define the threshold alert before the performance monitor job starts.

- 6. Create a performance monitor job. Performance data collection is performed through a performance monitor job. This job can be run immediately, can be scheduled to run one time only, or can be scheduled to run repeatedly as desired. Only after the device has been probed successfully can a monitor job be run successfully. There are two types of performance monitor jobs: one for Disk Manager to collect subsystem performance data and one for Fabric Manager to collect switch performance data.
- 7. Check the performance monitor status. When the performance monitor job starts to run, you begin to collect performance data for the device or switch. You should check the status of the performance monitor job to make sure it runs and continues running.
- 8. Specify the retention period for the performance data. After the monitor job is created, you can configure how long to keep performance data. You can specify a retention period for collected sample data, for aggregated hourly data, and for daily data.

Sample data is the data that is collected at the specified interval length of the monitor job, for example, data is collected every five minutes.

For subsystems, the largest component is volume, and the largest performance sample data will be that of the volume. For switches, the performance data is proportional to the number of ports in a switch.

Here is a general formula you can use to estimate the amount of performance data that will be generated.

#### NumSS

Number of Tivoli Storage Enterprise Storage Server / DS6000/ DS8000 / SAN Volume Controller / BSP subsystems. NumSW

Number of switches.

NumV

Average number of volumes in Tivoli Storage Enterprise Storage Server / DS6000 / DS8000 / SAN Volume Controller / BSP.

NumPt

Average number of ports in a switch.

- **CR** Number of sample data collected per hour (for a sample interval of 5 minutes, this should be 60/5=12 samples).
- **Rs** Retention for sample data in days.
- **Rh** Retention for hourly summarized data in days.
- **Rd** Retention for daily summarized data in days.

Here are the formulas:

Storage subsystem performance sample data size =
NumSS \* NumV \* CR \* 24 \* Rs \* 200 bytes
Storage subsystem performance aggregated data size =
NumSS \* NumV \* (24 \* Rh + Rd) \* 200 bytes

Switch performance sample size = NumSw \* NumPt \* CR \* 24 \* Rs \* 150

Switch performance aggregated data size = NumSw \* NumPt \* (24 \* Rh + Rd) \* 150

## **Tivoli Provisioning Manager 5.1 for storage workflows**

IBM Tivoli Storage Productivity Center supports Tivoli Provisioning Manager 5.1 for storage workflows. For information about how to use storage workflows, see *IBM Tivoli Storage Productivity Center Workflow User's Guide*.

## Microsoft Cluster Server

Data Manager can monitor and report on Microsoft Cluster Server (MSCS) clustered nodes and cluster resource groups.

Microsoft Cluster Server (MSCS) is a built-in feature of Windows 2000 and Windows 2003. It is software that supports the connection of up to eight servers into a "cluster" for higher availability and easier manageability of data and applications. MSCS can automatically detect and recover from server or application failures. It can be used to move server workload to balance utilization and to provide for planned maintenance without downtime.

As with standard Windows clusters, you perform most of the configuration tasks, and also the management tasks, associated with Exchange clusters using the Cluster Administrator. Cluster Administrator is installed by default on servers that have Cluster Service installed.

You can also use Cluster Administrator to remotely administer a server cluster. Computers that are used to administer a server cluster remotely must be secure and restricted to trusted personnel.

When a cluster node is probed, there will be normal errors in the logs for the disks belonging to the cluster resource groups that are not currently hosted on this node.

For more information about MSCS, go to this Web site: http://www.nwnetworks.com/mscsbasics.htm.

When looking at an MSCS cluster problem, the current state of the clustering environment is often needed. Microsoft provides a tool to dump the MSCS cluster configuration into a set of files.

**Note:** The term "virtual servers" has been replaced with "cluster resource groups" in IBM Tivoli Storage Productivity Center. Microsoft still refers to "virtual servers."

## **Microsoft Cluster Server environment**

This topic provides information about IBM Tivoli Storage Productivity Center support in an MSCS environment.

Report information can include a clustered node's local resources as well as the resources in a cluster resource group. The Data agent is not cluster aware so the Data agent cannot run in the cluster resource group and fail over from one node to another. The Data agent supports failover of a clustered file system so that Tivoli Storage Productivity Center scan jobs can continue to work when the clustered file system has moved from one node to another. The Data agent running on the node hosting the cluster resource group will discover the resources on that cluster resource group. The Data agents need to be installed on every node in the cluster.

The following information lists the requirements for using the Data Server in an MSCS cluster environment.

#### Server requirements

Not applicable. The server component can be installed on a node in an MSCS cluster, but the Data Manager can only monitor and report on nodes that have an agent installed.

#### agent requirements

You must install the Data agents on all cluster nodes. The following clustered environments are supported:

- Windows 2000 Advanced Server (supports a two-node cluster)
- Windows 2000 Datacenter (supports a four-node cluster)
- Windows 2003 Server (supports a four-node cluster)
- Windows 2003 Server Enterprise Edition (supports an eight-node cluster)

**Note:** The agent component is not a cluster-aware application. An agent will not fail over between clustered nodes.

#### client requirements

Not applicable. The client component can be installed on a node in an MSCS cluster, but the Data Manager can monitor and report on only the nodes with an agent installed.

**Note:** The Data Server does not currently support the monitoring of clustered database application.

## Microsoft Cluster Server support

Use this information to plan for running IBM Tivoli Storage Productivity Center with MSCS.

## **Cluster resource groups**

A cluster resource group represents an MSCS entity.

You can configure MSCS into cluster resource groups. You can define resource group policies and attributes that dictate how MSCS manages resources to keep them highly available at different stages of cluster operation (startup, failover, and fallback). The types of resources you can put into clustered resource groups are:

#### Logical volumes

A set of logical partitions that MSCS makes available as a single storage unit that is, the logical volume is the "logical view" of a physical disk.

#### Filesystem

A filesystem is written to a single logical volume. Typically, you organize a set of files as a filesystem for convenience and speed in managing data.

#### Shared filesystems

A filesystem that resides entirely in a shared logical volume.

#### Physical disk

A physical disk.

Network name

A network name.

```
IP address
```

An IP address.

#### Reports

The asset reporting navigation tree will include a By Cluster report that shows the nodes and cluster resource groups in each cluster. The disks and file systems that are shared as clustered resources are associated with the cluster resource group and not with the node where they are hosted.

When generating reports, you can use the By Cluster report subtype wherever the By Computer subtype is available. The By Cluster report summarizes the results of the nodes and the cluster resource groups in the cluster.

#### Monitoring groups

When you create a monitoring group or create a data collection schedule, you can select individual nodes and cluster resource groups. You can create a file system monitoring group that includes clustered and non-clustered resources.

#### **Computer alerts**

You can register for cluster specific alerts that will notify you that your cluster has gone through a configuration change such as a cluster resource being added or removed. You can also register for an alert that will be triggered when a cluster resource group is moved. The same alert is used for a cluster resource group failover, cluster resource group fallback, and when the cluster resource group is manually moved to a new node.

Cluster alerts will not be triggered until the next time the cluster is probed.

## Upgrading agents in an MSCS cluster

The following steps should be followed when upgrading the Tivoli Storage Productivity Center agents in an MSCS cluster:

- Make sure that all agents in the cluster are configured to use the same port address.
- Use either the Tivoli Storage Productivity Center installation program or the graphical user interface to perform the agent upgrades.
- Do not probe or scan the agents in the cluster while the agent upgrade is in progress.
- Once all agents in the cluster have been upgraded successfully, create and run a new probe job on the cluster.

For more information about upgrading Tivoli Storage Productivity Center agents, see "Upgrading the IBM Tivoli Storage Productivity Center agents" on page 369.

## Installing MSCS support

Complete the following general steps to install MSCS support:

- 1. Make sure your MSCS environment is configured for Tivoli Storage Productivity Center support.
- 2. Install a Data agent on each node of the cluster. All agents in the cluster must be configured to use the same listening port.
- 3. Install a Fabric agent on any number of nodes in a cluster (optional).
- 4. Run a discovery job for the agent.
- 5. Add a Network Name resource with an IP address that can be contacted from the Tivoli Storage Productivity Center server.
- 6. Run a scan job for the agent.
- 7. Run a probe job for the agent.
- 8. View reports for the MSCS entities.
- 9. View the MSCS environment in the topology viewer.

## Planning for High-Availability Cluster Multi-Processing

IBM Tivoli Storage Productivity Center supports Data agents and Fabric agents installed on HACMP nodes. Use this information to configure the HACMP environment before using it with Tivoli Storage Productivity Center.

#### Cluster resource groups

A *cluster resource group* represents an HACMP entity.

You can configure HACMP into cluster resource groups so that they can be highly available. You can define resource group policies and attributes that dictate how HACMP manages resources to keep them highly available at different stages of cluster operation (startup, failover, and fallback). The types of resources you can put into clustered resource groups are:

#### Volume groups

A set of physical volumes that AIX treats as a contiguous, addressable disk region.

#### Logical volumes

A set of logical partitions that AIX makes available as a single storage unit that is, the logical volume is the "logical view" of a physical disk.

#### Filesystem

A filesystem is written to a single logical volume. Typically, you organize a set of files as a filesystem for convenience and speed in managing data.

#### Shared filesystems

A journaled filesystem that resides entirely in a shared logical volume.

#### Applications

Critical services that are accessible to users.

#### Service IP labels or addresses

A way to establish communication between client nodes and the server node. Services, such as a database application, are provided using the connection mode over the service IP label.

#### Tape resources

You can configure a SCSI or a Fibre Channel tape drive as a cluster resource in a non-concurrent resource group, making it highly available to two nodes in a cluster.

#### **Communication links**

You can define communication links as resources in an HACMP resource group.

## Support in an HACMP environment

Tivoli Storage Productivity Center supports Data agents and Fabric agents installed on HACMP nodes.

Tivoli Storage Productivity Center supports HACMP 5.3.0.4 or HACMP 5.4.0.1 or later. APAR IY87543 is required for HACMP 5.3.0.4. APAR IY87447 is required for HAMCP 5.4.0.1. Also check the HACMP version compatibility matrix on the support site at HACMP Version Compatibility Matrix.

## Planning for HACMP support

With HACMP, you can use the following types of configurations:

- HACMP with cluster resources groups that are nonconcurrent. Concurrent cluster resource groups are not supported.
- The following volume groups in an HACMP environment:
  - Standard volume groups
  - Enhanced concurrent-mode volume groups
  - Scalable volume groups

When you create an Tivoli Storage Productivity Center configuration, include the following agents:

• A Data agent, which must be installed on each node of the cluster. All agents in a cluster must be configured to use the same listening port. You must also have a cluster resource group (CRG) with at least one IP address that is accessible from the Tivoli Storage Productivity Center server if you plan to perform scans on the cluster resource group.

Each Data agent collects information about the local node and the clustered resources that are currently hosted on the node.

• The Fabric agent can be installed on any number of nodes in a cluster. The Fabric agent function remains unchanged.

The following operations are not supported:

- · Probing and scanning of clustered databases
- Reporting on cluster information when the cluster is configured to have concurrent cluster resource groups

### **Reports**

The asset reporting navigation tree will include a By Cluster report that shows the nodes and cluster resource groups in each cluster. The disks, volume groups, and file systems that are shared as clustered resources are associated with the cluster resource group and not with the node where they are hosted.

When generating reports, you can use the By Cluster report subtype wherever the By Computer subtype is available. The By Cluster report summarizes the results of the nodes and the cluster resource groups in the cluster.

#### Monitoring groups

When you create a monitoring group or create a data collection schedule, you can select individual nodes and cluster resource groups. You can create a file system monitoring group that includes clustered and non-clustered resources.

#### **Computer alerts**

You can register for cluster specific alerts that will notify you that your cluster has gone through a configuration change such as a cluster resource being added or removed. You can also register for an alert that will be triggered when a cluster resource group is moved. The same alert is used for a cluster resource group failover, cluster resource group fallback, and when the cluster resource group is manually moved to a new node.

Cluster alerts will not be triggered until the next time the cluster is probed.

## Installing HACMP support

Complete the following steps to install HACMP support:

- 1. Make sure your HACMP environment is configured for Tivoli Storage Productivity Center support.
- **2.** Create a service IP label for the CRG with an IP address that can be contacted from the Tivoli Storage Productivity Center server.
- **3**. Install a Data agent on each node of the cluster. All agents in the cluster must be configured to use the same listening port.
- 4. Install a Fabric agent on any number of nodes in a cluster (optional).
- 5. Run a discovery job for the agent.
- 6. Run a probe job on the agents.
- 7. Run a scan job on the agents.
- 8. Run a scan job on the cluster resource groups.
- 9. View reports for the HACMP entities.
- 10. View the HACMP environment in the topology viewer.

## **HACMP** environment

This topic provides information about IBM Tivoli Storage Productivity Center support in an HACMP environment.

IBM Tivoli Storage Productivity Center supports Data agents and Fabric agents installed on High-Availability Cluster Multi-Processing (HACMP) nodes. The Fabric agent can be installed on any number of nodes in the cluster, but the Data agent must be installed on every node in the cluster. Neither of the agents can be clustered, so they cannot be configured to fail over from one node to another. The Data agent collects information from the cluster when the node is probed and the information that is collected is available in the Data Manager and Disk Manager reports and the topology viewer. Resources that are not clustered are reported under the node and resources that are associated with a cluster resource group are reported under a computer entity that represents the cluster resource group. For example, if a single node cluster that has one cluster resource group is probed it will produce two computer entities in the Data Manager and Disk Manager reports and the topology viewer. Volume groups, NFS shares, and service IP labels that are associated with a clustered resource group can only be reported under the clustered resource group and not the node. Physical volumes, logical volumes, and file systems for clustered volume groups will also be reported under the cluster resource group. Scan and ping jobs can be created for a cluster resource group and these jobs will work regardless of which node is hosting the cluster resource group. Scan and ping requests for a cluster resource group are sent to the service IP label defined for the cluster resource group. Therefore, in order for these jobs to succeed the service IP label must be accessible from the Data server and the CRG must be online.

The following information lists the support requirements for an HACMP cluster environment.

#### Agent requirements

Each node in an HACMP cluster must have a Data agent installed. The Data Manager can only monitor and report on nodes that have a Data agent installed. All agents installed in a cluster must use the same port number to communicate with the IBM Tivoli Storage Productivity Center server. Agents in other clusters can be configured with a different port address, but all agents in the cluster must use the port address used by the other agents in that cluster.

Fabric agents are optional in an HACMP cluster. Fabric agents can be installed on any number of nodes in the HACMP cluster.

#### **Probe requirements**

Note that probes are not automatically executed in response to cluster events. Probes should be scheduled to run as appropriate for the needs of the environment.

#### Scan requirements

In order to perform scans on a cluster resource group, the cluster resource group must be configured with an IP address that the IBM Tivoli Storage Productivity Center server can communicate with. This is the IP address that is displayed in reports associated with HACMP clusters. If the server cannot contact this address once it has been configured, the server will try the next known address for the cluster resource group until it successfully contacts an IP address. **Note:** Cluster resource groups are now listed as computers in scan job results, and now have log files specific to the cluster resource group.

## NAS and NetWare support

This section provides information for the planning of NAS and NetWare support.

## Novell NetWare system requirements

This section provides information about the requirements for installing and running the Data Server in a Novell NetWare environment.

IBM Tivoli Storage Productivity Center supports Novell NetWare 5.1 or later.

For detailed information about configuring NetWare and Tivoli Storage Productivity Center, see http://www.redbooks.ibm.com/. Search for **sg247490**.

The requirements are as follows:

#### Server requirements

Not applicable. You cannot install the server on a Novell NetWare device.

#### Agent requirements

You must install the agent on a machine that meets these requirements:

- A supported Windows platform. To use the Data Server for retrieving storage information from the servers and volumes within the Novell Directory Services (NDS) trees, you must install the agent on a Windows computer or computers where a Novell NetWare client is already located. The Data Server gathers detailed storage information about the NetWare servers and volumes using native NetWare calls from the Windows computers.
- NetWare Client.
- Access to the Novell NetWare servers and volumes within your environment.

#### **Client requirements**

Not applicable. You cannot install the client component on a Novell NetWare device.

#### Novell NetWare

You must be running v5.1 or above of the Novell operating system. The Data Server is optimized for NetWare version 5.1 or above, which contains NDS.

## Network attached storage system requirements

This section provides information about the requirements for installing and running the Data Manager within a network attached storage (NAS) environment.

IBM Tivoli Storage Productivity Center supports the monitoring of the NetApp Data ONTAP.

To be supported, NAS devices other than Network Appliance Filers must meet the following criteria:

- If scanned from a UNIX agent, a NAS device must support Network File System (NFS) queries.
- If scanned from a Windows agent, a NAS device must support Common Internet File System (CIFS) queries.

- A NAS device must support SNMP queries (sysName and sysOID).
- A NAS device must supply a unique sysName.
- If a NAS device hosts both Windows and UNIX filesystems, you will need at least two proxy Data agents to monitor the device. At least one Windows proxy Data agent will be required to probe and scan the Windows CIFS shares, and at least one UNIX proxy Data agent will be required to probe and scan those UNIX NFS shares.

For detailed information about configuring NAS and Tivoli Storage Productivity Center, see http://www.redbooks.ibm.com/. Search for **sg247490**.

Here are the requirements for installing and running the Data Manager within a NAS environment.

#### Server requirements

Not applicable. You cannot install the server on a NAS filer.

#### Agent requirements

You must install the agent on a machine that has access to the NAS filers within your environment that you want to monitor.

#### Windows

The agent that is logging into and scanning the NAS filer is not required to be in the same domain as the user or the NAS filer. If you install the agent on a different domain from the NAS filer, the agent will scan the NAS filer *if* the domain of the agent computer is a "trusted domain" by the domain of the NAS filer.

#### UNIX and Linux

The agent computer must import the NAS filer's exports as NFS mounts (or automounts on Solaris).

#### Note:

- You do not install agents to the NAS filers themselves.
- For Tivoli Storage Productivity Center 5196 network attached storage 300 G machines only, install the agent directly on those machines. If the 300 G is clustered, you will need to install an agent on each local node.

#### **Client requirements**

Not applicable. You cannot install the client component to a NAS filer.

#### NAS requirements

The NAS filers within your environment must be visible to the machines where you install the agent or agents. If you want to monitor NAS filers from Windows, you must configure those NAS filers to be members of a Windows domain.

## Planning for NetApp device support

NetApp devices provide unified storage for organizations with network-attached storage or storage area network environments that have file and block-level services. IBM Tivoli Storage Productivity Center provides the same file and block-level support for NetApp devices as is provided for other filers and storage subsystem devices.

## **Overview**

Tivoli Storage Productivity Center provides the following support for NetApp devices:

- supports NetApp Data ONTAP SMI-S Agent 3.0
- supports the SMI-S 1.2 Array profile implemented by the NetApp SMI-S agent
- supports all filer models running NetApp Data ONTAP version 7.2 and 7.3

NAS Gateway and V Series are not supported with the Array profile.

The supported OS platforms for the Data agent are:

- Windows 32-bit
- Red Hat Linux 32-bit and 64-bit
- SuSE Linux 32-bit and 64-bit (9.0, 10.0, SLES 9)
- VMWare ESX Server version 3.5

The following licenses are required:

- For performance monitoring, a IBM Tivoli Storage Productivity Center for Disk license is required
- For SNMP discovery, a IBM Tivoli Storage Productivity Center Standard Edition license is required

## **Configuration considerations**

The way you use Tivoli Storage Productivity Center to interact with NetApp devices, and the data you can collect for NetApp devices, depends on how you configure your NetApp devices. For example:

- if you configure a Data Manager agent to be a Scan/Proxy agent, you use Data Manager to work with NetApp devices. The Data Manager user interface displays a NetApp filer as a "computer". For NetApp devices configured this way, Tivoli Storage Productivity Center collects file storage information.
- if you configure a NetApp SMI-S agent (CIMOM), you use Disk Manager to work with NetApp devices. The Disk Manager user interface displays a NetApp device as a "subsystem". For NetApp devices configured this way, Tivoli Storage Productivity Center collects block storage information.
- if you configure a NetApp device as both a filer and a subsystem, Tivoli Storage Productivity Center collects both file and block storage information. You can use Disk Manager and Data Manager to work with the NetApp device. Keep in mind that the Data Manager user interface displays a NetApp filer as a "computer," and the Disk Manager user interface displays a NetApp device as a "subsystem".

If you initially configure a NetApp device using a data agent, you will not lose any functionality if you later decide to also configure the NetApp device using a CIM agent.

## General procedure to install and configure NetApp devices

The general steps to install and configure a NetApp device to enable Data Manager functionality are:

1. Select a machine to act as the Data Manager agent that meets the auto-discovery requirements for Tivoli Storage Productivity Center to auto-discover the NetApp filers.

- 2. Install a Data Manager agent on that machine.
- 3. Set the license for the NetApp filers that are discovered.
- 4. Set the Scan/Proxy agent for the discovered filers.
- 5. Create and run a probe job for each of the filers to collect Data Manager information.

The general steps to install and configure a NetApp device in order to enable Disk Manager functionality are:

- 1. Install Tivoli Storage Productivity Center or upgrade to version 4.1 or later.
- 2. Install the NetApp SMI-S agent and add filers to its configuration using the NetApp SMI-S agent utility
- Add the NetApp CIMOM by using Administrative Services>Data Sources>CIMOM Agents:Add CIMOM. To automatically discover the NetApp SMI-S agent using SLP, skip this step.
- 4. Run a CIMOM discovery.
- If you want to use SLP to discover the NetApp SMI-S agent, make sure your SLP directory agents are configured or the Scan local subnet box is checked on the Administrative Services>Discovery>CIMOM>Options panel before you run the discovery.
- **6**. Create and run a probe job for the configured filers to collect Disk Manager information.
- 7. If desired, use the command-line interface (CLI) tpctool command to view information for NetApp storage subsystems.

Refer to the *IBM Tivoli Storage Productivity Center User's Guide* for more information on how to collect and view information gathered by NetApp devices. Refer to the *IBM Tivoli Storage Productivity Center Command-Line Interface Reference* for information about using the tpctool command.

## Removing a NetApp device

If you later decide to remove a NetApp device, the steps to remove it depend on how you configured it. For example, if the NetApp device is configured only as a filer, you can remove it using the **Administrative Services>Configuration>Scan/ Probe Agent Administration** panel. If the NetApp device is configured only as a subsystem, you can remove it using the **Disk Manager>Storage Subsystems** panel. If the NetApp device is configured as both a filer and a subsystem, then you must perform both of the preceding steps.

## Limitations of NetApp support

Keep in mind the following limitations for NetApp support:

- The NetApp Data ONTAP SMI-S Agent 3.0 implements the Block Server Performance subprofile. It provides volume performance data but, for now, does not provide performance data at the storage subsystem level.
- Tivoli Storage Productivity Center supports only the SMI-S Array profile of the NetApp Data ONTAP SMI-S Agent. Other SMI-S profiles, including the self-contained NAS profile and the NAS Head profile, are not supported.
- For the Data ONTAP SMI-S 3.0 agent, if a volume is offline, the performance monitor might fail with the message: PM HWNPM2132W Performance data could not be collected for device <device>.

• To work with Network Appliance quotas (using **Data Manager>Policy Management>Network Appliance Quotas**), the NetApp device must be configured as a filer. This functionality is not available if the NetApp device is configured only as a CIMOM.

## Identifying NetApp devices in the user interface

The way you configure a NetApp device determines how the NetApp device is represented in the Tivoli Storage Productivity Center user interface, as follows:

- NetApp device configured as a filer: the NetApp device appears as a "computer" in the user interface.
- NetApp device configured as a storage subsystem using a CIMOM: the NetApp device appears as a "subsystem" in the user interface.
- NetApp device configured as both a filer and storage subsystem: the NetApp device appears as either a "computer" or a "subsystem" in different places in the user interface. For example, some reports under My Reports refer to the NetApp filer as a "computer" while others refer to the NetApp device as a "subsystem".

The locations in the user interface where the NetApp device will either be represented as a "computer" or a "subsystem", or both, depending on how you have configured the NetApp device, are:

- Dashboard
- My Reports
- Topology viewer
- Alerting
- Data Manager
- Disk Manager

#### For example:

- Data Manager>Reporting>Asset>By Storage Subsystem lists a NetApp device as a storage subsystem if the device was probed by the NetApp Data ONTAP SMI-S agent.
- System Reports>Data>Disk Defects displays a NetApp device name as either a "computer" or a "subsystem", depending on whether the device information was collected by the data agent or the SMI-S agent

In the topology viewer, the NetApp device appears as follows:

- If a data agent is configured to probe the NetApp device, the NetApp device will be displayed as a "computer"
- If a CIM agent is configured to probe the NetApp device, the NetApp device will be displayed as a "storage subsystem"

## Planning for IBM System Storage N Series Gateway servers

IBM Tivoli Storage Productivity Center supports the IBM System Storage N Series Gateway servers as the **Other NAS** node.

#### Upgrade information

If you are upgrading IBM Tivoli Storage Productivity Center from IBM TotalStorage Productivity Center 3.3.x, there are specific steps to follow. You must delete and un-license existing N Series Gateway servers first before adding the N Series Gateway servers. For information about upgrading IBM Tivoli Storage Productivity Center with N Series Gateway servers, see "Configuring IBM System Storage N Series Gateway servers" on page 377.

#### New installation

If you are installing IBM Tivoli Storage Productivity Center as a new installation, the N Series Gateway servers can be automatically discovered after the Data agent is installed. If the N Series Gateway servers are automatically discovered, they will be listed under Administrative Services > Configuration > License Keys for IBM TPC for Data's Licensing tab as NetApp Data ONTAP with the Licensed box unchecked.

To manually add the N Series Gateway servers as **Other NAS**, the Licensed box must be unchecked. The OS Type and Licensed fields will be updated after the N Series Gateway Server is manually added as **Other NAS**. For more information, see "Manually adding an N Series Gateway server " on page 378.

## Planning for VMware

IBM Tivoli Storage Productivity Center supports the VMware Virtual Infrastructure which consists of the ESX Server and VMware VirtualCenter.

#### Overview

The ESX Server is a true hypervisor product which can host multiple virtual machines that run independently of each other while sharing hardware resources. The VirtualCenter is the management application that is the central entry point for the management and monitoring of a data center's ESX Servers. You would install a Data agent on each virtual machine that you want to monitor.

For more information about the ESX Server or VMware VirtualCenter, see http://www.vmware.com.

The storage subsystems supported through VMware are:

- IBM DS4000
- IBM DS6000
- IBM DS8000
- SAN Volume Controller
- Enterprise Storage Server (Tivoli Storage Enterprise Storage Server)
- IBM XIV Storage System
- Hewlett Packard Enterprise Virtual Arrays (EVA)
- Hitachi Data Systems 9xxxx
- EMC Symmetrix
- EMC CLARiiON
- 3PAR

For full functionality, both the Data agent and Virtual Infrastructure must be up and running. If one of the items is not present in a given environment, only a limited picture is presented to the user (some virtual machines might not be recognized).

The hierarchical mapping of storage allocated to the virtual machine will be available for the virtual machines on the ESX Server.

**Note:** Tivoli Storage Productivity Center now supports the mapping of storage from the ESX Server to the disk drives for the ESX Server 3.5.

Note the following limitations:

- No HBA virtualization is available for the VMware virtual machines. Therefore, if you install a Fabric agent on a VMware virtual machine, the Fabric agent will not be useful.
- No events directly generated by the Virtual Infrastructure will be supported.
- No VMware clusters will be supported.
- Data path explorer is not supported for VMware ESX Server and virtual machines.

#### Software requirements

Use this information to help you plan for your ESX Server or VMware VirtualCenter environment.

Tivoli Storage Productivity Center supports the following ESX Servers and VirtualCenter:

- ESX Server 3.0.1 or later (LUN correlation is not supported)
- VMware VirtualCenter 2.0.1 or later (LUN correlation is not supported)
- ESX Server 3.5 or later (LUN correlation is supported)
- ESX Server 3.5 3i or later (LUN correlation is supported)
- VMware VirtualCenter 2.5 or later (LUN correlation is supported)

The supported guest operating systems that can be run on a virtual machine are those that are supported both by the Data agent and ESX Server. The supported operating systems are:

- Windows Server 2003 Standard and Enterprise Editions with service pack 1
- Windows 2000 Advanced Server
- Red Hat Enterprise Linux Advanced Server 3.0 and 4.0 with the following updates:
  - Updates 4, 5, 6, and 7 for 32-bit machines
  - Updates 4, 5, 6, and 7 for 64-bit machines
- SUSE Linux Enterprise Server 8 and 9 with the following service packs:
  - Service packs 1, 2, and 3 for 32-bit machines
  - Service packs 1, 2, and 3 for 64-bit machines
- SUSE Linux Enterprise Server 8 with service packs 1, 2, 3, and 4

## Installing Tivoli Storage Productivity Center server on a virtual machine

You can install the Tivoli Storage Productivity Center server on a virtual machine on VMware ESX server 3.5.x. The hardware and operating system requirements are the same requirements as for a physical machine.

In addition, the following requirements must be met:

**CPU** For the ESX server, do not have more virtual CPUs than there are physical cores in the system. Plan your system so that no CPU scheduling is required by the VM kernel for the virtual machine.

- **RAM** Ensure that you have enough RAM in the ESX server to service all the virtual machines with a maximum RAM usage. Plan your system so that the ESX server does not need to swap RAM for the virtual machine.
- **Disk** Use the SAN-attached RDM with SCSI pass-through for DB2 data and log storage.

For more information about VMware, see the following publications:

- "Using VMware ESX Server with IBM WebSphere Application Server" at http://www.vmware.com/partners/vmware/ESX\_WAS\_WP.pdf.
- Scaling IBM DB2 9 in a VMware Infrastructure 3 Environment" at http://www.vmware.com/pdf/db2\_scalability\_wp\_vi3.pdf.

## VMware configuration

Before you can display reports or see the topology for VMware Virtual Infrastructure, you must configure the VMware environment.

You must complete the following general steps:

- 1. If the VMware Virtual Infrastructure uses SSL certificates for communication, you will have to use **keytool** to manually import the SSL certificates into a truststore. Each Virtual Infrastructure data source provides an individual certificate. There will be a default truststore registered in the Device server's system properties file. **Keytool** is a tool shipped with the Java run-time environment. For information about how to import the SSL certificates, see "Importing SSL certificates for VMware" on page 489.
- 2. Add the VMware VI data source. The data source can be a hypervisor (ESX Server or VirtualCenter). This is the first step in getting information from VMware Virtual Infrastructure. Adding a VMware data source is similar to adding a CIM agent or Data agent.
- **3**. Test the connection to the VMware VI data source. This ensures that you can access information from the VMware data source.
- 4. Run a discovery job for the VMware environment. The discovery is needed to retrieve every ESX Server instance that is part of the Virtual Infrastructure that has been added. The discovery mechanism is similar to a discovery for storage subsystems. Discovery jobs can be scheduled and are performed on the complete list of known VMware data sources.
- 5. Run a probe job for the ESX Server, hypervisor, and virtual machines. This step will get the detailed information from the hypervisors and virtual machines for IBM Tivoli Storage Productivity Center.
- **6**. Configure alerts for VMware. You can create alerts for the following alert conditions:
  - Hypervisor discovered
  - Hypervisor missing
  - Virtual Machine added
  - Virtual Machine deleted
- 7. Install the Data agent on each of the virtual machines you wish to monitor. For full functionality, you need two data sources.
- 8. You will now be able to view VMware reports and VMware topology.

## VMware capacity reports

You must probe both the ESX Server and the Data agent in the virtual machines before you can generate accurate reports for disk and file system capacity.

If you have an ESX Server that has 100 GB and 60 GB is allocated to the virtual machine. The virtual machine uses 5 GB of space. Both the ESX Server (H1) and the virtual machine (VC1) have been probed. You also have a physical computer (PC1) that has been probed. The TOTAL capacity for the file system or disk capacity row includes everything - virtualized disks and virtual machines as well as non-virtualized disks and machines.

Column heading	Capacity	Used Space (this is calculated as capacity minus free space)	Free Space
TOTAL	130 GB	25 GB	105 GB
H1	100 GB	60 GB	40 GB
VC1	60 GB	5 GB	55 GB
PC1	30 GB	20 GB	10 GB

If you have probed the PC1 (physical computer) and VC1 (virtual computer) but have not probed the ESX Server (hypervisor), the capacity will be shown as follows:

	<i>c i</i>	Used Space (this is calculated as capacity minus free space, any negative values will be	F - 0
Column heading	Capacity	represented as 0)	Free Space
TOTAL	30 GB	0 GB	65 GB
PC1	30 GB	20 GB	10 GB
VC1	60 GB	5 GB	55 GB

If you have probed the hypervisor (H1) and PC1 (physical computer) but have not probed the VC1 (virtual computer), the capacity will be shown as follows:

Column heading	Capacity	Used Space (this is calculated as capacity minus free space)	Free Space
TOTAL	130 GB	80 GB	50 GB
H1	100 GB	60 GB	40 GB
PC1	30 GB	20 GB	10 GB

## Planning for the Virtual I/O Server

You can use IBM Tivoli Storage Productivity Center agents to gather information about Virtual I/O Servers. Before you can monitor Virtual I/O Servers, you must plan on how to install the agents in your environment.

## **Overview**

The Virtual I/O Server is part of the IBM System p Advanced Power Virtualization hardware feature. The Virtual I/O Server allows the sharing of physical resources

between LPARs including virtual SCSI and virtual networking. This allows more efficient utilization of physical resources through sharing between LPARs and facilitates server consolidation.

#### Login requirements

Use the **padmin** user ID when logging into a Virtual I/O Server, **padmin** is the main administrator ID for Virtual I/O Servers. Upon login, a password change is required. There is no default password to remember.

The Virtual I/O Server does not support users logging in as root to install or configure Tivoli Storage Productivity Center agents. However, you can debug errors generated by agents as a root user. For example, you can run the service.sh script to gather debugging information.

Upon logging into the Virtual I/O Server, you will be placed into a restricted Korn shell. The restricted Korn shell works the same way as a regular Korn shell, except you cannot:

- Change the current working directory.
- Set the value of the SHELL, ENV, or PATH variable.
- Specify the path name of the command that contains a redirect output of a command with a >, > | , <>, or >.

As a result of these restrictions, you cannot run commands that are in locations not defined in your PATH variable. These restrictions prevent you from directly sending the output of the command to a file, instead requiring you to pipe the output to the **tee** command.

#### Installation requirements

A script enables you to silently install the Data and Fabric agents on a Virtual I/O Server. The script is run when you run the **cfgsvc** command. The script is located on the Tivoli Storage Productivity Center disk2 image for the agents. You must use the **padmin** user ID to perform the following actions:

- Install the Data agent and Fabric agents.
- Run the commands to configure, start and stop the agents.

These are the installation requirements:

- Tivoli Storage Productivity Center supports Virtual I/O Server version 1.5.2 or later.
- The Virtual I/O Server for POWER5 processor-based systems, must have a minimum of 512 MB of memory.
- The Virtual I/O Server for POWER6 processor-based systems, must have a minimum of 768 MB of memory.
- In addition to the memory required by Virtual I/O Server, the Tivoli Storage Productivity Center agent on Virtual I/O Server must have a minimum of 1 GB of memory.
- Ensure there are no other operations running on the Virtual I/O Server when installing the agents. The machine that is running the Tivoli Storage Productivity Center agents require 100 % of CPU time.

## **Upgrade requirements**

Once installed on a Virtual I/O Server, you cannot upgrade the Data and Fabric agents locally because of restrictions on the shell of the **padmin** user ID. However, you can upgrade them in the following ways:

- Upgrade Data agents using the Administrative Services > Configuration > Data Agent Upgrades window in the Tivoli Storage Productivity Center user interface.
- Upgrade Fabric agents using remote fabric deployment in the Tivoli Storage Productivity Center installation program.

## General procedure to install and configure agents

The general steps to install and configure the agents on the Virtual I/O Server are:

- 1. Install Tivoli Storage Productivity Center or upgrade to 4.1 or later.
- 2. Install and configure the agents on the Virtual I/O Server by running the **cfgsvc** command.
- 3. When you install the agents, they are automatically started
- 4. Run a discovery job for the agents on the Virtual I/O Server.
- 5. Collect information about a Virtual I/O Server by running probes, scans, and ping jobs.
- 6. View the storage information gathered by the monitoring jobs through the topology viewer and reports that you can generate through Fabric Manager and Data Manager.

See the *IBM Tivoli Storage Productivity Center User's Guide* for more information on how to use the Tivoli Storage Productivity Center user interface to collect and view information gathered by agents on Virtual I/O Servers.

## Support for Virtual I/O Servers

This topic provides information about IBM Tivoli Storage Productivity Center's support of AIX Virtual I/O Servers.

Use Tivoli Storage Productivity Center agents to collect data about Virtual I/O Servers. Tivoli Storage Productivity Center agents are pre-installed on Virtual I/O Servers but you must configure and start those agents before you can run monitoring jobs to collect data. See "Administering agents on the Virtual I/O Server" on page 461 for more information.

After the agents are configured and running, you can perform the following actions:

- Run probes and scans to collect data about a Virtual I/O Server and the clients connected to it.
- Enforce storage policies using quotas, constraints, and scheduled actions.
- View data collected by agents in Tivoli Storage Productivity Center reports and the Topology viewer.

Some of the data collected by agents includes:

- For Virtual I/O Server client partitions:
  - File system storage resources, such as space allocated and space available (probes)
  - File storage usage and trending (scans)

- Database storage resources, usage, and trending (probes and scans).

#### Note:

- Tivoli Storage Productivity Center does not collect data about the client partitions to the Virtual I/O Server storage relationships. Information about the mapping between the disks on the client partitions and Virtual I/O Server storage is not available.
- Tivoli Storage Productivity Center does not determine whether disks on two client partitions are shared Virtual I/O disks. Therefore, the HACMP support implemented in Tivoli Storage Productivity Center does not function correctly if the HACMP software is installed on two client partitions.
- For Virtual I/O Server partitions:
  - File system storage resources, such as space allocated and space available (probes)
  - File storage usage and trending (scans)
  - Connectivity to HBAs and SAN Fabric and disks (probes)
  - Storage subsystem storage resources (probes)

**Note:** We do not recommend installing a database on a Virtual I/O Server as it could impact the performance of client partitions.

- View the data collected by probes and scans in the following reports:
  - Data Manager > Reporting:
    - Asset reports
    - TPC-wide Storage Space reports
    - Usage reports
    - Monitored Computer Storage Space reports
  - Disk Manager > Reporting > Storage Subsystems
  - IBM Tivoli Storage Productivity Center > Topology:
    - Computers view
    - Storage view
    - Data Path Explorer view

## Planning for the universal agent

A universal agent for IBM Tivoli Storage Productivity Center is available to report Tivoli Storage Productivity Center asset information to IBM Tivoli Monitoring. This data is available for display in the Tivoli Enterprise Portal for reporting, charting, and establishing situations in Tivoli Monitoring.

For more information about IBM Tivoli Monitoring and Tivoli Enterprise Portal, see http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?toc==/ com.ibm.itm.doc/toc,.xml

The universal agent is located in the following Tivoli Storage Productivity Center directory:

- For Windows: <TPC\_install\_dir>\tool\TPCUA.zip>
- For UNIX and Linux: /<opt or usr>/tool/TPCUA.tar

The zip or tar file contains a readme file that describes how to install and configure the universal agent.

## **IBM Tivoli Storage Productivity Center installation**

Use this information to learn about the steps required to install IBM Tivoli Storage Productivity Center as a new installation.

#### **Overview**

When you install Tivoli Storage Productivity Center, you will also be installing IBM Tivoli Integrated Portal and IBM Tivoli Storage Productivity Center for Replication.

External non-WebSphere applications will authenticate single sign-on users using IBM Embedded Security Services version 6.2 or later, which is contained within IBM Tivoli Integrated Portal. The Embedded Security Services server is basically a wrapper around the Virtual Member Manager component of the IBM Tivoli Integrated Portal WebSphere instance. The Embedded Security Services server is used as the single point of authentication for multiple non-WebSphere applications within a single sign-on environment.

The Tivoli Storage Productivity Center user interface can be launched from IBM Tivoli Integrated Portal using a Web browser and Java Web Start. When you launch the Tivoli Storage Productivity Center user interface via Java Web Start, the user interface is downloaded from the Java Network Launching Protocol (JNLP) servlet within the Tivoli Storage Productivity Center Device server. Once downloaded, the user interface opens a new window.

When you install Tivoli Storage Productivity Center, you can specify a location to install a new instance of Tivoli Integrated Portal or you can reuse an existing Tivoli Integrated Portal instance, as long as its authentication mechanism is the operating system or an LDAP-compliant repository.

When you install Tivoli Storage Productivity Center and Tivoli Integrated Portal, you can elect to use the operating system (OS) or an LDAP-compliant directory as the centralized authentication repository. If you select local OS authentication, then no other Tivoli Integrated Portal-based product will be supported in this instance of Tivoli Integrated Portal.

For more information about IBM Tivoli Integrated Portal, see https:// publib.boulder.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.tip.doc/ welcome\_tip\_ic.htm.

#### Fully-qualified host names

Tivoli Storage Productivity Center requires fully-qualified host names. Some systems might be configured to return a short host name, such as ddunham instead of a fully-qualified host name, such as ddunham.myorg.mycompany.com. Tivoli Storage Productivity Center should only be installed on a computer that has a fully-qualified host name. If you install Tivoli Storage Productivity Center on a system without a fully-qualified host name, the installation might appear to be successful but the single sign-on feature for Tivoli Integrated Portal, Tivoli Storage Productivity Center, and Tivoli Storage Productivity Center for Replication might fail to operate. For information about fully-qualified host names, see "Checking for a fully qualified host name" on page 487.

## Procedure

If you are installing Tivoli Storage Productivity Center as a new installation, follow these general steps:

- 1. Install DB2 V9.5. See "Installing DB2" on page 121.
- 2. If you want to use the agents, install Agent Manager now or later. To install the Agent Manager, see "Installing the Agent Manager" on page 131.

**Note:** If you have an Agent Manager in your environment, you do not have to install another Agent Manager.

**3**. Install Tivoli Storage Productivity Center 4.1. See "Installing the IBM Tivoli Storage Productivity Center family" on page 165.

If you installed the Agent Manager, install the agents. See "Installing the agents" on page 241.

# Upgrading and migrating the IBM Tivoli Storage Productivity Center family

You can upgrade previous TotalStorage Productivity Center 3.1.3 or later releases to Tivoli Storage Productivity Center version 4.1. You can migrate previous IBM TotalStorage Productivity Center for Replication version 3.x to Tivoli Storage Productivity Center version 4.1. This section provides information about upgrading and migrating.

## Overview

When you upgrade Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication, if a component fails to upgrade, then just the component will not be upgraded.

If Tivoli Storage Productivity Center exists but Tivoli Storage Productivity Center for Replication does not, then this upgrade will be a fresh installation of Tivoli Storage Productivity Center for Replication and an upgrade of Tivoli Storage Productivity Center. If a failure occurs, an error message will be displayed but there will be no rollback.

If Tivoli Storage Productivity Center for Replication exists and Tivoli Storage Productivity Center does not, then this upgrade will be a fresh installation of Tivoli Storage Productivity Center and an upgrade of Tivoli Storage Productivity Center for Replication. If there is a failure in the Tivoli Storage Productivity Center installation, a rollback will occur of Tivoli Storage Productivity Center (Tivoli Storage Productivity Center for Replication will still remain).

Tivoli Storage Productivity Center for Replication is no longer a stand-alone application. Tivoli Storage Productivity Center Version 4.1 now installs Tivoli Integrated Portal and Tivoli Storage Productivity Center for Replication Version 4.1.

## Upgrading and migrating Tivoli Storage Productivity Center

All PTFs and patches use the upgrade procedure to install Tivoli Storage Productivity Center and do not require you to run the migration tool. You must have a valid Tivoli Storage Productivity Center license to use the upgrade procedure. For information about PTFs and patches, go to http://www.ibm.com/

## systems/support/storage/software/tpc/. Click **IBM Tivoli Storage Productivity Center for Data.** Click **Download**. Click **Downloadable files**.

If you are upgrading from one license to a higher-level license, for example, you have IBM Tivoli Storage Productivity Center Basic Edition installed and want to upgrade to IBM Tivoli Storage Productivity Center Standard Edition, you must first install the IBM Tivoli Storage Productivity Center Standard Edition license, then you can upgrade the product.

#### Note:

#### IPv6

You can upgrade an existing version of Tivoli Storage Productivity Center on an IPv4-only computer for use on a computer that is configured for both IPv4 and IPv6 (dual stack). You cannot upgrade Tivoli Storage Productivity Center on an IPv4-only computer for use on a computer that is configured for IPv6 only. If you want to use Tivoli Storage Productivity Center on an IPv6-only computer, you must perform a new install of the product on that computer.

#### Agent Manager and agents

Agent Manager version 1.3.2 is available for use with Tivoli Storage Productivity Center 4.1. If you have Agent Manager 1.2, it is optional to upgrade to V1.3.2. Note that the common agents remain at release 1.2 and is compatible with Agent Manager 1.3.2. If this is a new installation of Tivoli Storage Productivity Center, then you can optionally install Agent Manager version 1.3.2 as part of the new Tivoli Storage Productivity Center environment.

If you install an agent locally through the Tivoli Storage Productivity Center installation program, and a Common agent already exists on the system, the Common agent will be upgraded from version 1.2.2 to version 1.2.3.

**Note:** If you have Agent Manager 1.2.3 and it is running well, do not upgrade Agent Manager.

#### Upgrading database schema

If you are upgrading the database schema from TotalStorage Productivity Center 3.3.x to Tivoli Storage Productivity Center 4.1 on Windows Server 2003, there is an issue with the maximum size of environment variables like the PATH variable. The maximum size of the PATH variable is 2048 . However, in some cases, the PATH variable is truncated to 1024 characters. You need to install a hot fix from Microsoft. For information about the hot fix, go to http://support.microsoft.com/kb/906469.

#### Upgrading the Tivoli Storage Productivity Center license

For information about upgrading the Tivoli Storage Productivity Center installation license, see "Adding an installation license" on page 240.

## **Database migration tool**

After you perform the upgrade operation, you must migrate the Tivoli Storage Productivity Center database using the database migration tool (**partitiontables.bat** or **partitiontables.sh**). The Tivoli Storage Productivity Center version 4.1 database has been changed to improve performance of some queries by either partitioning some databases or including multidimensional clustering. These changes are automatically included when you install Tivoli Storage Productivity Center (but the Tivoli Storage Productivity Center version 3.x database is not migrated at this time). Because the database migration tool can take a long time to run (depending on the size of the database to be migrated), you can run the migration tool at a time that is convenient for you. You only have to run the database migration tool one time. You must run the database migration tool before you apply any patches or PTFs for Tivoli Storage Productivity Center.

When you run the database migration tool, you can check the progress of the database migration in the migrateTable.log file in the <TPC\_install\_directory>\ data\server\tools directory. You will see warning messages if the migration cannot be performed on the database or if the migration has been previously completed. The database migration tool prints out messages indicating which table is currently being migrated and which subsystem ID is currently being migrated. The database migration tool can be run more than once if an error occurred during execution. Tables that were migrated during previous attempts will not be migrated in subsequent runs.

## InstallShield limitations

These are some limitations you might encounter when installing Tivoli Storage Productivity Center:

- When running the Tivoli Storage Productivity Center installation program on Solaris systems, some of the graphical elements in the installation panels might not display correctly. For example, in the Select the type of installation you want to run panel, the TPC Installation Location button might appear truncated. This is due to an InstallShield limitation on Solaris systems.
- When using the Tivoli Storage Productivity Center installation program to install IBM Tivoli Integrated Portal on AIX systems, the progress bar incorrectly indicates that IBM Tivoli Integrated Portal installation is 100% complete even though it is not yet complete. You must continue to wait until installation is complete. This is due to an InstallShield limitation on AIX systems that prevents the progress bar from correctly reflecting the installation progress.
- When you install Tivoli Storage Productivity Center on AIX, the progress bar can incorrectly display 100% for any component that is installed even though the installation is not complete. This does not affect the installation.
- When you are upgrading the system, you might see several windows prompting you with the text **Replace Existing File**. Reply **Yes to All** to these prompts.

## Upgrading IBM Tivoli Storage Productivity Center from 3.x

If you are upgrading IBM Tivoli Storage Productivity Center from version 3.x, follow these general steps.

You can upgrade the following TotalStorage Productivity Center releases to Tivoli Storage Productivity Center version 4.1:

- TotalStorage Productivity Center version 3.1.3 or later to 4.1.
- TotalStorage Productivity Center for Replication version 3.x to 4.1. For information about upgrading, see "Migrating IBM Tivoli Storage Productivity Center for Replication from V3.x to V4.1" on page 348.

Follow these general steps to upgrade:

1. If you are using DB2 version 8, you must migrate to DB2 version 9.5. See "Migrating the database repository" on page 349.

2. If you have Agent Manager 1.2, you can optionally upgrade to Agent Manager 1.3.2. See "Upgrading Agent Manager" on page 360.

Note: If your Agent Manager 1.2 is running fine, do not upgrade.

- **3.** Upgrade Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication to version 4.1. See "Upgrading and migrating the IBM Tivoli Storage Productivity Center family" on page 111.
- 4. Migrate the Tivoli Storage Productivity Center database.

# Planning for SQL access to IBM Tivoli Storage Productivity Center's views

Use this topic for planning to retrieve storage information that is stored in the Tivoli Storage Productivity Center database repository.

Tivoli Storage Productivity Center stores the information collected by data collection jobs in its DB2 database repository. The information in the database repository is organized into a set of tables. A view is a way of describing data that exists in one or more of these tables.

You can use the Structured Query Language (SQL) to retrieve the information from these views and then use that information in reports and applications outside of Tivoli Storage Productivity Center, such Business Intelligence and Reporting Tools (BIRT), Microsoft Excel, and Crystal Reports. Other applications can also use these views to gather and import information that is collected by Tivoli Storage Productivity Center.

The views are created within a DB2 schema when you install the Tivoli Storage Productivity Center server. A schema defines the views and the fields within each view. The name of the schema containing the views for Tivoli Storage Productivity Center is TPCREPORT. To view this schema using the DB2 Control Center, complete these steps:

- 1. Start the DB2 Control Center.
- 2. Expand **All Databases** > **TPCDB** in the left pane.
- 3. Click Schemas.
- 4. Click **TPCREPORT** in the right pane.

Before you can work with the data stored in views, keep in mind the following planning considerations:

- A view is a logical table that consists of data that is generated by a query. A view is based on an underlying set of base tables in the database repository, and the data in a view is determined by a SELECT statement that is run on the base tables. See "SQL access to IBM Tivoli Storage Productivity Center's views" on page 616 for more information about Tivoli Storage Productivity Center views and how to retrieve information from them.
- The views are available in Tivoli Storage Productivity Center version 4.1 or higher. If you want to retrieve data from the database repositories of previous versions of the product, you must first upgrade to version 4.1 or higher. See "Upgrading and migrating the IBM Tivoli Storage Productivity Center family" on page 111 for information about how to upgrade Tivoli Storage Productivity Center.
- You must run data collection jobs to collect data about the storage resources in your environment before you can retrieve data from views. The data collected

by probes, scans, pings, switch performance monitors, and subsystem performance monitors populates those views.

- You must have proper authority to access and retrieve data from the views. The views can be accessed by the following users:
  - DB2 administrator
  - The DB2 user that Tivoli Storage Productivity Center uses to store and retrieve information in the database repository
  - A view-only user that uses the operating system credentials associated to DB2 (for example, db2admin/password). See "Setting up a view-only user on Windows" for information about how to set up view-only authority for a user on Windows.
- See "Accessing views in the database repository" on page 619 for an example of how to perform the following tasks:
  - Use the Business Intelligence and Reporting Tools (BIRT) report designer to create a report based on the information available in Tivoli Storage Productivity Center's exposed views. See the following Web site for more information about BIRT: http://www.eclipse.org/birt/phoenix/.
  - View the report you created in BIRT through the Tivoli Common Reporting v1.2 feature of Tivoli Enterprise Portal. See the following Web site for more information about Tivoli Common Reporting: http://www.ibm.com/ developerworks/spaces/tcr.
- See the following page on Tivoli Storage Productivity Center's support Web site for detailed information about the views provided with Tivoli Storage Productivity Center: http://www.ibm.com/systems/support/storage/software/ tpc

## Setting up a view-only user on Windows

This topic provides information on how to set up a user with view-only privileges for the exposed views in the TPCREPORT schema. This procedure is for Windows only.

To set up a user with view-only privileges on Windows, complete these steps:

- 1. Create a new user on Windows. For example, create a user named TPCRPT.
  - a. Open Administrative Tools > Computer Management in the Control Panel.
  - b. Click **New User** on the **Action** menu.
  - c. Enter information about the new user and click Create.
  - d. Click Close.
- 2. Add the new user to the DB2USERS group. When you add the new user to the DB2USERS group it automatically provides that user with SQL connect authority only.
  - a. Open User Accounts in the Control Panel.
  - b. On the **Users** tab under **Users for this computer**, select the user account name and click **Properties**.
  - c. On the Group Membership tab, select the DB2USERS group and then OK.
- 3. Use the DB2 Control Center to assign SELECT only authority to the new user.
  - a. Start the DB2 Control Panel.
  - b. Expand **TPCDB** > **User and Group Objects** in the left pane.
  - c. Select the DB Users folder. A list of users appears in the right pane.
  - d. Select the new user that you created in step 1.

- e. Select Change... from the Selected menu while the new user is highlighted.
- f. Click the View tab. A list of views appears in the right pane. A green check mark in the columns next to each view indicates that the user can perform the actions represented by those columns. A red circle with a line through it indicates that the user cannot perform the actions represented by those columns.
- g. Do not change the privileges for the views in the TPCREPORT schema. The default settings for the views in the TPCREPORT schema indicate that the new user cannot perform the following SQL commands against those views: INSERT, UPDATE, DELETE, CONTROL. Accept the default settings that restrict the new user from performing actions against the views.
- h. Click the **Schema** tab. A list of schemas and the users level of authority for each appears in the right pane.
- i. Make sure that the user does not have **CREATEIN**, **DROPIN**, or **ALTERIN** privileges. This ensures that the user has read-only access to the exposed Tivoli Storage Productivity Center views.

## Running the DB2 health monitor

It is a good practice to run the DB2 health monitor which is a DB2 tool which monitors the health of an instance and active databases.

The health monitor also has the capability to alert a database administrator (DBA) of potential system health issues. The health monitor proactively detects issues that might lead to hardware failures, or to unacceptable system performance or capability. The proactive nature of the health monitor enables users to address an issue before it becomes a problem that affects system performance.

The health monitor checks the state of your system using health indicators to determine if an alert should be issued. Preconfigured actions can be taken in response to alerts. The health monitor can also log alerts in the administration management-by-exception model to free up valuable DBA resources by generating alerts to potential system health issues without requiring active monitoring.

The health monitor gathers information about the health of the system using interfaces that do not impose a performance penalty. It does not turn on any snapshot monitor switches to collect information.

It is recommended that you monitor DB2's database performance for table spaces for IBM Tivoli Storage Productivity Center. You can do this through DB2's Health Center. A health indicator measures the health of some aspect of a particular class of database objects, such as table spaces. Criteria are applied to the measurement to determine healthiness. The criteria applied depends on the type of health indicator. A determination of unhealthiness based on the criteria generates an alert.

Threshold-based indicators are measurements that represent a statistic (on a continuous range of values) of the behavior of the object. Warning and alarm threshold values define boundaries or zones for normal, warning, and alarm ranges.

**Note:** An SMS table space is considered full if there is no more space on any of the file systems for which containers are defined, although it might still have some space left in other data containers or their file systems.
To get to DB2's Health Center on Windows, go to **Start > All Programs > IBM DB2 > Monitoring Tools > Health Center**.

To get to DB2's Health Center on UNIX, log on as the DB2 user, like db2inst1, and run this command: **db2cc**. Before running the command, make sure you source the profile: . / home/<instance\_owner>/sqllib/db2profile.

On the Health Center window, click **Health Center > Configure > Health Indicator Settings**. On the Health Indicator Configuration Launchpad window, click **Instance Settings**. On the Instance Health Indicator Configuration window, enter **DB2** for instance. These defaults should be set for the Monitor Heap Utilization:

- Default is Yes
- Evaluate is Yes (indicates that evaluation is enabled)
- Warning is 85% (indicates that the warning threshold level is set)
- Alarm is 95% (indicates that the alarm threshold level is set)

On the Health Center window, click **Health Center > Configure > Health Indicator Settings**. On the Health Indicator Configuration Launchpad window, click **Global Settings**. On the Global Health Indicator Configuration window, enter DB2 for the Instance and Database for Object Type. Check **Application Currency**, Deadlock Rate. The defaults should be set as follows:

- Default is Yes
- Evaluate is Yes (indicates that evaluation is enabled)
- Warning is 5 (indicates that the warning threshold level is set)
- Alarm is 10 Deadlocks per hour (you get warning if this threshold is reached).

Other parameters you might want to check for global health monitor are:

- Logging Log filesystem Utilization
- Database Automatic Storage Utilization

You can check the health of the database by going to the DB2 Health Center and follow the directions for the Health Center.

Tivoli Storage Productivity Center uses the default configuration of IBM DB2's health monitor. This health monitor configuration should be sufficient in most cases. If you wish to get earlier warnings or include more parameters to the monitor, you can do so.

For more information about DB2's health monitor, go to the DB2 Information Center. Search for **health monitor**.

# Additional IBM Tivoli Storage Productivity Center publications

This topic provides information about additional Tivoli Storage Productivity Center publications.

There are several Tivoli Storage Productivity Center publications on the technical support Web site which provide additional information about planning for your environment:

- IBM TotalStorage Productivity Center Hints and Tips
- IBM TotalStorage Productivity Center V3 Performance Management Best Practices

- IBM TotalStorage Productivity Center V3 Best Practices
- IBM TotalStorage Productivity Center V3 Best Practices
- IBM TotalStorage Productivity Center V3 Best Practices

For more information about these publications, see this Web site: http://www.ibm.com/systems/support/storage/software/tpc/. Select a product. Click on the Install and Use tab. On the right, click on **Best Practices**.

# Subscribing to IBM Tivoli Storage Productivity Center technical support Web site

It is a good practice to subscribe to the IBM Tivoli Storage Productivity Center technical support Web site to receive information about important technical notes, flashes, and APAR information.

For more information about the IBM Tivoli Storage Productivity Center technical support Web site, see http://www.ibm.com/systems/support/storage/software/tpc/.

To receive future support notifications, go to the right and under **Stay informed**, click **Subscribe**. You will be required to enter your IBM ID and password. Once authenticated, you will see a Subscriptions page which provides information about the following:

- How to create and organize subscriptions
- How you are notified about subscriptions
- · How to specify the frequency of e-mail notifications
- How to subscribe for specific topics per product
- How to unsubscribe

# Chapter 2. Installing the IBM Tivoli Storage Productivity Center family

This section describes how to install DB2, Agent Manager, IBM Tivoli Storage Productivity Center, and IBM Tivoli Storage Productivity Center for Replication. This section also provides information about the preparation work required before installing the Tivoli Storage Productivity Center family.

# Installing IBM Tivoli Storage Productivity Center overview

This section provides information on the preparation work required before you can install IBM Tivoli Storage Productivity Center as well as the information to install Tivoli Storage Productivity Center for Replication.

### **Overview**

You can install all the the Tivoli Storage Productivity Center family using typical installation or custom installation. Custom installation allows you to see what components are being installed and where the components are being installed as well as set different passwords for user IDs.

Tivoli Storage Productivity Center for Replication is no longer a stand-alone application. Tivoli Storage Productivity Center Version 4.1 now installs Tivoli Integrated Portal and Tivoli Storage Productivity Center for Replication Version 4.1.

When you install Tivoli Storage Productivity Center, you have these installable components:

- Database schema
- Data Server and Device server
- Graphical User Interface (GUI)
- Command Line Interface (CLI)
- Data agent
- Fabric agent

You will need to install most of these components in order to get Tivoli Storage Productivity Center to work. The CLI is considered optional. The Data agents and Fabric agents will most likely be installed in multiple locations. The GUI is installed wherever a user might wish to control Tivoli Storage Productivity Center.

If you are using a remote database for Tivoli Storage Productivity Center, you must install the database schema on that remote database after you have installed DB2 on that remote machine.

After Tivoli Storage Productivity Center is installed, the installation program will start the Tivoli Storage Productivity Center for Replication installation wizard.

Tivoli Storage Productivity Center also supports a Java Web based GUI which gives you the option of installing the GUI wherever you wish to use Tivoli Storage Productivity Center. For information about the Java Web based GUI, see "Configuring Java Web Start to start the IBM Tivoli Storage Productivity Center GUI" on page 323. If you are using IPv6, see "Planning for Internet Protocol Version 6" on page 34.

DB2 and Agent Manager are separate installation programs from Tivoli Storage Productivity Center. The DB schema, Data Server, Device server, agents, GUI, and CLI are all components of Tivoli Storage Productivity Center. They can be installed all at once or at different times.

You can install Tivoli Storage Productivity Center with or without Agent Manager and agents. If you install Tivoli Storage Productivity Center without Agent Manager and agents, you can install Agent Manager and agents at a later time and register the Agent Manager with Tivoli Storage Productivity Center.

If you install the Tivoli Storage Productivity Center components at different times, you must install the components in this order:

- 1. DB2 (DB2 is required for Agent Manager and Tivoli Storage Productivity Center)
- 2. Agent Manager (including the embedded version of IBM WebSphere Application Server Express)
- **3**. DB schema (this is installed using the Tivoli Storage Productivity Center installation program)
- 4. Data Server and Device server (this is installed using the Tivoli Storage Productivity Center installation program)
- 5. Data agent, Fabric agent, GUI, or CLI (you can install one, all, or a combination of these components using the Tivoli Storage Productivity Center installation program)

#### Fully-qualified host names

Tivoli Storage Productivity Center requires fully-qualified host names. Some systems might be configured to return a short host name, such as ddunham instead of a fully-qualified host name, such as ddunham.myorg.mycompany.com. Tivoli Storage Productivity Center should only be installed on a computer that has a fully-qualified host name. If you install Tivoli Storage Productivity Center on a system without a fully-qualified host name, the installation might appear to be successful but the single sign-on feature for Tivoli Integrated Portal, Tivoli Storage Productivity Center, and Tivoli Storage Productivity Center for Replication might fail to operate. For information about fully-qualified host names, see "Checking for a fully qualified host name" on page 487

### Accessing IBM Tivoli Storage Productivity Center for Replication

If you install IBM Tivoli Storage Productivity Center using operating system authentication, the IBM Tivoli Storage Productivity Center user group is not automatically added to the IBM Tivoli Storage Productivity Center for Replication administration role. If you want to start IBM Tivoli Storage Productivity Center for Replication from IBM Tivoli Storage Productivity Center using the same user ID, you must explicitly add the IBM Tivoli Storage Productivity Center user group (that has that user ID) to IBM Tivoli Storage Productivity Center for Replication. For an example of adding a user group to IBM Tivoli Storage Productivity Center user group name to IBM Tivoli Storage Productivity Center for Replication" on page 462.

### InstallShield limitations

These are some limitations you might encounter when installing Tivoli Storage Productivity Center:

- When running the Tivoli Storage Productivity Center installation program on Solaris systems, some of the graphical elements in the installation panels might not display correctly. For example, in the **Select the type of installation you want to run** panel, the **TPC Installation Location** button might appear truncated. This is due to an InstallShield limitation on Solaris systems.
- When using the Tivoli Storage Productivity Center installation program to install IBM Tivoli Integrated Portal on AIX systems, the progress bar incorrectly indicates that IBM Tivoli Integrated Portal installation is 100% complete even though it is not yet complete. You must continue to wait until installation is complete. This is due to an InstallShield limitation on AIX systems that prevents the progress bar from correctly reflecting the installation progress.
- When you install Tivoli Storage Productivity Center on AIX, the progress bar can incorrectly display 100% for any component that is installed even though the installation is not complete. This does not affect the installation.

# Installing DB2

This topic describes how to perform a new installation of IBM DB2 Version 9 for Linux, UNIX, and Windows. DB2 is required for the Agent Manager and IBM Tivoli Storage Productivity Center. IBM Tivoli Storage Productivity Center for Replication does not use DB2 as the database repository.

# Preparing to install DB2

Before you install DB2, it is important to understand the default user IDs and groups created. The DB2 administrator user ID and password created will be the user ID and password you use to install Agent Manager and IBM Tivoli Storage Productivity Center. You can use the default user ID and password or provide your own user ID and password.

If you are using IPv6–only machines, you must install DB2 Database V9.1 or V9.5 for Linux and UNIX. This is required for the database repository on IPv6–only machines. Note that Windows platforms do not support machines configured for IPv6–only (Windows is enabled for both IPv6 and IPv4.)

### Preparing to install DB2 on Windows

If you have an administrator user ID that you want to use for installing DB2 and IBM Tivoli Storage Productivity Center, make sure this user ID is a member of DB2ADMNS group and the Administrators' group.

When you install DB2, two groups will be created:

- DB2ADMNS this group will have all the required user rights assigned for administrative authority.
- DB2USERS this group will have user rights assigned for DB2 users.

Assign users that need administrative authority to the DB2ADMNS group and DB2 users to the DB2USERS group. When you assign a user ID to either group, that user ID will have all the user rights required for that group; you do not have to assign individual user rights to each user ID.

**Note: Important:** DB2 can automatically create a DB2 user ID with administrative authority. The default user ID is **db2admin**. If you do not want to use this user ID to install Tivoli Storage Productivity Center, you can create a new administrative user ID, for example **tpcadmin**. If DB2 creates this user ID, this user ID will be added to the DB2ADMNS group and the Windows Administrators group.

## Preparing to install DB2 on UNIX or Linux

Three users and groups are required to operate DB2 UDB on UNIX or Linux: the instance owner, the fenced user, and the DB2 administration server user. These users and groups are automatically created during the installation of DB2.

Table 21. DB2 Setup Wizard default user and group names

Required user	Default user name	Default group name	Description
instance owner	db2inst1	db2iadm1	Created in the instance owner home directory. This user ID controls all DB2 processes and owns all file systems and devices used by the databases contained within the instance.
fenced user	db2fenc1	db2fadm1	Used to run user-defined functions (UDFs) and stored procedures outside of the address space used by the DB2 database.
DB2 administration server user	dasusr1	dasadm1	Used to run the DB2 administration server on your system. Used by the DB2 GUI tools to perform administration tasks. This user does not contain any databases and there is only one administration server per machine.

# **Installing DB2 on Windows**

This topic describes how to install DB2 on Windows. DB2 must be installed before you install Agent Manager and IBM Tivoli Storage Productivity Center.

To install DB2, follow these steps:

- 1. Log on with a user ID with Administrator authority on Windows.
- 2. Insert the DB2 product CD into the CD-ROM drive or use the unzipped DB2 installation image. Windows Autorun starts the LaunchPad.

The DB2 installation program should start within 15 - 30 seconds if you have Windows Autorun mode set on your system. If the installation program does not start, do one of the following steps:

• Use a command prompt to change to the root of the CD-ROM and enter: setup.exe

- Use Windows Explorer, open the root of the CD-ROM, and double-click the setup.exe file.
- 3. On the "Welcome" panel, click **Install a Product**. In the right pane, click **Install New** for **DB2 Enterprise Server Edition**.
- 4. On the "Welcome to the DB2 Setup wizard for DB2 Enterprise Server Edition, Version 9.5" panel, click **Next**.
- 5. On the "Software License Agreement" panel, read the license agreement and select **I accept the terms in the license agreement** if you agree to the terms. Click **Next**. If you click **Cancel**, the installation program ends without installing any programs.
- 6. In the "Select the installation type" panel, select Typical. Click Next.
- 7. The "Select installation, response file creation, or both" panel is displayed. Select **Install DB2 Enterprise Server Edition on this computer and save my settings in a response file**. Enter a response file name or accept the default. Click **Next**.
- 8. In the "Select the installation folder" panel, enter a directory or use the default. (For ease of maintenance, use the default directory.) Click Next.
- **9**. The "Set user information for the DB2 Administration Server" panel is displayed. Enter the following information for User information:
  - a. Domain (leave this field blank).
  - b. User name (Type a user name of the DB2 user account that you want to use. DB2 adds this user ID to the DB2ADMNS group.)
  - c. Password and confirm password

Select the check box for **Use the same user name and password for the remaining DB2 services**. The user ID and password will be used to install Tivoli Storage Productivity Center. Click **Next**.

**10.** The "Set up a DB2 instance" panel is displayed. Click **Next** to create the default DB2 instance.

**Note:** This panel appears if you are installing DB2 on a computer that belongs to an accessible domain.

11. The "Set up partitioning options for the default DB2 instance" panel is displayed. Select to set up a single partition instance or multiple partition instance. Click **Next** to continue.

**Note:** To support multiple partitioned DB2 database servers, the computer on which you are installing DB2 must belong to an accessible domain.

- **12.** The "Configure DB2 instances" panel is displayed. Click **Next** to accept the default instance of DB2.
- **13**. The "Prepare the DB2 tools catalog" panel is displayed. Accept the defaults and click **Next**. (The default is to not prepare the DB2 tools catalog.)
- 14. The "Set up notifications" panel is displayed. Clear the check box for **Set up** your **DB2 server to send notifications**. Click **Next**.
- **15**. The "Enable operating system security for DB2 objects" panel is displayed. Accept the defaults for this panel and click **Next**. (The default is to enable operating system security.)

**Note:** If this is not the first time you have installed DB2 on this system, the DB2ADMS group may still be on the machine. If so, you will see a warning dialog when you click **Next** in the security panel. The message is:

Warning The group; name "DB2ADMS" already exists in the system and will be granted complete access to the DB2 folders and objects through the operating system. Click OK to continue installation, or click Cancel to input another group name.

- **16.** The "Start copying files and create response file" panel is displayed. After you have reviewed the summary information, click **Finish**.
- 17. You will see a progress window as DB2 is installed. Wait for installation to complete.
- **18**. The "Setup is complete" panel is displayed. Read the information on the panel and click **Finish**.
- **19**. The "Install additional products" panel is displayed. Do not install additional products at this time. Click **Finish**.
- 20. The setup wizard closes and you are back on the DB2 Welcome screen which now has "Welcome to First Steps" in the left pane. This panel includes a **Product Updates** button in the left pane. Click the button to see if there are any product updates. Click **Exit** when you have finished checking for updates.
- 21. Restart the machine.

## Installing DB2 on UNIX or Linux - GUI install

This topic describes how to install DB2 on UNIX or Linux using a GUI installation program.

**Note:** You must have the X11 graphic capability installed before installing DB2 using the GUI.

To install DB2, complete the following steps:

- 1. Log in as a user ID with root authority.
- 2. If you are not using a CD to install DB2, you can skip to step 5 and invoke **db2setup** from the directory where you have the DB2 source installation program. If you are installing DB2 using the CD, create a mount point or choose an existing mount point. To create a mount point called /cdrom, entering the following command:

mkdir /cdrom

**3.** Insert the DB2 CD into the CD-ROM drive. Mount the CD-ROM file system at the desired mount point.

On AIX, you can use the **crfs** command to add an entry to /etc/filesystems for the cdrom mount point. Run the following commands:

/usr/sbin/crfs -v cdrfs -p ro -d'cd0' -m'/cdrom' -A'no' mount /cdrom

The **crfs** command only has to be run once for a given mount point, and after that you can use **mount** and **umount** for each CD or DVD you put in the drive, for example, **mount /cdrom** and **umount /cdrom**.

On Linux, run these commands:

mkdir /cdrom
mount -o ro /dev/cdrom /cdrom

4. Change to the directory where the CD-ROM is mounted by entering the following command:

cd /cdrom

5. Enter the ./db2setup command to start the DB2 Setup wizard.

- 6. On the "Welcome" panel, click **Install a Product**. In the right pane, click **Install New** for **DB2 Enterprise Server Edition**.
- 7. In the "Welcome to the DB2 Setup wizard" panel, click Next.
- 8. On the "License Agreement" panel, read the license agreement. Click **Read non-IBM terms** to read additional license terms. If you agree with all the terms, select **Accept** and click **Next**. If you click **Cancel**, the installation program ends without installing any programs.

Note: On DB2 version 9.1, there are no additional non-IBM license terms.

- 9. In the "Select the installation type" panel, select Typical. Click Next.
- 10. The "Select installation, response file creation, or both" panel is displayed. Select Install DB2 Enterprise Server Edition on this computer and save my settings in a response file. Enter a response file name or accept the default. Click Next.
- 11. In the "Select the installation directory" panel, enter a directory or use the default. (It is recommended that you use the default directory.) Click Next.

**Note:** After you click **Next**, if your system is an IBM xSeries or pSeries, you might see a panel titled "Install the IBM Tivoli System Automation for Multiplatforms Base Component (SA MP Base Component)." This component might be installed but is not required by IBM Tivoli Storage Productivity Center. Make a selection to install SA MP Base Component. Click **Next**. This applies to DB2 version 9.5 only.

- 12. The "Set user information for the DB2 Administration Server" panel is displayed. Select **New user**. Enter the following information for a new user:
  - a. User name (Type a user name and password of the DB2 user account that you want to use. DB2 adds this user ID to the DB2ADMNS group. If this user ID does not exist, DB2 will create it.)
  - b. Group name
  - c. Password and confirm password
  - d. Home directory
  - e. Use the default UID
  - f. Use the default GID

The DAS user is used to administer the DB2 database. Click Next.

- **13**. The "Set up a DB2 instance" panel is displayed. Select **Create a DB2 instance**. Click **Next**.
- 14. The "Set up partitioning options for the DB2 instance" panel is displayed. Select **Single partition instance**. Click **Next**.
- 15. The "Set user information for the DB2 instance owner" panel is displayed. The DB2 instance owner user is the user you enter when installing IBM Tivoli Storage Productivity Center. Select New user. Enter the following information:
  - User name
  - Group name
  - Password and confirm password
  - Home directory
  - Use the default UID
  - Use the default GID

Click Next.

- The "Set user information for the fenced user" panel is displayed. Select New user. Enter the following information:
  - User name
  - Group name
  - · Password and confirm password
  - · Home directory
  - Use the default UID
  - Use the default GID

Click Next.

- The "Prepare the DB2 tools catalog panel is displayed. Select Do not prepare the DB2 tools catalog. Click Next.
- The "Set up notifications" panel is displayed. Select Do not set up your DB2 server to send notifications at this time. Click Next.
- **19**. The "Start copying files and create response file" panel is displayed. After you have reviewed the summary information, click **Finish**.
- **20.** You will see a progress window as DB2 is installed. Wait for installation to complete.
- **21.** The "Setup is complete" panel is displayed. Read the information on the panel and click **Finish**.
- 22. The setup wizard closes.

**Note:** After you have completed installing DB2 UDB, edit the file /etc/group and add **root** to the **db2iadm1** group. The **db2iadm1** line in /etc/group should look similar to the following line:

db2iadm1:x:102:root

This applies to DB2 version 9.5 only.

### Installing DB2 on AIX - Command line

This topic describes how to install DB2 on AIX using a command line.

To install DB2, complete the following steps:

- 1. Log in as a user ID with root authority.
- 2. If you are not using a CD to install DB2, you can skip to step 5 and work from the directory where you have the DB2 source installation program. If you are installing DB2 using the CD, create a mount point or choose an existing mount point. To create a mount point called /cdrom, entering the following command:

mkdir /cdrom

3. Insert the DB2 CD into the CD-ROM drive. Mount the CD-ROM file system at the desired mount point.

On AIX, you can use the **crfs** command to add an entry to /etc/filesystems for the cdrom mount point. Run the following commands:

/usr/sbin/crfs -v cdrfs -p ro -d'cd0' -m'/cdrom' -A'no' mount /cdrom

The **crfs** command only has to be run once for a given mount point, and after that you can use **mount** and **umount** for each CD or DVD you put in the drive, for example, **mount /cdrom** and **umount /cdrom**.

4. Change to the directory where the CD-ROM is mounted by entering the following command:

cd /cdrom

- 5. Install the DB2 Manager.
  - a. Create a temporary directory (for example, db2temp) to hold the DB2 installer tar file and untarred files. These files require 2-3 gigabytes of hard drive space.
  - b. Copy or download the DB2 installer into db2temp. The name of the file varies depending on the location from where the file is downloaded or copied and the language to which it is associated.
  - c. (optional) Use the appropriate unzipping tool to unzip the DB2 installer file if it is compressed. For example, ,if the name of the file is v9fp2\_aix\_ese.tar.gz, type gunzip v9fp2\_aix\_ese.tar.gz. In this example, v9fp2\_aix\_ese.tar appears in the db2temp directory.
  - d. Make an installer directory. For example, type **mkdir install**.
  - e. Change to the new install directory. Type cd install.
  - f. Un-tar the DB2 installer file. For example, of the name of the installer file is v9fp2\_aix\_ese.tar, type tar xvf ./v9fp2\_aix\_ese.tar.
  - g. Go to the directory that contains the DB2 installer executable. Type cd /db2temp/installer/ese/disk1.
  - h. Execute the command line installer. Type ./db2\_install.
  - i. Select the product to install: DB2.ESE. A number of messages appear in the command window. The Installation Summary eventually appears and indicates a successful installation. DB2 is installed in /opt/IBM/db2.
- 6. Create users and groups for use with DB2.
  - a. Type mkgroup id=999 db2iadm1.
  - b. Type mkgroup id=998 db2fadm1.
  - c. Type mkgroup id=997 dasadm1.
  - d. Type mkuser id=1004 pgrp=db2iadm1 groups=db2iadm1 home=/home/db2inst1 db2inst1.
  - e. Type mkuser id=1003 pgrp=db2fadm1 groups=db2fadm1 home=/home/db2fenc1 db2fenc1.
  - f. Type mkuser id=1002 pgrp=dasadm1 groups=dasadm1 home=/home/dasusr1 dasusr1.
  - g. Verify the owner of the directories. To do this, type **ls -ld /home/db2inst1**. The directory ownership should appear as follows:
    - /home/db2inst1 should show group db2iadm1 and user db2inst1
    - /home/db2fenc1 should show group db2fadm1 and user db2fenc1
    - /home/dasusr1 should show group dasadm1 and user dasusr1

If the directory ownership is not correct, run the following commands as appropriate:

- chown -R db2inst1:db2iadm1 /home/db2inst1
- chown -R db2fenc1:db2fadm1 /home/db2fenc1
- chown -R dasusr1:dasadm1 /home/dasusr1
- h. Type **passwd db2inst1** *password*, where *password* represents the password you want to use for the DB2 instance.
- i. Type pwdadm -f NOCHECK db2inst1.
- j. Type **passwd db2fenc1***password*, where *password* represents the password you want to use for the fenced user.
- k. Type pwdadm -f NOCHECK db2fenc1.

- I. Type **passwd dasusr1***password*, where *password* represents the password you want to use for the DB2 administration server (DAS) user.
- m. Type pwdadm -f NOCHECK dasusr1.
- n. Type chgroup users=db2inst1,root db2iadm1.
- Create a DB2 Administrative Server (DAS). Type /opt/db2/V9.5/instance/dascrt -u dasusr1.
- 8. Create a DB2 instance:
  - a. Type /opt/db2/V9.5/instance/db2icrt -a server -u db2fenc1 db2inst1.
  - b. Type . /home/db2inst1/sqllib/db2profile.
- 9. Change the default location for database repositories. By default, this location is /home/db2inst1. /home is usually not large enough for database repositories. Choose a file system with enough free space (30 gigabytes or higher) to contain the IBM Tivoli Storage Productivity Center repository. To change the default location, complete the following steps:
  - a. Type **db2 update dbm cfg using DFTDBPATH** *<new repository path>* **IMMEDIATE**, where *<new repository path>* represents the new location for the repository.
  - b. Type chown -R db2inst1:db2iadm1 <new repository path> to assign ownership to db2inst1 and permission to anyone in db2iadm1 (same as the ownership for /home/db2inst1).
- 10. Configure DB2 communication:
  - Edit /etc/services and verify or add the following line at the end of the file: db2c\_db2inst1 50000/tcp
  - b. Type db2 update dbm cfg using svcename db2c\_db2inst1.
  - c. Type db2set DB2COMM=tcpip.
- 11. Add the DB2 license:
  - a. Type cd /opt/IBM/db2/V9.5/adm.
  - b. Type ./db2licm -a <DB2 installer location>/db2/ese/disk1/db2/license/ db2ese\_o.lic, where <DB2 installer location> represents the directory where the DB2 installer is located (for example, /db2temp/install).
- 12. Restart DB2:
  - a. Type db2stop force.
  - b. Type db2 terminate.
  - c. Type db2start.
- 13. Test your DB2 instance:
  - a. Type . /home/db2inst1/sqllib/db2profile.
  - b. Type db2level . Information about the instance and DB2 is displayed.
  - c. Type db2 create db test to create a test database.
  - d. Type **db2 list db directory** to list information about all the databases created for this instance.
  - e. Type **db2 connect to test user db2inst1 using** *<password>*, where password represents the password you defined in step 6 for the DB2 instance.
  - f. Type db2 disconnect test.
  - g. Type db2 drop db test.

# Verifying that DB2 is installed correctly

You can verify that DB2 has been installed properly using the command line processor (CLP) or the First Steps GUI.

The general steps to verify that DB2 has been installed properly is as follows:

- 1. Create the SAMPLE database.
- 2. Connect to the SAMPLE database.
- 3. Run a query against the SAMPLE database.
- 4. Drop the SAMPLE database.

# Verifying DB2 installation using the command-line processor (CLP)

You can verify that DB2 has been successfully installed using the command-line processor (CLP).

To verify that DB2 has been installed successfully, complete the following steps:

- 1. Log on to the system as a user with SYSADM authority.
- 2. Start the database manager by entering the db2start command.

**Note:** For UNIX and Linux, you must source the db2profile before you run the db2start command. See "Using the command line on UNIX and Linux" on page 400 for information on how to do this.

- **3**. Enter the db2sampl command to create the SAMPLE database. This command may take a few minutes to process. There is no completion message. When the command prompt returns, the process is complete. The SAMPLE database is automatically cataloged with the database alias SAMPLE when it is created.
- 4. Enter the following DB2 commands from a DB2 command window to connect to the SAMPLE database, retrieve a list of all the employees that work in Department 20, and reset the database connection:

db2 connect to sample db2 "select \* from staff where dept = 20" db2 connect reset

5. After you have verified the installation, you can remove the SAMPLE database to free up disk space. Enter the db2 drop database sample command to drop the SAMPLE database.

For more information about verifying DB2 installation, refer to the DB2 documentation for your operating system.

### Verifying DB2 installation using First Steps

You can use First Steps to verify that DB2 has been installed successfully.

You must have the Control Center and the First Steps component installed to perform this task. First Steps is part of the getting started component grouping in the DB2 Setup wizard. It is installed as part of a Typical installation or may be selected when performing a Custom installation.

To verify the DB2 installation, complete the following steps:

- 1. Log on to the system with the user account that you want to use to verify the installation. Ensure that the domain user account you use to create the sample database has SYSADM or SYSCTRL authority.
- 2. Start First Steps.
  - On UNIX or Linux, type db2fs.

- On Windows, type db2fs.bat.
- **3**. Select **Create Sample Databases** in the First Steps launchpad to open the Create Sample Databases window.
- 4. In the Create Sample Databases window, select the databases you want to create. The DB2 UDB sample database is used to verify the installation.
- 5. Click **OK**. By default, the SAMPLE database is created on the computer where DB2 is installed. The command may take a few minutes to process. When the SAMPLE database has been created, you receive a completion message. Click **OK**.
- 6. Once the database is created, select **Work with Databases** on the First Steps launchpad to start the Control Center. You can perform administration tasks on different instance and database objects through the Control Center. In the left pane of the Control Center screen, expand the object tree to view the SAMPLE database and SAMPLE database objects. Select the Tables object to view the SAMPLE database tables in the right pane of the Control Center screen.
- 7. After you have verified the installation, you can remove the SAMPLE database to free up disk space. Enter the db2 drop database sample command to drop the SAMPLE database. For more information about verifying DB2 installation, refer to the DB2 documentation for your operating system.

# Configuring DB2, AIX, and Linux for IPv6-only environment

Use this information to configure DB2, AIX, and Linux for an IPv6-only environment.

#### Configuring the AIX system for IPv6 only

**Note:** For IPv6 support, the AIX operating system must have level TL 5300–06 installed.

Follow these steps:

- 1. Obtain the most recent versions of openssh and openssl packages for AIX and install them. Some older versions of openssh will not work in an IPv6–only environment.
- 2. Change sshd (Secure Shell Daemon) on AIX system to accept IPv6 connections.
  - a. In the /etc/ssh/sshd\_config file, uncomment the line "ListenAddress ::".
  - b. Restart sshd with the following commands:

```
stopsrc -g ssh
startsrc -g ssh
```

- **c.** From another IPv6 system, verify that you contact AIX over IPv6 (using ssh).
- 3. In SMIT, set the IPv4 address to 0.0.0.0 for all interfaces. Save the file.
- 4. Edit the /etc/resolv.conf file to use IPv6 DNS server or servers.

#### Configuring DB2 on AIX for IPv6 systems

To get DB2 on AIX to work on IPv6 systems, follow these steps:

1. Identify the host name used by DB2 in the db2nodes.cfg file:

```
# cat ~db2inst1/sqllib/db2nodes.cfg
0 <myhost> 0
#
```

2. Edit the /etc/hosts file and make sure that the host name found in the db2nodes.cfg file resolves to an IPv6 address. Use the **vi** editor to verify that

the host name is not on any line with an IPv4 address. In particular, ensure that the host name is not listed as an alias for the IPv4 loopback address 127.0.0.1.

```
# vi /etc/hosts
```

```
127.0.0.1 loopback localhost
::1 localhost
```

```
2001:db8:0:0:209:6bff:fe09:63fa <myhost.mydomain> <myhost>
```

- 3. Stop DB2 and set DB2 to use IPv6 addressing. Restart DB2.
  - a. Source the DB2 profile:

. ~db2inst1/sqllib/db2profile

b. Stop DB2:

db2stop

- c. Configure DB2 to use IPv6. db2set DB2FCMCOMM=TCPIP6
- d. Start DB2.

db2start

In some installations, the AIX server does not have a graphical console attached to the server. In this situation, you can select another system with an X11 server to display the IBM Tivoli Storage Productivity Center installation and Tivoli Storage Productivity Center application. The X11 server must have IPv6 configured and an SSH client installed. Open an SSH connection from a shell on the X11 server's desktop with the -X option to permit forwarding of X11 applications from the remote AIX server. Start the Tivoli Storage Productivity Center installation program or application from the SSH shell.

ssh -X <my\_IPv6\_host>
/opt/IBM/TPC/gui/TPCD.sh

# Configuring DB2 on Linux for IPv6-only systems

To get DB2 on Red Hat Enterprise Linux Version 4 systems to work in an IPv6–only environment, follow these steps:

- 1. Install DB2 in dual-stack configuration.
- 2. Stop DB2 and set DB2 to use IPv6 addressing:
  - As the root user from the UNIX command line, run this command:
     su db2inst1
  - b. Stop DB2 by running this command:

db2stop

c. Configure DB2 to use IPv6 by running this command: db2set DB2FCMCOMM=TCPIP6

**Note:** The host name in the db2nodes.cfg file should resolve to an IPv6 address. This can require you to change the domain or search directive in the /etc/resolv.conf file to specify a domain in which the host name can resolve to IPv6. You can also edit the /etc/hosts file so that the host name resolves to an IPv6 address.

d. Start DB2 by running this command:

db2start

# Installing the Agent Manager

The Agent Manager is required only if you are installing the Data agents and Fabric agents.

Agent Manager is optional. If you decide at a later time to install the Agent Manager, you can do so. After you install the Agent Manager, you must register the Device server and Data server with the Agent Manager before installing the Data agents and Fabric agents. For information about registering the Device server and Data server with the Agent Manager, see "Agent Manager Registration" on page 294.

When you install a new version of Agent Manager on your system, you will be installing version 1.3.2. You can also upgrade Agent Manager from 1.2.x to 1.3.2. To upgrade Agent Manager from version 1.2.x to 1.3.2, run the Agent Manager installation program. If you have Agent Manager 1.2, it is mandatory that you upgrade to 1.3.2 because the embedded WebSphere shipped with Agent Manager 1.2 is no longer supported. Note that the common agents remain at release 1.2 and are compatible with Agent Manager 1.3.2.

Agent Manager requires a DB2 database repository. You can install Agent Manager using a 32–bit DB2 instance or a 64–bit DB2 instance. To determine the level of DB2 you have, run the **db2level** command.

To check for the version of Agent Manager you have, run the **HealthCheck** command. For information about the **HealthCheck** command, see "Agent Manager toolkit for administrators" on page 605.

#### Notes:

- The installation of the Agent Manager takes approximately 30 minutes.
- You can use a GUI-based installation program or a console-based (command line) installation program to install the Agent Manager.
- If you need to upgrade the Agent Manager, run the Agent Manager installation wizard and it will allow you to upgrade the Agent Manager.
- When you install the Agent Manager, you will also be installing the Embedded version of IBM WebSphere Application Server Express (WebSphere Express).
- The Agent Manager is disabled for IPv6 communication. Agent Manager and agent communication use IPv4 only.
- You must install the Data agent and Agent Manager to run IBM Tivoli Storage Productivity Center batch reports.

# Installing the Agent Manager using a 32-bit DB2 instance - GUI install

Use a GUI-based installation program to install the Agent Manager using a 32-bit DB2 instance. You must install DB2 before you install the Agent Manager.

To install the Agent Manager, complete the following steps:

- 1. Log on with a user ID that has the appropriate authority:
  - For Windows, you must have administrative authority.
  - For UNIX or Linux, you must have root authority.
- For UNIX or Linux platforms, you need to set the environment variables for the database instance (source db2profile). For example, if your DB2 instance is db2inst1, source the db2profile:
  - . /home/db2inst1/sqllib/db2profile

where home is the home directory of the instance owner.

**3**. Go to the Agent Manager CD or directory where you have downloaded the Agent Manager code. For the CD, select one of the following Agent Manager directory:

Windows/EmbeddedInstaller AIX/EmbeddedInstaller Linux/EmbeddedInstaller

For the electronic image, select one of the following files:

AgentManagerEmbeddedWS\_Aix.tar AgentManagerEmbeddedWS\_Linux.tar AgentManagerEmbeddedWS\_Windows.exe

Untar the file or download the exe file to your Agent Manager source installation directory.

- 4. To start the Agent Manager installation program, run one of the following programs from the Agent Manager CD or source installation directory:
  - For Windows: setupwin32.exe
  - For AIX: setupAix.bin
  - For Linux: setupLinux.bin
  - For Linux on POWER PC: setupLinuxPPC.bin
  - For Solaris: setupSolaris.bin
- 5. The Choose the runtime container for Agent Manager panel is displayed.

🍟 InstallShield Wizard for Insta	alling the Agent Manager
	Choose the runtime container for the Agent Manager:
IBM.	The embedded version of the IBM WebSphere Application Server delivered with the Agent Manager installer. The WebSphere Application Server. Make sure that the WebSphere Application Server is already installed.
InstallShield	
	< <u>Back</u> <u>Next</u> > <u>Cancel</u>

Figure 1. Agent Manager runtime container panel

You have the following options:

# The embedded version of the IBM WebSphere Application Server delivered with the Agent Manager installer.

Select this option. To ensure ease of installation, configuration, and maintenance, Tivoli Storage Productivity Center only supports an Agent Manager configured to run with the embedded version of the IBM WebSphere Application Server.

# The WebSphere Application Server. Make sure that the WebSphere Application Server is already installed. Do not select this option.

Click Next.

6. The Directory Name panel is displayed.

InstallShield Wizard for	Installing the Agent Manager
	Click Next to install "Tivoli Agent Manager" to this directory, or click Browse to install to a different directory.
IBM.	Directory Name.
	Browse
InstallShield	< Back Next > Cancel

Figure 2. Directory Name panel

Type the directory name or accept the default for the Agent Manager target directory. These are the default directory paths:

C:\Program Files\IBM\AgentManager (for Windows) /opt/IBM/AgentManager (for UNIX or Linux)

Enter the directory name and click Next.

7. The Type and Location of Registry panel is displayed.

InstallShield Wizard for	Installing the Agent Manager
	Type and Location of Registry
	Type and Location of the Database for the Registry
IBM.	<ul> <li>DB2 database on this computer</li> </ul>
	O DB2 database on another computer (without DB2 Administration Client)
	O Local alias to a DB2 database on another computer (using DB2 Administra
	<ul> <li>Oracle database on this computer</li> </ul>
	Oracle database on another computer (using Oracle Database Client)
	O database on this computer
InstallShield	
	< <u>Back</u> <u>N</u> ext > Cancel

Figure 3. Type and Location of Registry panel

You have these options:

#### DB2 database on this computer

Select this option. To ensure ease of installation, maintenance, and support, Tivoli Storage Productivity Center only supports an Agent Manager configured to run a local DB2 database server.

DB2 database on another computer (without DB2 Administration Client) Not supported by Tivoli Storage Productivity Center.

# Local alias to a DB2 database on another computer (using DB2 Administration Client)

Not supported by Tivoli Storage Productivity Center.

- Oracle database on this computer Not supported by Tivoli Storage Productivity Center.
- Oracle database on another computer (using Oracle Database Client) Not supported by Tivoli Storage Productivity Center.

#### <Derby or Cloudscape> database on this computer Not supported by Tivoli Storage Productivity Center.

#### Click Next.

8. The DB2 Universal Database Connection information panel is displayed.

InstallShield Wizard for	Installing the Agent Manager	_ 🗆 🛛
	DB2 Universal Database Connection Information	
	Database Software Directory	21
IBM.	C:\Program Files\IBM\SQLLIB	
	Database Name	Browse
	IBMCDB	
	If the database already exists, it will be reused. If it does not e be created for you.	xist, it will
InstallShield		
	< <u>B</u> ack Next >	<u>C</u> ancel

Figure 4. DB2 Universal Database Connection Information panel

Enter the following information:

#### **Database Software Directory**

Enter the directory where DB2 is installed. The default directory is: C:\Program Files\IBM\SQLLIB (for Windows)

/<db2home>/<db2instance>/IBM/SQLLIB (for UNIX or Linux)

#### Database Name

This is the name for the Agent Manager database. If this database does not exist, it will be created.

9. The Database User Information panel is displayed.

InstallShield Wizard for I	nstalling the Agent Manager
	Database User Information
IBM.	Specify the user ID and password for accessing the database Database Runtime User ID
	db2admin
	Password
	******
	Use a different user ID during the installation Specify a separate user ID for installing the agent manager. This user must have the authority to create a database and tables. This lets you limit the authority you give the runtime user ID because it does not need the authority to create objects. Database Administrator User ID
	db2admin
	Password
	******
InstallShield	
	< <u>Back</u> <u>N</u> ext > <u>C</u> ancel

Figure 5. Database User Information panel

Enter the following information:

#### Database Runtime User ID

Enter the database user name. This is the DB2 administrator user ID that is in the DB2ADMNS group and Administrators group.

#### Password

Enter the password for this user ID.

#### Use a different user ID during the installation

If you want to use a different user ID for installation of Agent Manager, select this check box and enter the user ID and password:

#### Database Administrator User ID

Enter the database user name. This is the DB2 administrator user ID that is in the DB2ADMNS group and Administrators group.

#### Password

Enter the password for this user ID.

10. The WebSphere Application Server Connection Information panel is displayed.

linstallShield Wizard for	Installing the Agent Manager	
	WebSphere Application Server Connection Information	
TEM	Host Name or Alias of Agent Manager	
	Tip: This is the network name that common agents and resource managers use to connect to the agent manager. Use a host name that can be resolved by those syster For example, use a network alias such as AgentManagerServer or a fully qualified ho name such as agman.mycompany.com. Registration Port	ns. st
	9511	
	Secure Port	
	9512	
	Public Port and Alternate Port for the Agent Recovery Service	
	9513	
	Do not use port 80 for the agent recovery service	
InstallShield		
	<u>Back</u>	el 📄

Figure 6. WebSphere Application Server Connection Information panel

Enter the following information:

#### Host Name or Alias of Agent Manager

If you specify a host name, use the fully qualified host name. For example, specify **mylab.tivlab.raleigh.ibm.com**. This value is used for the URLs for all Agent Manager services. It is preferable to use the fully qualified host name rather than an IP address.

**Note:** If you specify an IP address, you will see this panel when you click **Next**.

Do you really want to use the value xxx.xxx.xxx for the agent manager server?

This panel explains why it is recommended to use the host name rather than an IP address.

#### **Registration Port**

Use the default port of 9511 for the server-side SSL.

#### **Secure Port**

Use the default port of 9512 for client authentication, two-way SSL.

# Public Port and Alternate Port for the Agent Recovery Service

Use the public communication port default of 9513.

#### Do not use port 80 for the agent recovery service

Accept the default and do not check this box. If you check this box, make sure that port 80 is not being used by another application. To check for other applications which are using port 80, run this command:

netstat -anb (for Windows)
netstat -a -n (for Linux)

Look for port 80 in the listening state. This command provides the name of the executable file involved in creating the connection. If there is an application using port 80, stop that application and then continue with the installation of Agent Manager.

Enter the information and click Next.

11. The WebSphere Application Server Connection Information panel is displayed.

InstallShield Wizard for	Installing the Agent Manager 📃 🗆 🔀
	WebSphere Application Server Connection Information
	Application Server Name
IBM.	AgentManager
	Use this name to start and stop the application server and to locate the agent manager files in the WebSphere directory.
	/AgentMgr
	The context root is part of the URL that common agents and resource managers use to contact the agent manager. The underlined string in the following URL, including the forward slash, is the context root: http://IBM-84AA714148F.krakow.pl.ibm.com:8513 <u>/AgentMgr</u>
InstallShield	< Back Next > Cancel

Figure 7. WebSphere Application Server Connection Information panel

Accept the defaults and click Next.

12. The Security Certificates panel is displayed.

InstallShield Wizard for	Installing the Agent Manager
	Security Certificates
IBM.	Do you want to create certificates that are specific to this installation of the agent manager, or use the demonstration certificates?
	<ul> <li>Create certificates for this installation</li> </ul>
	O Use the demonstration certificates
	Demonstration certificates are publicly available and do not provide the level of security required by a typical IT environment. They are provided for testing or demonstration environments only.
InstallShield	< <u>B</u> ack <u>N</u> ext > <u>C</u> ancel

Figure 8. Security Certificates panel

Specify whether to create new certificates or to use the demonstration certificates. It is highly recommended that you generate new certificates for a secure environment. You have these options:

#### Create certificates for this installation

This is for a secure environment. This is the default and is recommended.

#### Use the demonstration certificates

Provided as a convenience for testing and demonstration purposes.

Make a selection and click Next.

**Note:** If you are creating new certificates, back up the certificates in case your Agent Manager server goes down or for disaster recovery purposes. If you do not back up the certificates, you will not be able to recover your system.

**13**. The Define the Certificate Authority panel is displayed.

lnstallShield Wizard for I	nstalling the Agent Manager	
	Define the Certificate Authority	67
	Certificate Authority Name	
IBM.	TivoliAgentManagerCA	
	Security Domain	
	krakow.pl.ibm.com	
	Certificate Authority Password This password locks the certificate authority truststore. The CA passw only by the agent manager.	ord is typically used
	If your security policies do not require you to examine the contents you can leave this field blank to generate a randomized password.	of the CA truststore
	rassworu	
And the second second	Confirm Password	
InstallShield		
	< <u>B</u> ack Next >	<u>C</u> ancel

Figure 9. Define the Certificate Authority panel

This panel is displayed if you are creating new certificates. Accept all the defaults.

Provide this information:

#### Certificate Authority Name

Accept the default. This value must be unique in your environment. If you have multiple Agent Managers installed, this value must be different on each Agent Manager. This might apply if you have the Agent Manager software installed for both a testing and production environment.

#### Security Domain

The domain name is used in the right-hand portion of the distinguished name (DN) of every certificate issued by the Agent Manager. It is the name of the security domain defined by the Agent Manager. Typically, this value is the registered domain name or contains the registered domain name. For example, for the computer system myserver.ibm.com, the domain name is ibm.com. This value must be unique in your environment. If you have multiple Agent Managers installed, this value must be different on each Agent Manager.

#### **Certificate Authority Password**

The certificate authority password locks the truststore file. The truststore files are CARootKeyRing.jks and CARootKey.pwd.

Specifying a value for this password is optional. You need to specify this password only if you want to be able to unlock the certificate authority truststore files to examine the certificates that they contain. If you do not specify a value for this password, one is generated automatically and used by the Agent Manager. **Note:** It is recommended that you specify a password so that you can look at the certificate files if you have problems. If you do not specify a password, you will not be able to look at the certificate files. Enter this password.

Enter the information and click Next.

14. The Set Passwords panel is displayed.

	Set Passwords	
IBM.	Agent Manager Password This password looks the agent manager truststore file (AgentManagerTrust.jks) and keystore file (agentManagerKeys.jks). This password is used internally by the agent manager. Password Confirm Password Agent Registration Password	•
	A common agent must provide this password to register with the agent manager. This password also locks the agent Trust, jks truststore file. A common agent or resource manager compares the certificate in its copy of the agent Trust, jks file with the certificate presented by the agent manager to make sure that it registers with the correct agent manager. This password is required to install a common agent or a resource manager. Password	
heislichiski		~
mstandfilleru	<u>Back</u> <u>N</u> ext > <u>C</u> ancel	

Figure 10. Set Passwords panel

Enter the following information:

#### Agent Manager Password

This is the resource manager registration password. This password is used to register the Data Server or Device Server with the Agent Manager. Enter the password twice.

Write this password down so that you can provide the proper password when you install the Tivoli Storage Productivity Center server.

**Note:** The default password is **password**. If you want to change this password, see "Changing the registration password for a resource manager" on page 483.

#### **Agent Registration Password**

This is the password used to register the common agents (for Fabric agent and Data agent). You must supply this password when you install the agents. This password locks the agentTrust.jks file. Enter the password twice.

Write this password down so that you can provide the proper password when you install the agents.

**Note:** The default password for this was **changeMe** in Agent Manager 1.2. In Agent Manager 1.3.2, a default password is no longer supplied.

Enter the information and click Next.

- 15. The User Input Summary panel is displayed. Review the information. If you want to change any settings, click **Back** and return to the window where you set the value. When you are satisfied with the changes, click **Next**.
- **16.** You will see several installing progress panels displayed for Embedded WebSphere. Wait for the installation to complete. Click **Next**.
- 17. After Embedded WebSphere has been installed and configured, you will see the summary information panel for Agent Manager. This panel indicates where Agent Manager will be installed and the size of the program. Review the information and click **Next**.
- **18**. You will see several installing progress panels displayed for the Agent Manager. Wait for the installation to complete.
- **19**. The Start the Agent Manager Application Server panel is displayed. You can select the following:
  - Yes, start Agent Manager now
  - No, I will start Agent Manager later

Make a choice and click **Next**. If you select to start the Agent Manager now, a panel is displayed indicating that the WebSphere server is starting the Agent Manager.

- **20**. The Summary of Installation and Configuration Results panel is displayed. This panel indicates if the Agent Manager has successfully installed all of its components. Review the panel. Click **Next**.
- **21**. The Summary Information panel is displayed. If the Agent Manager was installed successfully, the message should be:

The installation is complete and the agent manager application server has been started. Click Finish to exit the installation.

Click Finish.

22. At the end of the installation process, the Agent Manager starts automatically (if you specified that option). After the installation wizard completes, run the **HealthCheck** command to verify that the Agent Manager is running. This command is located in <directory>/toolkit/bin where <directory> is the location where Agent Manager is installed.

One example of using the **HealthCheck** command is to verify that the common agent password you are using is still valid. Here is an example of the command:

HealthCheck -registrationPw changeMe (for Windows)
./HealthCheck.sh -registrationPw changeMe (for UNIX)

# Installing the Agent Manager using a 32-bit DB2 instance - Console install

Use a console-based (command line) installation program to install the Agent Manager using a 32-bit DB2 instance. You must install DB2 before you install the Agent Manager.

The console-based installation program prompts you for values required to install the Agent Manager. In some cases, the prompts have default values, which are displayed in square brackets []. To accept a default value for a prompt, press **Enter** without entering a value for that prompt. For example: Directory Name: [C:\Program Files\IBM\AgentManager]

Press **Enter** in this example to accept the value of C:\Program Files\IBM\ AgentManager for Directory Name.

There are standard values you can enter at a prompt for navigating through the console-based installation program. For example:

- Accept the current value for prompts that list multiple choices: Type **0** and press **Enter**.
- Continue to the next step: Type 1 and press Enter.
- Return to the previous step: Type 2 and press Enter.
- Exit from the installation program: Type 3 and press Enter.
- Redisplay the current prompt: Type 4 and press Enter.

To install the Agent Manager, complete the following steps:

- 1. Log on the machine where you want to install Agent Manager with a user ID that has the appropriate authority:
  - For Windows, you must have administrative authority.
  - For UNIX or Linux, you must have root authority.
- For UNIX or Linux platforms, you need to set the environment variables for the database instance (source db2profile). For example, if your DB2 instance is db2inst1, source the db2profile:
  - . /home/db2inst1/sqllib/db2profile

where home is the home directory of the instance owner.

**3**. Go to the Agent Manager CD or directory where you have downloaded the Agent Manager code. For the CD, select one of the following Agent Manager directory:

Windows/EmbeddedInstaller AIX/EmbeddedInstaller Linux/EmbeddedInstaller

For the electronic image, select one of the following files:

AgentManagerEmbeddedWS\_Aix.tar AgentManagerEmbeddedWS\_Linux.tar AgentManagerEmbeddedWS\_Windows.exe

Untar the file or download the exe file to your Agent Manager source installation directory.

- 4. To start the Agent Manager installation program, run one of the following programs from the Agent Manager CD or source installation directory:
  - For Windows: setupwin32.exe -console
  - For AIX: setupAix.bin -console
  - For Linux: setupLinux.bin -console
  - For Linux on POWER PC: setupLinuxPPC.bin -console
  - For Solaris: setupSolaris.bin -console

For example, type setupAIX.bin -console at a console prompt to run the console version of the Agent Manager installation program on an AIX system. The Choose the runtime container for the Agent Manager: prompt appears.

5. Choose the runtime container that you want to use for the Agent Manager. You have the following options:

# The embedded version of the IBM WebSphere Application Server delivered with the Agent Manager installer.

Select this option. To ensure ease of installation, configuration, and maintenance, Tivoli Storage Productivity Center only supports an Agent Manager configured to run with the embedded version of the IBM WebSphere Application Server.

Follow the command prompts to make your selection. The default selection is The Websphere Application Server. To keep this selection, type **0** at the console prompt, press **Enter**, type **1**, and press **Enter** to continue. To select option 1 The embedded version of the IBM WebSphere Application Server delivered with the Agent Manager installer, type **1**, press **Enter**, type **0**, press **Enter**, type **1**, and press **Enter** to continue. The Directory Name: prompt is displayed.

6. Type the directory name or accept the default directory for where you want to install the Agent Manager These are the default directory paths:

C:\Program Files\IBM\AgentManager (for Windows) /opt/IBM/AgentManager (for UNIX or Linux)

Follow the prompts to indicate your selection and continue to the next prompt. The Type and Location of the Database for the Registry prompt is displayed.

7. Select a database and its location for use with Agent Manager. You have these options:

#### DB2 database on this computer

Select this option. To ensure ease of installation, maintenance, and support, Tivoli Storage Productivity Center only supports an Agent Manager configured to run a local DB2 database server.

DB2 database on another computer (without DB2 Administration Client) Not supported by Tivoli Storage Productivity Center.

# Local alias to a DB2 database on another computer (using DB2 Administration Client)

Not supported by Tivoli Storage Productivity Center.

Oracle database on this computer

Not supported by Tivoli Storage Productivity Center.

Oracle database on another computer (using Oracle Database Client) Not supported by Tivoli Storage Productivity Center.

#### <Derby or Cloudscape> database on this computer Not supported by Tivoli Storage Productivity Center.

Follow the prompts to indicate your selection and continue to the next prompt. The Host Name of DB2 Universal Database Server [localhost] prompt is displayed.

**8**. Enter the following information:

#### **Database Software Directory**

Enter the directory where DB2 is installed. The default directory is:

C:\Program Files\IBM\SQLLIB (for Windows) /<db2home>/<db2instance>/IBM/SQLLIB (for UNIX or Linux)

Follow the prompts to indicate your selection and continue to the next prompt. The Database Runtime User ID [db2admin] prompt is displayed.

9. Enter information about the database in the following prompts:

#### Database Runtime User ID

Enter the database user name. This is the DB2 administrator user ID that is in the DB2ADMNS group and Administrators group.

#### Password

Enter the password for this user ID.

#### Use a different user ID during the installation

If you want to use a different user ID for installation of Agent Manager, type **1**, press **Enter**, type **0**, press **Enter**, and enter the user ID and password in the prompts that follow:

#### **Database Administrator User ID**

Enter the database user name. This is the DB2 administrator user ID that is in the DB2ADMNS group and Administrators group.

#### Password

Enter the password for this user ID.

Follow the prompts to indicate your selections and continue to the next prompt. The Host Name or Alias of Agent Manager [homestar.storage.usca.ubm.com] prompt is displayed.

**10**. Enter the following connection information for the WebSphere Application Server:

#### Host Name or Alias of Agent Manager

If you specify a host name, use the fully qualified host name. For example, specify **mylab.tivlab.raleigh.ibm.com**. This value is used for the URLs for all Agent Manager services. It is preferable to use the fully qualified host name rather than an IP address.

**Note:** If you specify an IP address, you will see this message when you continue:

Do you really want to use the value xxx.xxx.xxx for the agent manager server?

This message explains why it is recommended to use the host name rather than an IP address.

#### **Registration Port**

Use the default port of 9511 for the server-side SSL.

#### Secure Port

Use the default port of 9512 for client authentication, two-way SSL.

**Public Port and Alternate Port for the Agent Recovery Service** Use the public communication port default of 9513.

#### Do not use port 80 for the agent recovery service

Accept the default by typing **0** and pressing Enter. If you select option 1, make sure that port 80 is not being used by another application. To check for other applications which are using port 80, run this command:

netstat -anb (for Windows) netstat -a -n (for Linux)

Look for port 80 in the listening state. This command provides the name of the executable file involved in creating the connection. If

there is an application using port 80, stop that application and then continue with the installation of Agent Manager.

Follow the prompts to indicate your selections and continue to the next prompt. The Application Server Name [AgentManager] prompt is displayed.

- 11. Accept the defaults for the following prompts: Application Server Name [AgentManager], Context Root of Application Server [/AgentMgr], and Automatically start the agent manager each time the system restarts. Follow the prompts to indicate your selections and continue to the next prompt. The Security Certificates prompts are displayed.
- **12.** Specify whether to create new certificates or to use the demonstration certificates. It is highly recommended that you generate new certificates for a secure environment. You have these options:

#### Create certificates for this installation

This is for a secure environment. This is the default and is recommended.

#### Use the demonstration certificates

Provided as a convenience for testing and demonstration purposes.

Follow the prompts to indicate your selection and continue to the next prompt.

**Note:** If you are creating new certificates, back up the certificates in case your Agent Manager server goes down or for disaster recovery purposes. If you do not back up the certificates, you will not be able to recover your system. The Define the Certificate Authority prompts are displayed. These prompts are displayed if you are creating new certificates.

13. Accept the defaults for the following prompts:

#### Certificate Authority Name

Accept the default. This value must be unique in your environment. If you have multiple Agent Managers installed, this value must be different on each Agent Manager. This might apply if you have the Agent Manager software installed for both a testing and production environment.

#### Security Domain

The domain name is used in the right-hand portion of the distinguished name (DN) of every certificate issued by the Agent Manager. It is the name of the security domain defined by the Agent Manager. Typically, this value is the registered domain name or contains the registered domain name. For example, for the computer system myserver.ibm.com, the domain name is ibm.com. This value must be unique in your environment. If you have multiple Agent Managers installed, this value must be different on each Agent Manager.

#### **Certificate Authority Password**

The certificate authority password locks the truststore file. The truststore files are CARootKeyRing.jks and CARootKey.pwd.

Specifying a value for this password is optional. You need to specify this password only if you want to be able to unlock the certificate authority truststore files to examine the certificates that they contain. If you do not specify a value for this password, one is generated automatically and used by the Agent Manager. **Note:** It is recommended that you specify a password so that you can look at the certificate files if you have problems. If you do not specify a password, you will not be able to look at the certificate files. Enter this password.

Follow the prompts to indicate your selection and continue to the next prompt. The Set Passwords prompts are displayed.

14. Enter the following information:

#### Agent Manager Password

This is the resource manager registration password. This password is used to register the Data Server or Device Server with the Agent Manager. Enter the password twice.

Write this password down so that you can provide the proper password when you install the Tivoli Storage Productivity Center server.

**Note:** The default password is **password**. If you want to change this password, see "Changing the registration password for a resource manager" on page 483.

#### Agent Registration Password

This is the password used to register the common agents (for Fabric agent and Data agent). You must supply this password when you install the agents. This password locks the agentTrust.jks file. Enter the password twice.

Write this password down so that you can provide the proper password when you install the agents.

**Note:** The default password for this was **changeMe** in Agent Manager 1.2. In Agent Manager 1.3.2, a default password is no longer supplied.

Follow the prompts to indicate your selection and continue to the next prompt. The first page of the User Input Summary information is displayed.

- 15. Review the information you have defined for the Agent Manager installation. Press Enter to continue to the next page. The second page of the User Input Summary information is displayed
- **16.** Review the information you have defined for the Agent Manager installation. Perform any of the following actions:
  - Type 1 and press Enter to install Agent Manager.
  - Type **2** and press **Enter** if you want to change the previous settings. You can continue to type **2** and press **Enter** to go back through all the previous prompts in the installation program.
  - Type **3** and press **Enter** to exit the installation program without installing Agent Manager.
  - Type 4 and press Enter to redisplay the user input summary information.

Continue to the next step if you type **1** and presses **Enter** to install the Agent Manager.

- 17. You will see several installing progress panels displayed for Embedded WebSphere. Wait for the installation to complete. Click **Next**.
- **18**. After Embedded WebSphere has been installed and configured, you will see the summary information panel for Agent Manager. This information indicates where Agent Manager will be installed and the size of the program. Review

the information and follow the prompts to continue. Several installing progress panels are displayed for the Agent Manager.

- 19. Wait for the installation to complete. The Start the AgentManager Application Server prompt is displayed.
- 20. Select one of the following options:
  - Yes, start AgentManager now
  - No, I will start AgentManager later

Make a choice and follow the prompts to continue. If you select to start the Agent Manager now, a message is displayed indicating that the WebSphere server is starting the Agent Manager. The Summary of Installation and Configuration Results information is displayed. This information indicates if the Agent Manager has successfully installed all of its components.

**21.** Review the panel and follow the prompts to continue. The Summary Information prompt is displayed. If the Agent Manager was installed successfully, the message should be:

The installation is complete and the agent manager application server has been started. Click Finish to exit the installation.

- 22. Follow the prompts to finish the installation.
- 23. At the end of the installation process, the Agent Manager starts automatically (if you specified that option). After the installation wizard completes, run the **HealthCheck** command to verify that the Agent Manager is running. This command is located in <directory>/toolkit/bin where <directory> is the location where Agent Manager is installed.

One example of using the **HealthCheck** command is to verify that the common agent password you are using is still valid. Here is an example of the command:

HealthCheck -registrationPw changeMe (for Windows)
./HealthCheck.sh -registrationPw changeMe (for UNIX)

# Installing the Agent Manager using a 64-bit DB2 instance - GUI install

Use a GUI-based installation program to install the Agent Manager using a 64-bit DB2 instance. You must install DB2 before you install the Agent Manager.

To install the Agent Manager, complete the following steps:

- 1. Log on as the root user of the Agent Manager host system.
- 2. Set the environment variables for the database instance (source db2profile). For example, if your DB2 instance is **db2inst1**, source the db2profile:
  - . /home/db2inst1/sqllib/db2profile

where home is the home directory of the instance owner.

Note: The dot, space, and slash syntax is important.

**3**. Enable TCP/IP communication. You must enable TCP/IP communication to be able to install Agent Manager with a 64-bit DB2 instance. Run the db2set command to check for the DB2COMM variable. Open a DB2 command prompt and run the command:

db2set DB2COMM=tcpip

The correct value returned is tcpip. If TCP/IP communication for the DB2 instance is not set, use the following documentation to configure it:

- For DB2 v9.1, see http://publib.boulder.ibm.com/infocenter/db2luw/v9/ index.jsp?topic=/com.ibm.db2.udb.uprun.doc/doc/t0004727.htm.
- For DB2 v9.5, see http://publib.boulder.ibm.com/infocenter/db2luw/v9/ index.jsp?topic=/com.ibm.db2.udb.uprun.doc/doc/t0004727.htm.
- 4. Configure the database on the DB2 instance.
  - a. Open a DB2 command prompt by typing **db2** in the shell command prompt.
  - b. Create this database object without any schema. Use the following command:

db2 =>CREATE DATABASE <DATABASE\_NAME> USING CODESET UTF-8 TERRITORY US

Where <DATABASE\_NAME> is the name of the database that is created. For example:

db2 =>CREATE DATABASE IBMCDB USING CODESET UTF-8 TERRITORY US DB20000I The CREATE DATABASE command completed successfully.

c. For DB2 v9.1 or 9.5: Run the following command:

db2 =>UPDATE DATABASE CONFIGURATION FOR <DATABASE NAME> USING DBHEAP 8192 APPLHEAPSZ 4096 APP CTL HEAP SZ 512 STMTHEAP 32768 PCKCACHESZ 2000 CATALOGCACHE SZ 360 LOGBUFSZ 800 UTIL HEAP SZ 10000 STAT\_HEAP\_SZ 6000 MINCOMMIT 1 NUM IOCLEANERS 1 NUM IOSERVERS 3 MAXAPPLS 120 AVG APPLS 5 NUM DB BACKUPS 30 LOGPRIMARY 6 LOGSECOND 50 LOGFILSIZ 1024

Where <DATABASE\_NAME> is the name of the database which is created. For example:

db2 => UPDATE DATABASE CONFIGURATION FOR IBMCDB USING DBHEAP 8192 APPLHEAPSZ 4096 APP\_CTL\_HEAP\_SZ 512 STMTHEAP 32768 PCKCACHESZ 2000 CATALOGCACHE\_SZ 360 LOGBUFSZ 800 UTIL\_HEAP\_SZ 10000 STAT\_HEAP\_SZ 6000 MINCOMMIT 1 NUM\_IOCLEANERS 1 NUM\_IOSERVERS 3 MAXAPPLS 120 AVG\_APPLS 5 LOGPRIMARY 6 LOGSECOND 50 LOGFILSIZ 1024 DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully.

d. Run this command to check if the database was created:

db2 => list db directory

System Database Directory

Number of entries in the directory = 1

Database 1 entry:

Database alias	= IBMCDB
Database name	= IBMCDB
Local database directory	= /home/db2inst1
Database release level	= b.00
Comment	=
Directory entry type	= Indirect

Catalog (	database	parti	tion	number	-	=	0
Alternat	e server	hostn	ame		-	=	
Alternat	e server	port	numbe	er		=	

- e. Type QUIT at the command prompt to exit DB2 interactive mode.
- Go to the Agent Manager CD or directory where you have downloaded the Agent Manager code. For the CD, select one of the following Agent Manager directory:

AIX/EmbeddedInstaller Linux/EmbeddedInstaller

For the electronic image, select one of the following files: AgentManagerEmbeddedWS\_Aix.tar AgentManagerEmbeddedWS\_Linux.tar

Untar the file to your Agent Manager source installation directory.

- 6. To start the Agent Manager installation program in a GUI format, run one of the following programs from the Agent Manager CD or source installation directory:
  - For AIX: setupAix.bin
  - For Linux: setupLinux.bin
  - For Linux on POWER PC: setupLinuxPPC.bin
  - For Solaris: setupSolaris.bin

The Choose the runtime container for Agent Manager panel is displayed.

7. Choose the runtime container that you want to use for the Agent Manager. You have the following options:

# The embedded version of the IBM WebSphere Application Server delivered with the Agent Manager installer.

Select this option. To ensure ease of installation, configuration, and maintenance, Tivoli Storage Productivity Center only supports an Agent Manager configured to run with the embedded version of the IBM WebSphere Application Server.

Click Next to continue. The Directory Name panel is displayed.

8. Type the directory name or accept the default directory for where you want to install the Agent Manager. These are the default directory paths:

C:\Program Files\IBM\AgentManager (for Windows) /opt/IBM/AgentManager (for UNIX or Linux)

Enter the directory name and click **Next** to continue. The Type and Location of Registry panel is displayed.

- 9. Select **DB2 database on another computer (without DB2 Administration Client)**. Even though the database is on the same local machine as the Agent Manager, this forces the use of the Type 4 JDBC driver. Click **Next** to continue. The DB2 Universal Database Connection Information panel is displayed.
- 10. Set the following for the fields and prompts:

#### Host Name of DB2 Universal Database Server Enter localhost.

#### Database port

Enter the port number on which the DB2 instance is running. 50000 is the default.

#### Database Name

Enter the name of the newly created database from step 4.

#### Location of the DB2 Universal Database Type 4 Drivers for JDBC

Enter the directory where DB2 is installed. The default directory is:

C:\Program Files\IBM\SQLLIB (for Windows) /<db2home>/<db2instance>/IBM/SQLLIB (for UNIX or Linux)

#### The following text appears:

Because you are not using the DB2 Administration Client to connect to the remote database, the database must be preconfigured on the remote system before you continue. For instructions for preconfiguring the database, see the agent manager documentation about configuring a remote registry.

Click Next to continue. The Database User Information panel is displayed.

11. Enter the following information:

#### Database Runtime User ID

Enter the database user name. This is the DB2 administrator user ID that is in the DB2ADMNS group and Administrators group.

#### Password

Enter the password for this user ID.

#### Use a different user ID during the installation

If you want to use a different user ID for installation of Agent Manager, select this check box and enter the user ID and password:

#### Database Administrator User ID

Enter the database user name. This is the DB2 administrator user ID that is in the DB2ADMNS group and Administrators group.

#### Password

Enter the password for this user ID.

12. The WebSphere Application Server Connection Information panel is displayed.
| InstallShield Wizard for I | nstalling the Agent Manager                                                                                                                                                                                                                                                                                              | K |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
|                            | WebSphere Application Server Connection Information                                                                                                                                                                                                                                                                      |   |
| TRM                        | Host Name or Alias of Agent Manager                                                                                                                                                                                                                                                                                      |   |
|                            | Tip: This is the network name that common agents and resource managers use to<br>connect to the agent manager. Use a host name that can be resolved by those systems.<br>For example, use a network alias such as AgentManagerServer or a fully qualified host<br>name such as agman.mycompany.com.<br>Registration Port |   |
| STILL BERTHE               | 9511                                                                                                                                                                                                                                                                                                                     |   |
|                            | Secure Port                                                                                                                                                                                                                                                                                                              |   |
|                            | 9512                                                                                                                                                                                                                                                                                                                     | L |
|                            | Public Port and Alternate Port for the Agent Recovery Service                                                                                                                                                                                                                                                            |   |
|                            | 9513                                                                                                                                                                                                                                                                                                                     |   |
|                            | Do not use port 80 for the agent recovery service                                                                                                                                                                                                                                                                        |   |
| hand a little back         |                                                                                                                                                                                                                                                                                                                          |   |
| InstallShield              | < Back Next > Cancel                                                                                                                                                                                                                                                                                                     | ) |

Figure 11. WebSphere Application Server Connection Information panel

Enter the following information:

## Host Name or Alias of Agent Manager

If you specify a host name, use the fully qualified host name. For example, specify **mylab.tivlab.raleigh.ibm.com**. This value is used for the URLs for all Agent Manager services. It is preferable to use the fully qualified host name rather than an IP address.

**Note:** If you specify an IP address, you will see this panel when you click **Next**.

Do you really want to use the value xxx.xxx.xxx for the agent manager server?

This panel explains why it is recommended to use the host name rather than an IP address.

## **Registration Port**

Use the default port of 9511 for the server-side SSL.

## **Secure Port**

Use the default port of 9512 for client authentication, two-way SSL.

## **Public Port and Alternate Port for the Agent Recovery Service** Use the public communication port default of 9513.

#### Do not use port 80 for the agent recovery service

Accept the default and do not check this box. If you check this box, make sure that port 80 is not being used by another application. To check for other applications which are using port 80, run this command:

netstat -anb (for Windows) netstat -a -n (for Linux) Look for port 80 in the listening state. This command provides the name of the executable file involved in creating the connection. If there is an application using port 80, stop that application and then continue with the installation of Agent Manager.

Enter the information and click Next.

13. The WebSphere Application Server Connection Information panel is displayed.

InstallShield Wizard for	Installing the Agent Manager
	WebSphere Application Server Connection Information
	Application Server Name
IBM.	AgentManager
	Use this name to start and stop the application server and to locate the agent manager files in the WebSphere directory.
	/AgentMgr
	The context root is part of the URL that common agents and resource managers use to contact the agent manager. The underlined string in the following URL, including the forward slash, is the context root: http://IBM-84AA714148F.krakow.pl.ibm.com:9513 <u>/AgentMgr</u>
InstallShield	< <u>B</u> ack <u>N</u> ext > <u>C</u> ancel

Figure 12. WebSphere Application Server Connection Information panel

Accept the defaults and click Next.

14. The Security Certificates panel is displayed.

InstallShield Wizard for	Installing the Agent Manager
	Security Certificates
IBM.	Do you want to create certificates that are specific to this installation of the agent manager, or use the demonstration certificates?
	Oreate certificates for this installation
	O Use the demonstration certificates
	Demonstration certificates are publicly available and do not provide the level of security required by a typical IT environment. They are provided for testing or demonstration environments only.
InstallShield	< Back Next > Cancel

Figure 13. Security Certificates panel

Specify whether to create new certificates or to use the demonstration certificates. It is highly recommended that you generate new certificates for a secure environment. You have these options:

## Create certificates for this installation

This is for a secure environment. This is the default and is recommended.

## Use the demonstration certificates

Provided as a convenience for testing and demonstration purposes.

Make a selection and click Next.

**Note:** If you are creating new certificates, back up the certificates in case your Agent Manager server goes down or for disaster recovery purposes. If you do not back up the certificates, you will not be able to recover your system.

15. The Define the Certificate Authority panel is displayed.

linstallShield Wizard for I	nstalling the Agent Manager	
	Define the Certificate Authority	62
	Certificate Authority Name	
IBM.	TivoliAgentManagerCA	
	Security Domain	
	krakow.pl.ibm.com	
	Certificate Authority Password This password locks the certificate authority truststore. The CA password is typically use only by the agent manager.	łd
	If your security policies do not require you to examine the contents of the CA truststore	
	Password	
	Confirm Password	
InstallShield		
	<u>Back</u> <u>N</u> ext > <u>C</u> ancel	

Figure 14. Define the Certificate Authority panel

This panel is displayed if you are creating new certificates. Accept all the defaults.

Provide this information:

## Certificate Authority Name

Accept the default. This value must be unique in your environment. If you have multiple Agent Managers installed, this value must be different on each Agent Manager. This might apply if you have the Agent Manager software installed for both a testing and production environment.

## Security Domain

The domain name is used in the right-hand portion of the distinguished name (DN) of every certificate issued by the Agent Manager. It is the name of the security domain defined by the Agent Manager. Typically, this value is the registered domain name or contains the registered domain name. For example, for the computer system myserver.ibm.com, the domain name is ibm.com. This value must be unique in your environment. If you have multiple Agent Managers installed, this value must be different on each Agent Manager.

## **Certificate Authority Password**

The certificate authority password locks the truststore file. The truststore files are CARootKeyRing.jks and CARootKey.pwd.

Specifying a value for this password is optional. You need to specify this password only if you want to be able to unlock the certificate authority truststore files to examine the certificates that they contain. If you do not specify a value for this password, one is generated automatically and used by the Agent Manager. **Note:** It is recommended that you specify a password so that you can look at the certificate files if you have problems. If you do not specify a password, you will not be able to look at the certificate files. Enter this password.

Enter the information and click Next.

16. The Set Passwords panel is displayed.

linstallShield Wizard for	Installing the Agent Manager	
	Set Passwords	101100
	Agent Manager Password This password looks the agent manager trustatore file (AgentManagerTrust.jks) and keystore file (agentManagerKeys.jks). This password is used internally by the agent manager. Password Confirm Password Agent Registration Password A common agent must provide this password to register with the agent manager. This password also looks the agentTrust.jks truststore file. A common agent or resource manager compares the certificate in its copy of the agentTrust.jks file with the certificate presented by the agent manager to make sure that it registers with the correct agent manager. This password is required to install a common agent or a resource manager. Password	
		V
InstallShield		
	≪ <u>B</u> ack <u>N</u> ext > <u>C</u> ance	el 📄

Figure 15. Set Passwords panel

Enter the following information:

#### Agent Manager Password

This is the resource manager registration password. This password is used to register the Data Server or Device Server with the Agent Manager. Enter the password twice.

Write this password down so that you can provide the proper password when you install the Tivoli Storage Productivity Center server.

**Note:** The default password is **password**. If you want to change this password, see "Changing the registration password for a resource manager" on page 483.

#### Agent Registration Password

This is the password used to register the common agents (for Fabric agent and Data agent). You must supply this password when you install the agents. This password locks the agentTrust.jks file. Enter the password twice.

Write this password down so that you can provide the proper password when you install the agents.

**Note:** The default password for this was **changeMe** in Agent Manager 1.2. In Agent Manager 1.3.2, a default password is no longer supplied.

Enter the information and click Next.

- 17. The User Input Summary panel is displayed. Review the information. If you want to change any settings, click **Back** and return to the window where you set the value. When you are satisfied with the changes, click **Next**.
- **18.** You will see several installing progress panels displayed for Embedded WebSphere. Wait for the installation to complete. Click **Next**.
- **19**. After Embedded WebSphere has been installed and configured, you will see the summary information panel for Agent Manager. This panel indicates where Agent Manager will be installed and the size of the program. Review the information and click **Next**.
- **20.** You will see several installing progress panels displayed for the Agent Manager. Wait for the installation to complete.
- **21**. The Start the Agent Manager Application Server panel is displayed. You can select the following:
  - Yes, start Agent Manager now
  - No, I will start Agent Manager later

Make a choice and click **Next**. If you select to start the Agent Manager now, a panel is displayed indicating that the WebSphere server is starting the Agent Manager.

- **22**. The Summary of Installation and Configuration Results panel is displayed. This panel indicates if the Agent Manager has successfully installed all of its components. Review the panel. Click **Next**.
- **23**. The Summary Information panel is displayed. If the Agent Manager was installed successfully, the message should be:

The installation is complete and the agent manager application server has been started. Click Finish to exit the installation.

Click Finish.

24. At the end of the installation process, the Agent Manager starts automatically (if you specified that option). After the installation wizard completes, run the **HealthCheck** command to verify that the Agent Manager is running. This command is located in <directory>/toolkit/bin where <directory> is the location where Agent Manager is installed.

One example of using the **HealthCheck** command is to verify that the common agent password you are using is still valid. Here is an example of the command:

HealthCheck -registrationPw changeMe (for Windows)
./HealthCheck.sh -registrationPw changeMe (for UNIX)

# Installing the Agent Manager using a 64-bit DB2 instance - Console install

Use a console-based (command line) installation program to install the Agent Manager using a 64-bit DB2 instance. You must install DB2 before you install the Agent Manager.

The console-based installation program prompts you for values required to install the Agent Manager. In some cases, the prompts have default values, which are displayed in square brackets []. To accept a default value for a prompt, press Enter without entering a value for that prompt. For example: Directory Name: [C:\Program Files\IBM\AgentManager]

Press Enter in this example to accept the value of C:\Program Files\IBM\ AgentManager for Directory Name.

There are standard values you can enter at a prompt for navigating through the console-based installation program. For example:

- Accept the current value for prompts that list multiple choices: Type **0** and press **Enter**.
- Continue to the next step: Type 1 and press Enter.
- Return to the previous step: Type **2** and press **Enter**.
- Exit from the installation program: Type 3 and press Enter.
- Redisplay the current prompt: Type 4 and press Enter.

To install the Agent Manager, complete the following steps:

- 1. Log on as the root user of the Agent Manager host system.
- 2. Set the environment variables for the database instance (source db2profile). For example, if your DB2 instance is **db2inst1**, source the db2profile:
  - . /home/db2inst1/sqllib/db2profile

where home is the home directory of the instance owner.

**Note:** The dot, space, and slash syntax is important.

3. Enable TCP/IP communication. You must enable TCP/IP communication to be able to install Agent Manager with a 64-bit DB2 instance. Run the db2set command to check for the DB2COMM variable. Open a DB2 command prompt and run the command:

db2set DB2COMM=tcpip

The correct value returned is tcpip. If TCP/IP communication for the DB2 instance is not set, use the following documentation to configure it:

- For DB2 v9.1, see http://publib.boulder.ibm.com/infocenter/db2luw/v9/ index.jsp?topic=/com.ibm.db2.udb.uprun.doc/doc/t0004727.htm.
- For DB2 v9.5, see http://publib.boulder.ibm.com/infocenter/db2luw/v9/ index.jsp?topic=/com.ibm.db2.udb.uprun.doc/doc/t0004727.htm.
- 4. Configure the database on the DB2 instance.
  - a. Open a DB2 command prompt by typing **db2** in the shell command prompt.
  - b. Create this database object without any schema. Use the following command:

db2 =>CREATE DATABASE <DATABASE\_NAME> USING CODESET UTF-8 TERRITORY US;

Where <DATABASE\_NAME> is the name of the database that is created. For example:

db2 =>CREATE DATABASE IBMCDB USING CODESET UTF-8 TERRITORY US; DB20000I The CREATE DATABASE command completed successfully.

c. For DB2 V9.1 or V9.5: Run the following command:

db2 =>UPDATE DATABASE CONFIGURATION FOR <DATABASE\_NAME> USING DBHEAP 8192 APPLHEAPSZ 4096 APP\_CTL\_HEAP\_SZ 512 STMTHEAP 32768 PCKCACHESZ 2000 CATALOGCACHE\_SZ 360 LOGBUFSZ 800 UTIL\_HEAP\_SZ 10000 STAT\_HEAP\_SZ 6000 MINCOMMIT 1 NUM\_IOCLEANERS 1 NUM\_IOSERVERS 3 MAXAPPLS 120 AVG\_APPLS 5 NUM\_DB\_BACKUPS 30 LOGPRIMARY 6 LOGSECOND 50 LOGFILSIZ 1024

Where <DATABASE\_NAME> is the name of the database which is created. For example:

db2 => UPDATE DATABASE CONFIGURATION FOR IBMCDB USING DBHEAP 8192 APPLHEAPSZ 4096 APP\_CTL\_HEAP\_SZ 512 STMTHEAP 32768 PCKCACHESZ 2000 CATALOGCACHE SZ 360 LOGBUFSZ 800 UTIL\_HEAP\_SZ 10000 STAT\_HEAP\_SZ 6000 MINCOMMIT 1 NUM\_IOCLEANERS 1 NUM\_IOSERVERS 3 MAXAPPLS 120 AVG\_APPLS 5 LOGPRIMARY 6 LOGSECOND 50 LOGFILSIZ 1024 DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully.

d. Run this command to check if the database was created:

```
db2 => list db directory
```

System Database Directory

Number of entries in the directory = 1

Database 1 entry:

Database alias	= IBMCDB
Database name	= IBMCDB
Local database directory	= /home/db2inst1
Database release level	= b.00
Comment	=
Directory entry type	= Indirect
Catalog database partition number	= 0
Alternate server hostname	=
Alternate server port number	=

- e. Type **QUIT** at the command prompt to exit DB2 interactive mode.
- Go to the Agent Manager CD or directory where you have downloaded the Agent Manager code. For the CD, select one of the following Agent Manager directory:

```
AIX/EmbeddedInstaller
Linux/EmbeddedInstaller
```

For the electronic image, select one of the following files:

AgentManagerEmbeddedWS\_Aix.tar AgentManagerEmbeddedWS\_Linux.tar

Untar the file or download the exe file to your Agent Manager source installation directory.

- 6. To start the Agent Manager installation program, run one of the following programs from the Agent ManagerAgent Manager CD or source installation directory:
  - For AIX: setupAix.bin -console
  - For Linux: setupLinux.bin -console
  - For Linux on POWER PC: setupLinuxPPC.bin -console

• For Solaris: setupSolaris.bin -console

For example, type setupAIX.bin -console at a console prompt to run the console version of the Agent Manager installation program on an AIX system. The Choose the runtime container for the Agent Manager: prompt appears.

7. Choose the runtime container that you want to use for the Agent Manager.

You have the following options:

## The embedded version of the IBM WebSphere Application Server delivered with the Agent Manager installer.

Select this option. To ensure ease of installation, configuration, and maintenance, Tivoli Storage Productivity Center only supports an Agent Manager configured to run with the embedded version of the IBM WebSphere Application Server.

Follow the command prompts to make your selection. The default selection is The Websphere Application Server. To keep this selection, type **0** at the console prompt, press **Enter**, type **1**, and press **Enter** to continue. To select option 1 The embedded version of the IBM WebSphere Application Server delivered with the Agent Manager installer, type **1**, press **Enter**, type **0**, press **Enter**, type **1**, and press **Enter** to continue. The Directory Name: prompt is displayed.

8. Type the directory name or accept the default directory for where you want to install the Agent Manager These are the default directory paths:

C:\Program Files\IBM\AgentManager (for Windows) /opt/IBM/AgentManager (for UNIX or Linux)

Follow the prompts to indicate your selection and continue to the next prompt. The Type and Location of the Database for the Registry prompt is displayed.

- 9. Select DB2 database on another computer (without DB2 Administration Client). Even though the database is on the same local machine as the Agent Manager, this forces the use of the Type 4 JDBC driver. Click Next to continue. The DB2 Universal Database Connection Information prompts are displayed.
- 10. Enter information for the following prompts:

## Host Name of DB2 Universal Database Server Enter localhost.

## Database port

Enter the port number on which the DB2 instance is running. 50000 is the default.

## Database Name

Enter the name of the newly created database from step 4.

## Location of the DB2 Universal Database Type 4 Drivers for JDBC

Enter the directory where DB2 is installed. The default directory is:

C:\Program Files\IBM\SQLLIB (for Windows) /<db2home>/<db2instance>/IBM/SQLLIB (for UNIX or Linux)

The following text appears:

Because you are not using the DB2 Administration Client to connect to the remote database, the database must be preconfigured on the remote system before you continue. For instructions for preconfiguring the database, see the agent manager documentation about configuring a remote registry.

Click Next to continue. The Database User Information prompts are displayed.

11. Enter information about the database in the following prompts:

## Database Runtime User ID

Enter the database user name. This is the DB2 administrator user ID that is in the DB2ADMNS group and Administrators group.

#### Password

Enter the password for this user ID.

## Use a different user ID during the installation

If you want to use a different user ID for installation of Agent Manager, type **1**, press Enter, type **0**, press Enter, and enter the user ID and password in the prompts that follow:

## Database Administrator User ID

Enter the database user name. This is the DB2 administrator user ID that is in the DB2ADMNS group and Administrators group.

#### Password

Enter the password for this user ID.

Follow the prompts to indicate your selections and continue to the next prompt. The WebSphere Application Server Connection Information prompts are displayed.

**12.** Enter the following connection information for the WebSphere Application Server:

#### Host Name or Alias of Agent Manager

If you specify a host name, use the fully qualified host name. For example, specify **mylab.tivlab.raleigh.ibm.com**. This value is used for the URLs for all Agent Manager services. It is preferable to use the fully qualified host name rather than an IP address.

**Note:** If you specify an IP address, you will see this message when you continue:

Do you really want to use the value xxx.xxx.xxx for the agent manager server?

This message explains why it is recommended to use the host name rather than an IP address.

## **Registration Port**

Use the default port of 9511 for the server-side SSL.

#### Secure Port

Use the default port of 9512 for client authentication, two-way SSL.

**Public Port and Alternate Port for the Agent Recovery Service** Use the public communication port default of 9513.

## Do not use port 80 for the agent recovery service

Accept the default by typing **0** and pressing Enter. If you select option 1, make sure that port 80 is not being used by another application. To check for other applications which are using port 80, run this command:

netstat -anb (for Windows) netstat -a -n (for Linux)

Look for port 80 in the listening state. This command provides the name of the executable file involved in creating the connection. If

there is an application using port 80, stop that application and then continue with the installation of Agent Manager.

Follow the prompts to indicate your selections and continue to the next prompt. The Application Server Name [AgentManager] prompt is displayed.

- 13. Accept the defaults for the following prompts: Application Server Name [AgentManager], Context Root of Application Server [/AgentMgr], and Automatically start the agent manager each time the system restarts. Follow the prompts to indicate your selections and continue to the next prompt. The Security Certificates prompts are displayed.
- 14. Specify whether to create new certificates or to use the demonstration certificates. It is highly recommended that you generate new certificates for a secure environment. You have these options:

#### Create certificates for this installation

This is for a secure environment. This is the default and is recommended.

## Use the demonstration certificates

Provided as a convenience for testing and demonstration purposes.

Follow the prompts to indicate your selection and continue to the next prompt.

**Note:** If you are creating new certificates, back up the certificates in case your Agent Manager server goes down or for disaster recovery purposes. If you do not back up the certificates, you will not be able to recover your system. The Define the Certificate Authority prompts are displayed. These prompts are displayed if you are creating new certificates.

15. Accept the defaults for the following prompts:

## Certificate Authority Name

Accept the default. This value must be unique in your environment. If you have multiple Agent Managers installed, this value must be different on each Agent Manager. This might apply if you have the Agent Manager software installed for both a testing and production environment.

#### Security Domain

The domain name is used in the right-hand portion of the distinguished name (DN) of every certificate issued by the Agent Manager. It is the name of the security domain defined by the Agent Manager. Typically, this value is the registered domain name or contains the registered domain name. For example, for the computer system myserver.ibm.com, the domain name is ibm.com. This value must be unique in your environment. If you have multiple Agent Managers installed, this value must be different on each Agent Manager.

## **Certificate Authority Password**

The certificate authority password locks the truststore file. The truststore files are CARootKeyRing.jks and CARootKey.pwd.

Specifying a value for this password is optional. You need to specify this password only if you want to be able to unlock the certificate authority truststore files to examine the certificates that they contain. If you do not specify a value for this password, one is generated automatically and used by the Agent Manager. **Note:** It is recommended that you specify a password so that you can look at the certificate files if you have problems. If you do not specify a password, you will not be able to look at the certificate files. Enter this password.

Follow the prompts to indicate your selection and continue to the next prompt. The Set Passwords prompts are displayed.

**16**. Enter the following information:

#### Agent Manager Password

This is the resource manager registration password. This password is used to register the Data Server or Device Server with the Agent Manager. Enter the password twice.

Write this password down so that you can provide the proper password when you install the Tivoli Storage Productivity Center server.

**Note:** The default password is **password**. If you want to change this password, see "Changing the registration password for a resource manager" on page 483.

#### Agent Registration Password

This is the password used to register the common agents (for Fabric agent and Data agent). You must supply this password when you install the agents. This password locks the agentTrust.jks file. Enter the password twice.

Write this password down so that you can provide the proper password when you install the agents.

**Note:** The default password for this was **changeMe** in Agent Manager 1.2. In Agent Manager 1.3.2, a default password is no longer supplied.

Follow the prompts to indicate your selection and continue to the next prompt. The first page of the User Input Summary information is displayed.

- Review the information you have defined for the Agent Manager installation. Press Enter to continue to the next page. The second page of the User Input Summary information is displayed
- **18**. Review the information you have defined for the Agent Manager installation. Perform any of the following actions:
  - Type 1 and press Enter to install Agent Manager.
  - Type **2** and press **Enter** if you want to change the previous settings. You can continue to type **2** and press **Enter** to go back through all the previous prompts in the installation program.
  - Type **3** and press **Enter** to exit the installation program without installing Agent Manager.
  - Type 4 and press Enter to redisplay the user input summary information.

Continue to the next step if you type **1** and press **Enter** to install the Agent Manager.

- **19.** You will see several installing progress panels displayed for Embedded WebSphere. Wait for the installation to complete. Click **Next**.
- **20.** After Embedded WebSphere has been installed and configured, you will see the summary information panel for Agent Manager. This information indicates where Agent Manager will be installed and the size of the program. Review

the information and follow the prompts to continue. Several installing progress panels are displayed for the Agent Manager.

- 21. Wait for the installation to complete. The Start the AgentManager Application Server prompt is displayed.
- 22. Select one of the following options:
  - Yes, start AgentManager now
  - No, I will start AgentManager later

Make a choice and follow the prompts to continue. If you select to start the Agent Manager now, a message is displayed indicating that the WebSphere server is starting the Agent Manager. The Summary of Installation and Configuration Results information is displayed. This information indicates if the Agent Manager has successfully installed all of its components.

**23**. Review the panel and follow the prompts to continue. The Summary Information prompt is displayed. If the Agent Manager was installed successfully, the message should be:

The installation is complete and the agent manager application server has been started. Click Finish to exit the installation.

- **24**. Follow the prompts to finish the installation.
- 25. At the end of the installation process, the Agent Manager starts automatically (if you specified that option). After the installation wizard completes, run the **HealthCheck** command to verify that the Agent Manager is running. This command is located in <directory>/toolkit/bin where <directory> is the location where Agent Manager is installed.

One example of using the **HealthCheck** command is to verify that the common agent password you are using is still valid. Here is an example of the command:

HealthCheck -registrationPw changeMe (for Windows)
./HealthCheck.sh -registrationPw changeMe (for UNIX)

## Installing the IBM Tivoli Storage Productivity Center family

This topic describes how to prepare for and install IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication.

Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication provides an installation program that helps guide you through the installation process. You can use typical installation or custom installation to install Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication.

## Preparing for installation

This topic provides information on what you need to do to prepare for installing IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication.

Before you begin the installation, complete the following steps:

- 1. Make sure you have the correct version of DB2 and Agent Manager installed on your system. (The Agent Manager could be on a remote computer.) Also make sure that DB2 is running.
- 2. Ensure that you do not have any port conflicts. See "TCP/IP ports used by the IBM Tivoli Storage Productivity Center family" on page 19.

- **3**. Make sure that your computers are using fully qualified host names. Make sure you change the HOSTS file. For information about the HOSTS file, see "Changing the HOSTS file" on page 323.
- 4. Check the readme file on the product CD for additional information about using the product. The readme files are in the readme directory. The files are: readme tpc <language>.txt

Where *language* can be one of the following:

- en English
- cs Czech
- de German
- es Spanish
- fr French
- hu Hungarian
- it Italian
- ja Japanese
- ko Korean
- pl Polish
- ru Russian
- pt\_BR Brazilian Portuguese
- zh\_CN Simplified Chinese
- zh\_TW Traditional Chinese
- 5. Check for any *Flashes* on the following Web site. The *Flash* contains last minute information that could not be included in the documentation. Click http://www.ibm.com/systems/support/storage/software/tpc/ Click on a product. Then click on **Flashes**.
- 6. It is a good practice to subscribe to the Tivoli Storage Productivity Center technical support Web site to receive information about important technical notes, flashes, and APAR information.

To receive future support notifications, go to the right and under **Stay informed**, click **Subscribe**. You will be required to enter your IBM ID and password. Once authenticated, you will see a Subscriptions page which provides information about the following:

- · How to create and organize subscriptions
- How you are notified about subscriptions
- How to specify the frequency of e-mail notifications
- How to subscribe for specific topics per product
- How to unsubscribe
- 7. If you are installing the server on a UNIX computer, you must set up your shell environment to point to the instance where the repository will be installed. To do this, source the **db2profile** script for the desired instance. For example, if the DB2 instance is **db2inst1**, perform the following steps:
  - a. Source the file by typing . /home/db2inst1/sqllib/db2profile
  - b. Start the installation program.
- 8. Plan for the user IDs and passwords you expect to use.
- **9**. If you install Tivoli Storage Productivity Center and select to authenticate users against an LDAP-compliant directory, then make sure you have all the necessary LDAP information:
  - Fully-qualified hostname of the server running the LDAP-compliant directory
  - Port on which the LDAP-compliant directory is listening
  - The Bind Distinguished Name and password for connecting to the LDAP-compliant directory

- The Relative Distinguished Names for the Tivoli Storage Productivity Center users and groups in the LDAP-compliant directory
- The attributes used to "name" the Tivoli Storage Productivity Center users and groups in the LDAP-compliant directory
- The LDAP TPC Administrator username and password; this must an existing entry in the LDAP-compliant directory in the "branch" specified by the "Relative Distinguished Name for usernames" value
- The LDAP TPC Administrator group; this must an existing entry in the LDAP-compliant directory in the "branch" specified by the "Relative Distinguished Name for groups" value; the LDAP TPC Administrator user must be a member of this group

## Note:

- On Windows, you cannot run the Tivoli Storage Productivity Center installation program from a network share (for example, Universal Naming Convention format). You must map your network share to your local drive and run the installation program from that drive.
- For custom installation: in UNIX, the Tivoli Storage Productivity Center installation program validates the WebSphere user ID and then gives an error if that user ID does not exist. In Windows, the Tivoli Storage Productivity Center installation program will create the WebSphere user ID if that user ID does not exist.
- For information about installing the Data agent and Fabric agent in silent mode, see "Installing IBM Tivoli Storage Productivity Center in silent mode" on page 262.
- If you are using an IPv6 machine, see "Planning for Internet Protocol Version 6" on page 34.

# Preparing to install Storage Resource agents remotely on Windows 2008 and Windows Vista

If you are planning to install Storage Resource agents remotely on a Windows 2008 or Windows Vista system, you must disable the User Account Control (UAC) remote restrictions on the Windows system. User Account Control is a security component on Windows.

**Note:** This task contains steps that tell you how to modify the registry. Serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then you can restore the registry if problems occur. For information about how to back up and restore the registry, see http://support.microsoft.com/kb/322756/.

To disable UAC remote restrictions, follow these steps:

- 1. Click **Start > Run**. Enter **regedit** and click **OK**.
- 2. Locate and click the following registry subkey:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

- **3.** If the LocalAccountTokenFilterPolicy registry entry does not exist, follow these steps:
  - a. On the Edit menu, click New > DWORD Value.
  - b. Enter LocalAccountTokenFilterPolicy as the name for the DWORD value in the right pane. Click Enter.
  - c. Right-click LocalAccountTokenFilterPolicy, then click Modify.

- d. In the Edit DWORD Value window, enter **1**, then click **OK**. This value can be 0 or 1:
  - **0** This value builds a filtered token. This is the default value. The administrator credentials are removed.
  - 1 This value builds an elevated token.
- e. Exit the registry editor.

## Starting the installation program

This topic describes how to start the IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication installation program.

If you are installing IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication using the electronic images, there are two installation images:

**disk1** Contains all the Tivoli Storage Productivity Center components. Also contains the files to perform remote Data agent installations.

The **disk1** image is in two parts. Both parts must be downloaded to the same directory.

For Storage Resource agents, the image is located in the following location: <DVD>/data/sra/<operating system name>

The operating systems supported are listed in the following table.

Operating system	Operating system name
AIX	aix_power
Linux x86	linux_ix86
Linux Power	linux_power
Linux s390	linux_s390
Windows	windows

Table 22. Operating system for Storage Resource agents

**disk2** Contains the files to perform local agent installations. This image also contains the installation script for the Virtual I/O server. Download the file for the platform you want the agent to reside on.

The **disk2** location and operating system file name is the same as the **disk1** image.

## Note:

- When you install Tivoli Storage Productivity Center on AIX or Linux, you must source the db2profile before running the installation program. You must also source the db2profile when you install the database and license.
- If you are using Tivoli Storage Productivity Center electronic installation images that are downloaded to a Windows directory, ensure that the directory does not have spaces or unusual special characters in the name. This will cause the Tivoli Storage Productivity Center installation to fail.

For example, if you have a directory name:

C:\tpc 41 standard edition\disk1

The Tivoli Storage Productivity Center installation will fail.

Change the directory name to one that does not have spaces, for example: C:\tpc41se\disk1

This will ensure a successful Tivoli Storage Productivity Center installation.

- If you are installing Tivoli Storage Productivity Center using DVD and CD, note the contents of the media:
  - DVD Contains all the components for Tivoli Storage Productivity Center.
  - CD Contains the **disk2** image for local agent installations.

To start the Tivoli Storage Productivity Center installation program, complete the following steps:

 For Windows DVD (disk1): Open Windows Explorer and go to the Tivoli Storage Productivity Center DVD drive or directory. Go to: cd <DVD\_drive>\disk1

Double-click on setup.exe.

- 2. For Windows electronic image: Download the electronic image into a directory, unzip the file, and run **setup.exe** from the source installation directory.
- **3**. For Windows CD (**disk2**): If Windows Autorun is enabled, the installation program should start automatically. If it does not, open Windows Explorer and go to the Tivoli Storage Productivity Center CD-ROM drive. Double-click on **setup.exe**.
- 4. For Linux DVD (disk1):
  - a. Create a mount point called /cdrom:
     mkdir /cdrom
  - Insert the DVD into the DVD drive. Mount the DVD file system at the desired mount point. For example, to mount a DVD into a DVD drive known as /dev/cd0 at mount point /cdrom, enter the following command: mount -o ro /dev/cdrom /cdrom
  - **c.** Change to the directory where the DVD is mounted by entering the following command:

cd /cdrom

- d. Set up your shell environment to point to the instance where the database repository will be installed. To do this, source the **db2profile** script for the desired instance. For example, if the DB2 instance is **db2inst1**, perform the following steps:
  - 1) Source the file by typing:
    - . /home/db2inst1/sqllib/db2profile

Note: Please note that there is a space between . and /home.

2) Start the installation program from the disk1 directory (for example, <TPC\_source\_install\_dir>/disk1). Run ./setup.sh.

**Note:** Sometimes **setup.sh** exits prematurely because the media (DVD) is not ready yet. In this case, invoke **./setup.sh** again until the installation wizard is displayed.

- 5. For AIX DVD (disk1):
  - a. Insert the DVD into the DVD drive. Mount the DVD file system at the desired mount point.

On AIX, you can use the **crfs** command to add an entry to /etc/filesystems for the cdrom mount point. Run the following commands:

/usr/sbin/crfs -v cdrfs -p ro -d'cd0' -m'/cdrom' -A'no' mount /cdrom

The **crfs** command only has to be run once for a given mount point, and after that you can use **mount** and **umount** for each CD or DVD you put in the drive, for example, **mount /cdrom** and **umount /cdrom**.

b. Change to the directory where the DVD is mounted by entering the following command:

cd /cdrom

- **c**. Set up your shell environment to point to the instance where the database repository will be installed. To do this, source the **db2profile** script for the desired instance. For example, if the DB2 instance is **db2inst1**, perform the following steps:
  - 1) Source the file by typing:
    - . /home/db2inst1/sqllib/db2profile

Note: Please note that there is a space between . and /home.

Start the installation program from the disk1 directory (for example, <TPC\_source\_install\_dir>/disk1). Run ./setup.sh.

**Note:** Sometimes **setup.sh** exits prematurely because the media (DVD) is not ready yet. In this case, invoke **./setup.sh** again until the installation wizard is displayed.

- 6. For Linux or AIX electronic image:
  - a. Create a directory:

mkdir /tpcinst

- Change to the directory: cd tpcinst
- c. FTP the Tivoli Storage Productivity Center installation tar file into a directory:

ftp <filename>.tar

d. Run the following command:

tar -xvf <filename>.tar

e. Set up your shell environment to point to the instance where the database repository will be installed. To do this, source the **db2profile** script for the desired instance.

For example, if the DB2 instance is **db2inst1**, perform the following steps:

- 1) Source the file by typing:
  - . /home/db2inst1/sqllib/db2profile

Note: Please note that there is a space between . and /home.

- 2) Start the installation program. Run ./setup.sh.
- f. For Linux and AIX CD (disk2):
  - Create a mount point called /cdrom: mkdir /cdrom
  - 2) Insert the CD into the CD-ROM drive. Mount the CD-ROM file system at the desired mount point. For example, to mount a CD, enter the following command:

mount -o ro /dev/cdrom /cdrom

3) Change to the directory where the CD-ROM is mounted by entering the following command:

cd /cdrom

- 4) Set up your shell environment to point to the instance where the database repository will be installed. To do this, source the db2profile script for the desired instance.
- 5) For example, if the DB2 instance is **db2inst1**, perform the following steps:
  - a) Source the file by typing:
    - . /home/db2inst1/sqllib/db2profile

Note: Please note that there is a space between . and /home.

b) Start the installation program. Run ./setup.sh.

## Using typical installation

This section describes how to install all the Tivoli Storage Productivity Center components on one computer using typical installation.

The approximate time to install Tivoli Storage Productivity Center and IBM Tivoli Integrated Portal is about 60 minutes. The approximate time to install IBM Tivoli Storage Productivity Center for Replication is about 20 minutes. The time to install IBM Tivoli Integrated Portal on the AIX or Linux operating system is about 15 minutes less than on Windows.

You can install Tivoli Storage Productivity Center (Tivoli Storage Productivity Center server) with or without Agent Manager registration.

#### With Agent Manager registration

If you intend to install and use the Data agent or Fabric agent (or both), you must first install an Agent Manager and register your Tivoli Storage Productivity Center server with the Agent Manager before you install your Data agent or Fabric agent (or both). A check box is provided at installation for registering the Tivoli Storage Productivity Center server with Agent Manager.

## Without Agent Manager registration

If you do not intend to install or use the Data agent or Fabric agent (or both), you do not need to install an Agent Manager and there is no need to check the check box to register the Tivoli Storage Productivity Center server with Agent Manager at the time of installation.

**Note:** You need to install the Data agent and Agent Manager if you want to run Tivoli Storage Productivity Center batch reports.

A typical installation can be done in the following ways:

- Selecting Agent Manager registration and agents. See "Installing with Agent Manager registration" on page 184.
- Selecting Agent Manager registration without installing local agents. In this scenario, you would select Agent Manager registration and not select the agents.
- No selection of Agent Manager registration or local agents. See "Installing without Agent Manager registration" on page 172.

These are things to note when using typical installation:

- If you install the Tivoli Storage Productivity Center servers using typical installation, the user ID and password you use for installation will be used for:
  - Database administrator user ID and password (for Data Server and the Device server to connect to the database).
  - Database user ID and password to create the database schema.
  - Host authentication password (for the Fabric agents to communicate with the Device server).
  - Common agent service logon user ID and password (for Windows only, if the user ID does not exist).
  - WebSphere administration user ID and password (for the Device server to communicate with embedded WebSphere if the user ID does not exist) only when you select "OS" as the authentication mechanism; if you select "LDAP" as the authentication mechanism, then the LDAP TPC Administrator username and password values you enter during installation are used for the WebSphere administration user ID and password.
- If you subsequently install the Data agent or Fabric agent on a different machine using typical installation, you must use the same installation logon user ID and password you used when installing the Tivoli Storage Productivity Center servers. If the server installation password is different or has changed, you should use custom installation to install the agents so that you can specify the passwords for the agents to match the password for the server.

## Installing without Agent Manager registration

This section describes how to install IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication on one computer using typical installation and without Agent Manager registration.

To install Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication using typical installation without Agent Manager registration, follow these steps:

- 1. Start the installation program. For information about starting the installation program, see "Starting the installation program" on page 168.
- 2. The Select a language panel is displayed. Select a language from the list box and click **OK**. This is the language that is used for installing this product.
- **3**. The Software License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select **I accept the terms of the license agreement**. Click **Next**.

**Note:** 8 GB of RAM is required. If you have 4-8 GB of RAM, you can still install Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication. However, you will get a warning message. You should run only Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication because of system load. For information about how to disable Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication after installation, see "Disabling Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication after installation, see "Disabling Tivoli Storage Productivity Center for Replication" on page 341.

4. The select the type of installation panel is displayed.

🕲 IBM Tivoli Storage Pro	ductivity Center - Installe	r)			_ 🗆 🗙
	Select the type of installat	ion you want to run			
IBM.	Typical installation This will install the Data and CLI. A new databas database during installa	server and Device e will be created, a ation. The database	server, Data agent a nd the schema will b and schema will be	nd Fabric agent, GUI le created on the reused for upgrade.	
	✓ Servers	🗹 Clients			
	Agents	🗖 Registe	r with the agent man	ager	
	C Custom installation				
	This will install the Data and CLI, and database computers. You can ch computer. You will have computer. O Installation licenses	server and Device on this computer. F oose any server, a <u>c</u> a choice to create	server, Data agent a temote agents are in jent, or client to be in the database and sc	nd Fabric agent, GUI Istalled on other stalled on this hema on this	
	C:\Program Files\IBM\T	PC	TPC Insta	llation Location	
	< <u>B</u> ac	k 🔤	<u>N</u> ext >	<u>C</u> ancel	

Figure 16. Select the type of installation you want to run panel

Enter the information below and click Next.

## Typical installation

Allows you to install all of the components in a group on the local computer by selecting **Servers**, **Agents**, and **Clients**. This selection requires a minimum amount of input from the user who installs Tivoli Storage Productivity Center.

Typical installation also installs IBM Tivoli Integrated Portal and IBM Tivoli Storage Productivity Center for Replication. If you want to use an existing Tivoli Integrated Portal, use custom installation.

Because this is a typical installation, select **Typical installation**. Under Typical installation, you have these options:

## Servers

This installs the database schema, the Data Server, and the Device server.

## Agents

This installs the Data agent and Fabric agent.

**Note:** This option is not selectable on systems that are configured for IPv6 only.

## Clients

This installs the Tivoli Storage Productivity Center GUI and the command-line interface (CLI).

## Register with the Agent Manager

This registers the Tivoli Storage Productivity Center server with the Agent Manager. Because you are installing Tivoli Storage Productivity Center without Agent Manager registration, do not select this option.

#### **Custom installation**

Allows you to install one or more components separately.

#### Installation licenses

This will install the Tivoli Storage Productivity Center license. The Tivoli Storage Productivity Center license is on the DVD. You only need to run this option when you upgrade a license to a Tivoli Storage Productivity Center package that has already been installed on your system. For example, if you have installed IBM Tivoli Storage Productivity Center for Data package, the license will be automatically installed when you install the product. If you decide to later install IBM Tivoli Storage Productivity Center for Fabric, run the installation program and select **Installation licenses**. This option will allow you to upgrade the license from the DVD that has the Tivoli Storage Productivity Center for Fabric license. You do not have to install the Tivoli Storage Productivity Center for Fabric product.

For information about upgrading the license, see "Adding an installation license" on page 240.

For this scenario, select **Typical installation**, **Servers**, and **Clients**. Clear the check box for Agents and Register with Agent Manager. All of the components will be installed on the local computer. This also installs the database schema on the local computer. When you install the database schema, this will create the database (if the database does not exist), the schema, and the table spaces. At the bottom of the panel, you can enter the directory where you want to install the components. The default location is:

C:\Program Files\IBM\TPC (for Windows) /<usr or opt>/IBM/TPC (for UNIX and Linux)

Click Next.

5. The User ID and password panel is displayed. Enter the user ID and password that has administrator and database administrator authority.

🕲 IBM Tivoli Storage Proc	luctivity Center - Ins	staller	_ 🗆 X
IBM.	User ID and pass This user ID an installation. This administrator au with the Device which allows yo with the server.	word, and server and agent information d password will be used for all user IDs and passwords required du s user ID should have operating system administrator and database uthority. Note: the password will be used for fabric agent authenticat server. If this is not suitable for your needs, please use the custom u to specify different passwords for local users and agent authentic	uring e ion install ation
	User ID Password	þb2admin	
	Server and agent i Enter the serve will use to com Domains, ente	information In name and port numbers that the Data agent, Fabric agent, GUI, ar Imunicate with the server. If the environment has multiple TCP/IP r the fully qualified hostname or IP address for the server name.	ıd TIP
And :	Server name Server port Agent port	mdm-b26-w2k3.beaverton.ibm.com 9549 9510	
	<	Back Next > Cancel	

Figure 17. User ID and password panel

Field descriptions:

## User ID

Enter the user ID and password that has administrator and database administrator authority. This user ID and password will be used for the following items:

- Database administrator user ID and password (for the Data Server or the Device server to connect to the database).
- Database user ID and password to create the database schema.
- Host authentication password (for the Fabric agents to communicate with the Device server).
- Common agent service logon user ID and password (for Windows only, if this user ID does not exist).
- WebSphere administration user ID and password (for the Device server to communicate with embedded WebSphere if the user ID does not exist) only when you select "OS" as the authentication mechanism; if you select "LDAP" as the authentication mechanism, then the LDAP TPC Administrator username and password values you enter during installation are used for the WebSphere administration user ID and password.

For information about these user IDs and passwords, see "Work sheet for user IDs and passwords" on page 23.

## Password

Password for the user ID.

## Server name

The Tivoli Storage Productivity Center server name. If your environment includes multiple Tivoli Storage Productivity Center

servers and IP domains, you should specify a fully-qualified host name. On Windows, this might appear as a short host name.

#### Server port

Port number for the Tivoli Storage Productivity Center server.

The default server port is 9549. This will be assigned to the Data server and port 9550 will be assigned to the Device server. If you specify a different server port, for example, 9569, then the the Device server will be assigned the next higher port number (9570)

#### Agent port

Port number for the agent. The default port is 9510. If the default port is not used for the agent port, then the Tivoli Storage Productivity Center agents need to be installed using custom installation.

If you install the servers and agents at different times, make sure that the host authentication password you used to install the Device server is the same password you use to install the Fabric agent.

Enter the information in the fields or accept the defaults. Click Next.

#### Note:

• If you are installing a client and server on a system that has IPv4 and IPv6 stacks enabled and both address configured (dual stack), you must enter the IPv4 address (or a host name that resolves to an IPv4 address) for the system in the **Server name** field. If an IPv6 address (or hostname that resolves to an IPv6 address) appears in the **Server name** field when you click **Next**, a pop-up message appears and provides you with valid IPv4 addresses and hostnames that you must enter instead. This ensures that if you later install Data and Fabric agents, they will be able to communicate with the server using that IPv4 address.

6. The Tivoli Integrated Portal panel is displayed.

🖞 IBM Tivoli Storage Produ	ictivity Center - Installer	_ 🗆 🗙
IBM.	Tivioli Integrated Portal (TIP) TIP provides TPC with the ability for Single Sign-On authentication, launch other applications in context, and reports to be viewed from Tivoli Common Reporting. Select an existing TIP install to be used with TPC or specify the install directory where TPC is to install TIP.	
	C:\Program Files\IBM\Tivoli\tip     Browse       Port     16310       C Reuse an existing TIP install	
	Existing TIP Installs:       TIP Administrator ID     db2admin       Password     ********	
	< Back Next > Cancel	

Figure 18. Tivoli Integrated Portal panel

Options and fields:

## Specify the location to install TIP

Accept the default or enter a location to install Tivoli Integrated Portal.

- **Port** Enter the port number for Tivoli Integrated Portal or accept the default (16310). Tivoli Integrated Portal uses 10 port numbers. For example, if the default port 16310 is accepted, Tivoli Integrated Portal uses the following ports: 16310, 16311, 16312, 16313, 16315, 16316, 16318, 16320, 16322, and 16323. If you enter a port number other than the default number, ensure that you have the following ports available for Tivoli Integrated Portal:
  - base port
  - base port +1
  - base port +2
  - base port +3
  - base port +5
  - base port +6
  - base port +8
  - *base port* +10
  - base port +12
  - base port +13

where *base port* is the port value entered in the **Port** field.

## Reuse an existing install TIP install

If you select this option, you will see a list of existing Tivoli Integrated Portal installations. Select a Tivoli Integrated Portal installation.

## **TIP Administrator ID**

Enter the Tivoli Integrated Portal administrator ID.

## Password

Enter the password for the Tivoli Integrated Portal administrator ID.

Click Next.

7. The authentication selection panel is displayed.

🕲 IBM Tivoli Storage Prod	uctivity Center - Installer	_ 🗆 🗙
	TPC may be configured for one of two methods to authenticate the user. The default option is to authenticate the user against the local operating system. Another option is to authenticate the user against an existing LDAP or Active Directory directory service. Selecting a directory service for authentication is required to enable Single Sign-On capability between TPC and other Tivoli products. Please select the desired authentication mechanism to be used for TPC.	
	< <u>B</u> ack <u>Cancel</u>	

Figure 19. Authentication selection panel

These are the options:

#### **OS** Authentication

This uses the operating system for user authentication. If you select this option, go to step 11.

## LDAP/Active Directory

If you select LDAP or Microsoft Active Directory for authentication, you must have an LDAP or Active Directory already installed.

If you select this option, go to step 8. Click Next.

8. The Lightweight Directory Access Protocol (LDAP server information) panel is displayed. Enter this information and click **Next**.

🕲 IBM Tivoli Storage Productivity Center - Installer 🛛 📃 🖬 🗙		
IBM.	Lightweight Directory Access Protocol (LDAP) Specify the LDAP server information required for TPC to use LDAP authentication. The Bind Distinguished Name and Bind Password options are optional if the LDAP server supports anonymous binds and user or group creation from TIP is not required.	
	LDAP Server Hostname LDAP Port Number 389 The following are optional if anonymous binds are allowed:	
	Bind Distinguished Name Bind Password	
	< <u>B</u> ack <u>N</u> ext > <u>C</u> ancel	

Figure 20. LDAP server information panel

Enter this information and click Next.

## LDAP Server Hostname

The fully-qualified host and domain name of the machine where your LDAP-based directory is running.

## LDAP Port Number

The port number on your LDAP server where the LDAP process is listening for communications.

## Bind Distinguished Name

The distinguished name used to bind to the LDAP-based directory when performing a user or group search. This name is optional because some LDAP-based directories allow anonymous binds and others require you to bind with a specific name and password.

**Note:** Depending on how the LDAP server is set up, the Bind DN and password might or might not be optional. If the LDAP server allows for anonymous binds, then the Bind DN and password are optional.

If you want the ability to create or modify LDAP users and groups from the Tivoli Integrated Portal admin panel, then the Bind DN and password are required.

## **Bind Password**

The password associated with the Bind Distinguished Name.

**9**. The Lightweight Directory Access Protocol (LDAP user and group information) panel is displayed.

🕲 IBM Tivoli Storage Produ	uctivity Center - Installer	_ 🗆 🗙
IBM.	Lightweight Directory Access Protocol (LDAP) Specify the LDAP user and group information required for TPC to use LDAP authentication.	
	Relative Distinguished Name for usernames Attribute to use for usernames uid Relative Distinguished Name for groups Attribute to use for groups cn	
	< <u>B</u> ack <u>N</u> ext > <u>C</u> ancel	

Figure 21. LDAP user and group information panel

Enter this information and click Next.

## **Relative Distinguished Name for usernames**

Tells Tivoli Storage Productivity Center where to start a search in the directory when performing user authentication.

## Attribute to use for usernames

Tells Tivoli Storage Productivity Center which attribute in a user's directory entry contains the user's name for authentication.

## **Relative Distinguished Name for groups**

Tells Tivoli Storage Productivity Center where in the directory to start a search when performing a group search for authorization.

## Attribute to use for groups

Tells Tivoli Storage Productivity Center which attribute in a group's directory entry contains the group's name for authorization.

**10.** The Lightweight Directory Access Protocol (LDAP TPC Administrator user and group information) panel is displayed.

🕲 IBM Tivoli Storage Proc	luctivity Center - Installer	_ 🗆 🗙
IBM.	Lightweight Directory Access Protocol (LDAP) Specify the LDAP TPC Administrator user and group that will have the TPC Administrator privileges.	
	LDAP TPC Administrator username	
	< Back Next > Cancel	

Figure 22. LDAP TPC Administrator user and group information panel

Enter this information and click Next.

## LDAP TPC Administrator username

The user ID that Tivoli Storage Productivity Center will configure as the Tivoli Storage Productivity Center superuser during installation. This user name should already exist in the directory before you start the Tivoli Storage Productivity Center installation and should be a member of your designated LDAP Tivoli Storage Productivity Center Administrator group in the directory.

**Note:** If you install Tivoli Storage Productivity Center on a Windows system and have Tivoli Storage Productivity Center authenticate users against an LDAP-based repository, then the LDAP Tivoli Storage Productivity Center Administrator username must **not** contain a space or blank character in it. See the WebSphere Application Server APAR PK77578.

Ensure that you use the correct case when entering the values for the LDAP TPC Administrator username and LDAP TPC Administrator group. If you use the incorrect case when entering these values, then you will not be able to login to Tivoli Storage Productivity Center for Replication with the user name you expected to use.

## LDAP TPC Administrator password

Password for the administrator.

## LDAP TPC Administrator group

The group that Tivoli Storage Productivity Center will map to the Tivoli Storage Productivity Center superuser role during installation. This group should already exist in the directory before you start the Tivoli Storage Productivity Center installation and should have the designated LDAP IBM Tivoli Storage Productivity Center Administrator as a member.

## Note:

Ensure that you use the correct case when entering the values for the LDAP TPC Administrator username and LDAP TPC Administrator group. If you use the incorrect case when entering these values, then you will not be able to login to Tivoli Storage Productivity Center for Replication with the user name you expected to use.

- 11. The Summary Information panel is displayed. Review the information. Click **Install**.
- **12.** You will see the installing panel. When Tivoli Integrated Portal has finished installing, Tivoli Storage Productivity Center will start the Tivoli Storage Productivity Center for Replication installation.
- **13.** Tivoli Storage Productivity Center starts the Tivoli Storage Productivity Center for Replication installation program.
  - a. The Welcome panel is displayed. Click Next.
  - b. The System prerequisites check panel is displayed. The installation wizard checks whether the prerequisites are installed, then confirms whether your operating system is supported and is at the appropriate fix pack or update level. Click **Next**.

🐻 IBM Tivoli Storage	e Productivity Center for Replication - InstallShield Wizard	
	System prerequisites check	
	The Installation wizard checks your system to determine whether a supported operating system is running and whether the operating system is at the appropriate fix pack or update level.	
- ji	Your system has all of the necessary prerequisites for IBM Tivoli Storage Productivity Center for Replication. You may continue.	
InstallShield		
	< Back Next > Cancel	

Figure 23. System prerequisites check panel

- c. The License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select I accept the terms of the license agreement. Click Next.
- d. The Directory Name panel is displayed. Accept the default installation directory by clicking **Next**, or specify a different installation directory and click **Next**.

🐻 IBM Tivoli Storage	Productivity Center for Replication - InstallShield Wizard	_ 🗆 X
	Click Next to install "IBM Tivoli Storage Productivity Center for Replication" to this directory, or click Browse to install to a different directory.	
	Directory Name: C:\Program Files\IBM\replication Browse	
InstallShield —		
	Seck Next > Cancel	

Figure 24. Directory Name panel

e. The Tivoli Storage Productivity Center for Replication Administrator ID and Password panel is displayed. Enter the administrator user ID and password. This ID is usually the operating system administrator user ID. If you use a different ID, create it beforehand and ensure that it has administrator rights.

**Note:** There is a limitation on the number of characters for the user name and password on AIX. At the time this document was written, AIX did not properly validate passwords that are longer than eight characters.

🐻 IBM Tivoli Storage	Productivity Center for Replication	- InstallShield Wizard		_ 🗆 🗙
	Enter the user name and passwor You must enter an existing user na	d for IBM Tivoli Storage Proc ame and be sure the passw	ductivity Center for Replication ord is correct.	on Administrator user.
Ĩ	TPC-R Administrator User Name Administrator Password			
InstallShield —		Put	Ned	
		< Back	Next >	Cancel

Figure 25. TPC-R Administrator ID and Password panel

f. The Default ports panel is displayed. Accept the defaults. Click Next.

	IBM Tivoli Storage Productivity Cent environment. This will be automatic numbers needed by WebSphere ap use.	er for Replication uses We ally installed by this install oplication server. You can c	bSphere application server ation wizard. You are require hange any default port num	as its runtime ed to specify the port bers that are already in
Ĩ	Default Host Port 3080 Default Host Secure Port 3443			
InstallShield				
		< Back	Next >	Cancel

Figure 26. Default ports panel

- g. The settings panel is displayed. Review the settings and change them if needed by clicking **Back**. Otherwise, click **Install** to begin the installation.
- h. You will see the status panel. Wait for installation to complete.
- i. You will see the summary information panel. Review the information and click **Finish**.
- j. Tivoli Storage Productivity Center for Replication is installed with no license. You must install the Two Site or Three Site Business Continuity (BC) license. For information about installing the license, see "Installing the Two Site or Three Site Business Continuity license" on page 197.
- 14. The Successfully installed panel is displayed. Click Finish.
- **15.** After you have installed Tivoli Storage Productivity Center, you can use the Configuration Utility to learn how to configure your system. Follow these steps to go to the Configuration Utility:
  - a. Open the Tivoli Storage Productivity Center GUI.
  - b. Go to Tivoli Storage Productivity Center > Configuration Utility.
- 16. For Tivoli Storage Productivity Center for Replication configuration, see the Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/ v4r1/index.jsp. Click Tivoli Storage Productivity Center for Replication > Configuring.

## Installing with Agent Manager registration

This section describes how to install IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication on one computer using typical mode with Agent Manager registration. In this scenario, Agent Manager must be installed before you register the servers with the Agent Manager.

To install Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication using typical mode with Agent Manager registration, follow these steps:

1. If you do not have Agent Manager installed, install Agent Manager. If you are installing Agent Manager on a different machine from Tivoli Storage Productivity Center, you must install DB2 9.1 or 9.5 on that machine. For information about installing the Agent Manager, see "Installing the Agent Manager" on page 131.

- 2. Start the Tivoli Storage Productivity Center installation program. For information about starting the installation program, see "Starting the installation program" on page 168.
- **3**. The Select a language panel is displayed. Select a language from the list box and click **OK**. This is the language that is used for installing this product.
- 4. The Software License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select I accept the terms of the license agreement. Click Next.

**Note:** 8 GB of RAM is required. If you have 4-8 GB of RAM, you can still install Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication. However, you will get a warning message. You should run only Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication because of system load. For information about how to disable Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication after installation, see "Disabling Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication after installation, see "Disabling Tivoli Storage Productivity Center for Replication" on page 341.

5. The select the type of installation panel is displayed.

**Note:** If you are using an IPv6–only machine, make sure the boxes are unchecked for **Agents** and **Register with the Agent Manager**. Agent Manager does not run on IPv6–only machines.

🕲 IBM Tivoli Storage Pro	ductivity Center - Install	er		_ 🗆 🗙
	Select the type of installation you want to run			
IBM.	Typical installation This will install the Data server and Device server, Data agent and Fabric agent, GUI and CLI. A new database will be created, and the schema will be created on the database during installation. The database and schema will be reused for upgrade.			
	✓ Servers	🔽 Clients		
	☑ Agents	🗹 Register with	the agent manager	
	C Custom installation			
	This will install the Dat and CLI, and database computers. You can ch computer. You will have computer.	a server and Device serve on this computer. Remot noose any server, agent, c e a choice to create the da	rr, Data agent and Fabric agent, GUI te agents are installed on other or client to be installed on this atabase and scherna on this	
	C:\Program Files\IBM\`	TPC	TPC Installation Location	
	< <u>B</u> a	ck <u>N</u> i	ext > <u>C</u> ancel	

Figure 27. Select the type of installation you want to run panel

You have the following options:

## Typical installation

Allows you to install all of the components in a group on the local

computer by selecting **Servers**, **Agents**, and **Clients**. This selection requires a minimum amount of input from the user who installs Tivoli Storage Productivity Center.

Typical installation also installs IBM Tivoli Integrated Portal and Tivoli Storage Productivity Center for Replication. If you want to use an existing Tivoli Integrated Portal, use custom installation.

Because this is a typical installation, select **Typical installation**. Under Typical installation, you have these options:

#### Servers

This will install the database schema, Data Server, and the Device server.

## Agents

This will install the Data agent and Fabric agent.

#### Clients

This will install the Tivoli Storage Productivity Center GUI and the command-line interface (CLI).

#### **Register with the Agent Manager**

This registers the Tivoli Storage Productivity Center server with the Agent Manager.

**Note:** The **Register with the Agent Manager** check box does not install the Agent Manager. You must have previously installed the Agent Manager before you install Tivoli Storage Productivity Center.

#### Custom installation

Allows you to install one or more components separately.

#### Installation licenses

This will install the Tivoli Storage Productivity Center license. The license is on the DVD. You only need to run this option when you upgrade a license to a Tivoli Storage Productivity Center package that has already been installed on your system. For example, if you have installed IBM Tivoli Storage Productivity Center for Data package, the license will be automatically installed when you install the product. If you decide to later install IBM Tivoli Storage Productivity Center for Fabric, run the installation program and select **Installation licenses**. This option will allow you to upgrade the license from the DVD that has the Tivoli Storage Productivity Center for Fabric license. You do not have to install the Tivoli Storage Productivity Center for Fabric product.

For information about upgrading the license, see "Adding an installation license" on page 240.

For this scenario, select **Servers**, **Agents**, **Clients**, and **Register with the Agent Manager**. All of the components will be installed on the local computer. This also installs the database schema on the local computer. When you install the database schema, this will create the database (if the database does not exist), the schema, and the table spaces. At the bottom of the panel, you can enter the directory where you want to install the components. The default location is:

C:\Program Files\IBM\TPC (for Windows) /<usr or opt>/IBM/TPC (for UNIX and Linux) Click Next.

6. The User ID and password panel is displayed. Enter the user ID and password that has administrator and database administrator authority.

🕲 IBM Tivoli Storage Proc	luctivity Center - Ins	staller	
	User ID and passy This user ID and installation. This administrator au with the Device s which allows you with the server.	word, and server and agent information d password will be used for all user IDs and passwords requin suser ID should have operating system administrator and dat othority. Note: the password will be used for fabric agent authe server. If this is not suitable for your needs, please use the cus u to specify different passwords for local users and agent auth	red during abase ntication stom install entication
	User ID Password Server and agent i	db2admin	
	Enter the serve will use to com Domains, enter Server name	r name and port numbers that the Data agent, Fabric agent, G municate with the server. If the environment has multiple TCP r the fully qualified hostname or IP address for the server nam mdm-b26-w2k3.beaverton.ibm.com	UI, and TIP /IP e.
	Server port Agent port	9549 9510 Back <u>N</u> ext > <u>C</u> ancel	

Figure 28. User ID and password panel

Field descriptions:

## User ID

Enter the user ID and password that has administrator and database administrator authority. This user ID and password will be used for the following items:

- Database administrator user ID and password (for Data Server or the Device server to connect to the database).
- Database user ID and password to create the database schema.
- Host authentication password (for the Fabric agents to communicate with the Device server).
- Common agent service logon user ID and password (for Windows only, if this user ID does not exist).
- WebSphere administration user ID and password (for the Device server to communicate with embedded WebSphere if the user ID does not exist) only when you select "OS" as the authentication mechanism; if you select "LDAP" as the authentication mechanism, then the LDAP TPC Administrator username and password values you enter during installation are used for the WebSphere administration user ID and password.

For information about these user IDs and passwords, see "Work sheet for user IDs and passwords" on page 23.

#### Password

Password for the user ID.

## Server name

The Tivoli Storage Productivity Center server name. If your environment includes multiple Tivoli Storage Productivity Center servers and IP domains, you should specify a fully-qualified host name. On Windows, this might appear as a short host name.

#### Server port

Port number for the Tivoli Storage Productivity Center server.

The default server port is 9549. This will be assigned to the Data server and port 9550 will be assigned to the Device server. If you specify a different server port, for example, 9569, then the Device server will be assigned the next higher port number (9570)

## Agent port

Port number for the agent. The default port is 9510. If the default port is not used for the agent port, then the Tivoli Storage Productivity Center agents need to be installed using custom installation.

If you install the servers and agents at different times, make sure that the host authentication password you used to install the Device server is the same password you use to install the Fabric agent.

Enter the information in the fields or accept the defaults. Click Next.

#### Note:

- If you are installing a client and server on a system that has IPv4 and IPv6 stacks enabled and both address configured (dual stack), you must enter the IPv4 address (or a host name that resolves to an IPv4 address) for the system in the **Server name** field. If an IPv6 address (or hostname that resolves to an IPv6 address) appears in the **Server name** field when you click **Next**, a pop-up message appears and provides you with valid IPv4 addresses and hostnames that you must enter instead. This ensures that if you later install Data and Fabric agents, they will be able to communicate with the server using that IPv4 address.
- 7. The Agent Manager information panel is displayed.
| 🕲 IBM Tivoli Storage Pro | ductivity Center - Installer                                              |                                                                                 |  |
|--------------------------|---------------------------------------------------------------------------|---------------------------------------------------------------------------------|--|
|                          | Agent manager information                                                 |                                                                                 |  |
| IBM.                     | Enter the information that the proc<br>server, Data agent, or Fabric ager | duct will use to register its Data server, Device<br>nt with the agent manager. |  |
|                          | Hostname or IP address                                                    | mdm-b26-w2k3.beaverton.ibm.com                                                  |  |
| A                        | Port (Secured)                                                            | 9511                                                                            |  |
|                          | Port (Public)                                                             | 9513                                                                            |  |
|                          | Enter the Data server and Device the agent manager.                       | server registration information as specified on                                 |  |
|                          | User ID                                                                   | manager                                                                         |  |
|                          | Password                                                                  |                                                                                 |  |
| 1 Mail                   | Enter the common agent registrat manager.                                 | tion password as specified on the agent                                         |  |
| 11.10+ =                 | Password                                                                  |                                                                                 |  |
| 11 -                     |                                                                           |                                                                                 |  |
|                          | < <u>B</u> ack                                                            | <u>N</u> ext ≻ <u>C</u> ancel                                                   |  |

Figure 29. Agent Manager information panel

Complete the following information:

# Hostname or IP address

Use fully-qualified host names (for example, tpcam.toronto.ibm.com) for this field. Do not use the short form of the host name (for example, tpcam). The short host name can prevent successful agent deployments. You can also specify the IPv4 IP address of the Agent Manager server, but this is not suggested for a production environment because it limits the flexibility if a server IP address needs to be changed. If a fully-qualified host name is used, it can be reassigned to the new IP address in the DNS and the Agent Manager environment should continue to operate as it did before the address change.

**Note:** Agent Manager does not support IPv6 addressing. If an IPv6 address is entered, you will receive an error message.

# Port (Secured)

Port number of the Agent Manager server. The default is 9511.

#### **Port (Public)**

The public communication port. The default is 9513.

# Enter the Data server and the Device server registration information as specified on the Agent Manager

#### User ID

This is the resource manager registration user ID. This user ID is used to register the Data Server or the Device server with the Agent Manager. The default is **manager**.

#### Password

This is the resource manager registration password. This

password is used to register the Data Server or the Device server with the Agent Manager. The default is **password**.

# Enter the Common agent registration password as specified on the Agent Manager

#### Password

This is the Common agent registration password used by the Common agent to register with the Agent Manager. This was specified when you installed the Agent Manager.

Click Next.

8. The Tivoli Integrated Portal panel is displayed.

() IBM Tivoli Storage Pro	ductivity Center - Installer	_ 🗆 🗙
	Tivioli Integrated Portal (TIP) TIP provides TPC with the ability for Single Sign-On authentication, launch other applications in context, and reports to be viewed from Tivoli Common Reporting. Select an existing TIP install to be used with TPC or specify the install directory where TPC is to install TIP. Specify the location to install TIP C:\Program Files\IBM\Tivoli\ttip	9
	Port 16310 C Reuse an existing TIP install Existing TIP Installs:	
	TIP Administrator ID db2admin Password *******	
	< <u>B</u> ack <u>N</u> ext > <u>C</u> ancel	

Figure 30. Tivoli Integrated Portal panel

Options and fields:

#### Specify the location to install TIP

Accept the default or enter a location to install Tivoli Integrated Portal.

- **Port** Enter the port number for Tivoli Integrated Portal or accept the default (16310). Tivoli Integrated Portal uses 10 port numbers. For example, if the default port 16310 is accepted, Tivoli Integrated Portal uses the following ports: 16310, 16311, 16312, 16313, 16315, 16316, 16318, 16320, 16322, and 16323. If you enter a port number other than the default number, ensure that you have the following ports available for Tivoli Integrated Portal:
  - base port
  - base port +1
  - base port +2

- base port +3
- base port +5
- *base port* +6
- base port +8
- *base port* +10
- base port +12
- *base port* +13

where *base port* is the port value entered in the **Port** field.

# Reuse an existing install TIP install

If you select this option, you will see a list of existing Tivoli Integrated Portal installations. Select a Tivoli Integrated Portal installation.

# **TIP Administrator ID**

Enter the Tivoli Integrated Portal administrator ID.

# Password

Enter the password for the Tivoli Integrated Portal administrator ID.

Click Next.

9. The authentication selection panel is displayed.

🕲 IBM Tivoli Storage Prod	uctivity Center - Installer	_ 🗆 🗙
	TPC may be configured for one of two methods to authenticate the user. The default option is to authenticate the user against the local operating system. Another option is to authenticate the user against an existing LDAP or Active Directory directory service. Selecting a directory service for authentication is required to enable Single Sign-On capability between TPC and other Tivoli products. Please select the desired authentication mechanism to be used for TPC.	
	< Back Cancel	

Figure 31. Authentication selection panel

These are the options:

# **OS** Authentication

This uses the operating system for user authentication. If you select this option, go to step 13.

#### LDAP/Active Directory

If you select LDAP or Microsoft Active Directory for authentication, you must have an LDAP or Active Directory already installed.

If you select this option, go to step 10. Click Next.

**10**. The Lightweight Directory Access Protocol (LDAP server information) panel is displayed. Enter this information and click **Next**.

🕲 IBM Tivoli Storage Prod	uctivity Center - Installer	
IBM.	Lightweight Directory Access Protocol (LDAP) Specify the LDAP server information required for TPC to use LDAP authentication. Th Bind Distinguished Name and Bind Password options are optional if the LDAP server supports anonymous binds and user or group creation from TIP is not required.	e
	LDAP Server Hostname LDAP Port Number 389	
	The following are optional if anonymous binds are allowed: Bind Distinguished Name Bind Password	
	< Back Next > Cancel	

Figure 32. LDAP server information panel

Enter this information and click Next.

#### LDAP Server Hostname

The fully-qualified host and domain name of the machine where your LDAP-based directory is running.

#### LDAP Port Number

The port number on your LDAP server where the LDAP process is listening for communications.

#### **Bind Distinguished Name**

The distinguished name used to bind to the LDAP-based directory when performing a user or group search. This name is optional because some LDAP-based directories allow anonymous binds and others require you to bind with a specific name and password.

**Note:** Depending on how the LDAP server is set up, the Bind DN and password might or might not be optional. If the LDAP server allows for anonymous binds, then the Bind DN and password are optional.

If you want the ability to create or modify LDAP users and groups from the Tivoli Integrated Portal admin panel, then the Bind DN and password are required.

#### **Bind Password**

The password associated with the Bind Distinguished Name.

11. The Lightweight Directory Access Protocol (LDAP user and group information) panel is displayed.

🕲 IBM Tivoli Storage Prod	luctivity Center - Installer	_ 🗆 🗙
TEM a	Intrivity Center - Installer         Lightweight Directory Access Protocol (LDAP)         Specify the LDAP user and group information required for TPC to use LDAP authentication.         Relative Distinguished Name for usernames         Image: Comparison of the transmission of transmission of the transmission of the transmission of the transmission of transmission of the transmission of transmission	
	cn < <u>Back</u> <u>N</u> ext > <u>C</u> ancel	

Figure 33. LDAP user and group information panel

Enter this information and click Next.

# **Relative Distinguished Name for usernames**

Tells Tivoli Storage Productivity Center where to start a search in the directory when performing user authentication.

#### Attribute to use for usernames

Tells Tivoli Storage Productivity Center which attribute in a user's directory entry contains the user's name for authentication.

# **Relative Distinguished Name for groups**

Tells Tivoli Storage Productivity Center where in the directory to start a search when performing a group search for authorization.

#### Attribute to use for groups

Tells Tivoli Storage Productivity Center which attribute in a group's directory entry contains the group's name for authorization.

**12.** The Lightweight Directory Access Protocol (LDAP TPC Administrator user and group information) panel is displayed.

🕲 IBM Tivoli Storage Prode	uctivity Center - Installer	_ 🗆 🗙
IBM.	Lightweight Directory Access Protocol (LDAP) Specify the LDAP TPC Administrator user and group that will have the TPC Administrator privileges.	
	LDAP TPC Administrator username	
	< <u>B</u> ack <u>N</u> ext > <u>C</u> ancel	

Figure 34. LDAP TPC Administrator user and group information panel

Enter this information and click Next.

# LDAP TPC Administrator username

The user ID that Tivoli Storage Productivity Center will configure as the Tivoli Storage Productivity Center superuser during installation. This user name should already exist in the directory before you start the Tivoli Storage Productivity Center installation and should be a member of your designated LDAP Tivoli Storage Productivity Center Administrator group in the directory.

**Note:** If you install Tivoli Storage Productivity Center on a Windows system and have Tivoli Storage Productivity Center authenticate users against an LDAP-based repository, then the LDAP Tivoli Storage Productivity Center Administrator username must **not** contain a space or blank character in it. See the WebSphere Application Server APAR PK77578.

Ensure that you use the correct case when entering the values for the LDAP TPC Administrator username and LDAP TPC Administrator group. If you use the incorrect case when entering these values, then you will not be able to login to Tivoli Storage Productivity Center for Replication with the user name you expected to use.

# LDAP TPC Administrator password

Password for the administrator.

# LDAP TPC Administrator group

The group that Tivoli Storage Productivity Center will map to the Tivoli Storage Productivity Center superuser role during installation. This group should already exist in the directory before you start the Tivoli Storage Productivity Center installation and should have the designated LDAP Tivoli Storage Productivity Center Administrator as a member.

#### Note:

Ensure that you use the correct case when entering the values for the LDAP TPC Administrator username and LDAP TPC Administrator group. If you use the incorrect case when entering these values, then you will not be able to login to Tivoli Storage Productivity Center for Replication with the user name you expected to use.

- **13**. The Summary Information panel is displayed. Review the information. Click **Install**.
- 14. You will see the installing panel. When Tivoli Integrated Portal has finished installing, Tivoli Storage Productivity Center will start the Tivoli Storage Productivity Center for Replication installation.
- **15.** Tivoli Storage Productivity Center starts the Tivoli Storage Productivity Center for Replication installation program.
  - a. The Welcome panel is displayed. Click Next.
  - b. The System prerequisites check panel is displayed. The installation wizard checks whether the prerequisites are installed, then confirms whether your operating system is supported and is at the appropriate fix pack or update level. Click **Next**.



Figure 35. System prerequisites check panel

- c. The License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select I accept the terms of the license agreement. Click Next.
- d. The Directory Name panel is displayed. Accept the default installation directory by clicking **Next**, or specify a different installation directory and click **Next**.

🐻 IBM Tivoli Storage	Productivity Center for Replication - Ins	tallShield Wizard			_ 🗆 X
	Click Next to install "IBM Tivoli Storage P install to a different directory.	roductivity Center for F	Replication" to this directory, (	or click Browse to	
	Directory Name: C:\Program Files\IBM\replication			Browse	
InstallShield —	_	< Back	Next ≻	Cancel	

Figure 36. Directory Name panel

e. The Tivoli Storage Productivity Center for Replication Administrator ID and Password panel is displayed. Enter the administrator user ID and password. This ID is usually the operating system administrator user ID. If you use a different ID, create it beforehand and ensure that it has administrator rights.

**Note:** There is a limitation on the number of characters for the user name and password on AIX. At the time this document was written, AIX did not properly validate passwords that are longer than eight characters.

IBM Tivoli Storage	Productivity Center for Replication	- InstallShield Wizard		_ 🗆 ×
	Enter the user name and password You must enter an existing user na	I for IBM Tivoli Storage Proc me and be sure the passw	luctivity Center for Replication ord is correct.	on Administrator user.
	TPC-R Administrator User Name			
	Administrator			
	Password			
and the second s	*******			
InstallShield				
		< Back	Next >	Cancel

Figure 37. Tivoli Storage Productivity Center for Replication Administrator ID and Password panel

f. The Default ports panel is displayed. Accept the defaults. Click Next.

IBM Tivoli Storage	Productivity Center for Replication IBM Tivoli Storage Productivity Cent environment. This will be automatic numbers needed by WebSphere aj use. Default Host Port 3080 Default Host Secure Port 3443	- InstallShield Wizard er for Replication uses Wel ally installed by this install oplication server. You can c	bSphere application server ation wizard. You are requirs hange any default port num	as its runtime ad to specify the port bers that are already in
InstallShield ——		< Back	Next >	Cancel

Figure 38. Default ports panel

- g. The settings panel is displayed. Review the settings and change them if needed by clicking **Back**. Otherwise, click **Install** to begin the installation.
- h. You will see the status panel. Wait for installation to complete.
- i. You will see the summary information panel. Review the information and click **Finish**.
- j. Tivoli Storage Productivity Center for Replication is installed with no license. You must install the Two Site or Three Site Business Continuity (BC) license. For information about installing the license, see "Installing the Two Site or Three Site Business Continuity license."
- 16. The Successfully installed panel is displayed. Click Finish.
- 17. After you have installed Tivoli Storage Productivity Center, you can use the Configuration Utility to learn how to configure your system. Follow these steps to go to the Configuration Utility:
  - a. Open the Tivoli Storage Productivity Center GUI.
  - b. Go to Tivoli Storage Productivity Center > Configuration Utility.
- For Tivoli Storage Productivity Center for Replication configuration, see the Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/ v4r1/index.jsp. Click Tivoli Storage Productivity Center for Replication > Configuring.

# Installing the Two Site or Three Site Business Continuity license

This section describes how to install the IBM Tivoli Storage Productivity Center for Replication Two Site or Three Site Business Continuity (BC) license.

To install the license for IBM Tivoli Storage Productivity Center for Replication, you must run as the root user on Linux or AIX, or as the administrator in Windows. Use the Two Site or Three Site CD for the installation of the license.

To install the IBM Tivoli Storage Productivity Center for Replication Two Site or Three Site Business Continuity license, follow these steps:

- 1. Begin the installation program by double-clicking the setup file:
  - Windows: <installation\_source\_directory>\setupwin32.exe

- Linux: <installation\_source\_directory>\setuplinux.bin
- AIX: <installation\_source\_directory>\setupaix.bin
- 2. On the Welcome page, click Next.
- The Software License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select I accept the terms of the license agreement. Click Next.
- 4. On the Directory name panel, click Next.
- 5. Review the settings and click Install.

# Using custom installation

This section describes how to install IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication using custom installation.

# Installing all the components

This procedure provides information on how to install all of the IBM Tivoli Storage Productivity Center components and IBM Tivoli Storage Productivity Center for Replication except for the deployment of remote agents.

To install all of the Tivoli Storage Productivity Center components and IBM Tivoli Storage Productivity Center for Replication, complete the following steps:

**Note:** The DB2 database schema name for Tivoli Storage Productivity Center cannot be longer than eight characters.

- If you do not have Agent Manager installed, but want to use Data agents or Fabric agents, install the Agent Manager first. If you are installing Agent Manager on a different machine from Tivoli Storage Productivity Center, install DB2 on that machine. For information about installing the Agent Manager, see "Installing the Agent Manager" on page 131.
- 2. Start the Tivoli Storage Productivity Center installation program. For information about starting the installation program, see "Starting the installation program" on page 168.
- 3. The Select a language panel is displayed. Select a language and click OK.
- The Software License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select I accept the terms of the license agreement. Click Next.

**Note:** 8 GB of RAM is required. If you have 4-8 GB of RAM, you can still install Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication. However, you will get a warning message. You should run only Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication because of system load. For information about how to disable Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication after installation, see "Disabling Tivoli Storage Productivity Center or Tivoli Storage Productivity Center or Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication after installation, see "Disabling Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication" on page 341.

5. The Select the type of installation you want to run panel is displayed.

🕲 IBM Tivoli Storage Pro	oductivity Center - Install	er	- 🗆 ×
	Select the type of installa	ation you want to run	
	C Typical installation	arros B	
IBM.	This will install the Dat and CLI. A new databa database during instal	a server and Device server, Data agent and Fabric agent, GUI se will be created, and the schema will be created on the lation. The database and schema will be reused for upgrade.	
	C Servers	Clients	
	C Agents	Register with the agent manager	
	Custom installation	1	
	This will install the Dat and CLI, and database computers. You can ch computer. You will haw computer.	a server and Device server, Data agent and Fabric agent, GUI on this computer. Remote agents are installed on other hoose any server, agent, or client to be installed on this e a choice to create the database and schema on this	
	C:\Program Files\IBM\"	TPC Installation Location	
	≺ Ba	ck Next≻ Cancel	

Figure 39. Select the type of installation you want to run panel

You have these options:

# Typical installation

For information about typical installation, see "Using typical installation" on page 171.

#### **Custom installation**

Allows you to install one or more components separately.

#### **Installation licenses**

This will install the Tivoli Storage Productivity Center licenses. The Tivoli Storage Productivity Center license is on the DVD. You only need to run this option when you add a license to a Tivoli Storage Productivity Center package that has already been installed on your system. For example, if you have installed Tivoli Storage Productivity Center for Data package, the license will be automatically installed when you install the product. If you decide to later enable IBM Tivoli Storage Productivity Center for Fabric, run the installation program and select **Product licenses Installation**. This option will allow you to install the license key from the DVD. You do not have to install the IBM Tivoli Storage Productivity Center for Fabric product.

For information about upgrading the license, see "Adding an installation license" on page 240.

Select **Custom installation**. Enter the Tivoli Storage Productivity Center Installation Location or accept the default:

C:\Program Files\IBM\TPC (for Windows) /opt/IBM/TPC (for UNIX or Linux)

Click Next.

6. The Select one or more components to install panel is displayed.



Figure 40. Select one or more components to install panel

Select the following:

- Create database schema
- Tivoli Storage Productivity Center Servers
- GUI
- Data Agent
- Remote Data Agent (for information, see "Installing the agents" on page 241)
- CLI
- Fabric Agent
- Remote Fabric Agent (for information, see "Installing the agents" on page 241)
- Register with the Agent Manager (if you have Agent Manager installed)

If you select Data Agent or Fabric Agent, the Agent Manager Registration box will also be checked. Click **Next**.

The **Register Launch Information With Other Applications** option does not install the main Tivoli Storage Productivity Center components (database schema, Data server, Device server, CLI, GUI, agents, IBM Tivoli Integrated Portal, or IBM Tivoli Storage Productivity Center for Replication). Instead, this option only installs and registers the Tivoli Storage Productivity Center web portal and portlets inside another WebSphere-based application, the most common being IBM Tivoli Integrated Portal. Once you have registered the Tivoli Storage Productivity Center launch information with an existing instance of IBM Tivoli Integrated Portal, then you will be able to launch the Tivoli Storage Productivity Center GUI from within that IBM Tivoli Integrated Portal Console.

Note:

- The Agent Manager and agents do not support IPv6 communication. Therefore, for an IPv6 only system, the check boxes for Data Agent, Remote Data Agent, Fabric Agent, Remote Fabric Agent, and Register with the Agent Manager will be disabled.
- If you are installing a new Tivoli Storage Productivity Center server using custom installation, you should install all of the components simultaneously rather than individually.
- 7. The Database administrator information panel is displayed. Enter a database administrator user ID and password. Click **Next**.

🕲 IBM Tivoli Storage Pro	ductivity Center - Installer		
	Database administrator inform	nation	
IBM.	Enter the database administr database during installation Database administrator	rator user ID and password to connect to the and uninstallation.	-
			-
	Password	*****	1
	< Back	Next > Cancel	

Figure 41. Database administrator Information panel

8. The new database schema information panel is displayed.

	New database sch Enter the database with the instance a	ema infor e informat ind creatir	mation ion that the pro ng the required	oduct will use when con I repository tables.	nmunicating
IDM 🛛 💋	DB user ID	db2a	ıdmin	Password	*****
	C Use local datab	ase			
	Port		Database	Path	Instance
7100	C Use remote dat	abase		Database name	ТРСОВ
	Host name		Port	50000	
	C:\PROGRA~1	VIBM\SQL	LIB91\java\db:	2jcc.jar	JDBC driver
prail-	Create local database		Database name	TPCDB	
Viet				Database creation de	etails
NP/L-					
		< Back		Next >	Cancel

Figure 42. New database schema information panel

If you click **Database creation details**, you will see the Database schema creation information panel. Use this panel to change the database schema. Do not change the default values unless you are a knowledgeable DB2 administrator. The Database Management (DMS) and Automatic Storage options are for advanced users only. For information about tablespace allocation, see "Estimating tablespace allocation" on page 606. Also refer to your DB2 documentation. If you do change this information, click **OK**.

**Note:** The DB2 database schema name for Tivoli Storage Productivity Center cannot be longer than eight characters.

🕙 IBM Tivoli Storage Pr	oductivity Center - Installer				_ 🗆 🗙
TRM.	Database schema creation Enter the information to cr remote) computer.	i information eate the database schema o	n the specified	l (local or	
	Schema name	TPC			
	Database Drive	c:	Browse	200 MB 💌	
	Tablespace	Container directory		Size	
	Normal	C:\DB2\TPCDB\TPC	Browse	200 MB 💌	
- dealers	Key	C:\DB2\TPCDB\TPC	Browse	200 MB 💌	
	Big		Browse	350 MB 💌	
	Temp		Browse	200 MB 💌	
1 11 15	Temporary user	C:\DB2\TPCDB\TPC	Browse	200 MB 💌	
Wife .	<ul> <li>System managed (SM</li> <li>Log location</li> </ul>	IS) C Database n C Automatic Storage	nanaged (DMS	3)	
	C:\DB2\TPCDB\TPC	Browse	Size	20 MB 💌	
		ОК		Cancel	

Figure 43. Database schema creation information panel

**9**. The Data server, Device server, Data agent, and Agent information panel is displayed.

The Agent Manager and agents only support IPv4 communication. If you have a server that is enabled for both IPv6 and IPv4, specify the IPv4 address.

🖤 IBM Tivoli Storage Pro	oductivity Center - Insta	ller			
	Data server, Device ser	ver, Data agent, and Agent	Information		
IBM.	Enter the server name communicate with the	and port that the Data ager server.	it and Fabric agent, and	GUI will use to	
	Data server name	mdm-b26-w2k3.bea	Data server port	9549	
A	Device server name	mdm-b26-w2k3.bea	Device server port	9550	
	Enter an OS user grou administrators group.	p whose members will be <sup>-</sup>	TPC administrators in th	e	
	TPC superuser	C superuser Administrators Secu <u>r</u> ity roles		S	
	Enter a password that the Fabric agents will use to communicate with the Device server.				
	Host authentication pa	ssword			
1 Prost-	Enter a password that will be used to create the Data Server Account.				
111:1	Data Server Account Pa	assword			
UPA -	WAS admin ID	Passy	vord		
all all all			<u>N</u> AS discovery		
			Data agent <u>o</u> ptions	34 23	
	< <u>B</u> a	nck <u>N</u> e	ext >	<u>C</u> ancel	

Figure 44. Data server, Device server, Data agent, and Agent information panel

Enter the following information:

#### **Data Server Name**

Enter the fully-qualified host name of the Data server.

#### **Data Server Port**

Enter the Data server port. The default is 9549.

# Device Server Name

Enter the fully-qualified host name of the Device server.

#### **Device Server Port**

Enter the Device server port. The default is 9550.

#### **TPC Superuser**

Enter an operating system group name to associate with the TPC Superuser role. This group must exist in your operating system before you install Tivoli Storage Productivity Center. Membership in this group provides full access to the Tivoli Storage Productivity Center product. You can assign a user ID to this group on your operating system and start the Tivoli Storage Productivity Center GUI using this user ID.

**Note:** If you select LDAP authentication later in the Tivoli Storage Productivity Center installation, then the value you enter for LDAP TPC Administrator group overrides the value you entered here for the TPC Superuser.

#### Host authentication password

This is the password used by the Fabric agent to communicate with the Device server. This password must be specified when you install the Fabric agent.

### Data Server Account Password

For Windows only. You supply this password. When you supply this password, the Tivoli Storage Productivity Center installation program creates a user ID and the password you supplied to create the Data server account on Windows. This user ID and password is used by the Data server service.

The display name for the Data Server is:

IBM Tivoli Storage Productivity Center - Data Server

#### WAS admin ID and Password

This is the user ID and password required by the Device server to communicate with embedded WebSphere. This is only used at installation time.

**Note:** If you select LDAP authentication later in the Tivoli Storage Productivity Center installation, then the values you enter for LDAP TPC Administrator username and password override the value you entered here for WAS Admin ID and password.

#### Click Next.

#### If you click the Security roles button:

The Advanced security roles mapping panel is displayed. Enter the operating system group for each Tivoli Storage Productivity Center role you want to make an association with. The operating group must exist before you can associate a Tivoli Storage Productivity Center role with a group. Click **OK**. Click **Next**.

**Note:** You do not have to assign security roles at installation time. You can assign these roles after you have installed Tivoli Storage Productivity Center.

If you select LDAP authentication later in the Tivoli Storage Productivity Center installation, then the values you enter here for Security Roles Mapping will be deleted and you will have to assign roles to individuals after the installation is complete (use the **Role-to-Group Mapping** node).

🕲 IBM Tivoli Storage Pr	oductivity Center - Installer					
	Advanced security roles mapping					
IBM.	Product supports "Role Based" security for each of its manager components. You can assign a group to a role mapping for any of the following roles supported. By default, the TPC superuser role will have an Administrators group authority on Windows, and a system or root group authority on UNIX or Linux.					
	User role OS group User role OS group					
	TPC superuser Administrators TPC administrator					
	Data administrator Data operator					
	Disk administrator Disk operator					
	Fabric administrator Fabric operator					
11825	Tape administrator Tape operator					
White :						
	OK Cance					

Figure 45. Advanced security roles mapping panel

#### If you click the NAS discovery button:

The NAS discovery information panel is displayed. Enter the NAS filer login default user name and password. If you want to enter the SNMP communities to be used for NAS discovery, click **Add**, enter the community name, then click **OK**. Click **Next** on the Data server, the Device server, Data agent, and Agent information panel.

🕲 IBM Tivoli Storage Pro	ductivity Center - Installer	_ 🗆 X
	NAS Discovery Information (Optional)	
IBK.	Enter the default NAS filer login and SNMP community information for use by the Data agents on Windows during NAS discovery.	
	Default NAS Filer login to be used during NAS discovery	
	User name	
	Password	
	SNMP communities to be used during NAS discovery	
	SNMP community Add Delete	
1.1.1.2		
1 Ni At		
	<u> </u>	

Figure 46. NAS discovery information panel

# If you click the Data agent options button:

The Data agent options panel is displayed. You will be able to select whether or not you want the agent to perform an initial scan when first brought up. You can also select whether or not the agent can run scripts sent by the server. Make your selections and click **OK**.



Figure 47. Data Agent Options panel

The options are:

# Agent should perform a scan when first installed

Clear the check box for this option if you do not want Data Manager to perform an initial scan of your storage upon installation. This option is checked by default and gathers default statistics.

# Agent may run scripts sent by server

Leave this option checked if you want to store scripts in the server's \scripts directory that will run on all agents. When a script needs to be run on a particular agent, the server will access that script from its local \scripts directory and send it to the appropriate agent.

If you clear the check box for this option, the agents will ignore scripts sent by the server. You will have to store a copy of every script in every agent's \scripts directory.

The default \scripts directory for an agent behaves as described below:

If a script with the same name exists on both the server and the agent, the script stored on the agent will take precedence. This is useful if you want to run a special version of a script on one agent that is different from the version you are running on all the other agents.

The following example demonstrates the advantage of storing scripts at the server level. To monitor a computer's file system free space, you can store a script on the server that runs when any computer on the network meets a specified low file system free space threshold condition. But you could also store a special script on one computer that defined a different threshold for that computer. This script would take precedence over the script stored on the server.

The default directory for the \scripts directory is as follows:

C:\Program Files\IBM\TPC\data\scripts (for Windows)
/opt/IBM/TPC/data/scripts (for UNIX or Linux)

Click OK.

10. The Agent Manager information panel is displayed.

sibilition Scoluge in			
	Agent manager information		
IBM.	Enter the information that the prod server, Data agent, or Fabric agen	luct will use to register its Data server, Device t with the agent manager.	
	Hostname or IP address	mdm-b26-w2k3.beaverton.ibm.com	
	Port (Secured)	9511	
	Port (Public)	9513	
1000	Enter the Data server and Device : the agent manager.	server registration information as specified on	
	User ID	manager	
	Password		
free-	Enter the common agent registrat manager.	ion password as specified on the agent	
NY	Password		
APAL :			
	c Pask	Next > Cancel	1

Figure 48. Agent Manager information panel

Complete the following information:

#### Hostname or IP address

Use fully-qualified host names (for example, tpcam.toronto.ibm.com) for this field. Do not use the short form of the host name (for example, tpcam). The short host name can prevent successful agent deployments. You can also specify the IPv4 IP address of the Agent Manager server, but this is not suggested for a production environment because it limits the flexibility if a server IP address needs to be changed. If a fully-qualified host name is used, it can be reassigned to the new IP address in the DNS and the Agent Manager environment should continue to operate as it did before the address change.

**Note:** Agent Manager does not support IPv6 addressing. If an IPv6 address is entered, you will receive an error message.

#### Port (Secured)

Port number of the Agent Manager server. The default is 9511.

#### **Port (Public)**

The public communication port. The default is 9513.

Enter the Data server and the Device server registration information as specified on the Agent Manager

# User ID

This is the resource manager registration user ID. This user ID is used to register the Data server or the Device server with the Agent Manager. The default is **manager**.

#### Password

This is the resource manager registration password. This password is used to register the Data server or the Device server with the Agent Manager. The default is **password**.

# Enter the Common agent registration password as specified on theAgent Manager

# Password

This is the Common agent registration password used by the Common agent to register with the Agent Manager. This was specified when you installed the Agent Manager.

Click Next.

11. The Common agent selection panel is displayed. You can install a new Common agent or use an existing Common agent. Select Install the new Common agent at the location listed below for a new Common agent. Enter a directory or accept the default directory where the Common agent will be installed. Enter the port that the Data agent and Fabric agent will use to listen and communicate with the Common agent. The default port is 9510. Click the Windows service info button to enter user ID and password information for the Windows service account. Click Next.

If you have an existing Common agent already installed, select **Select an existing Common agent from the list below**. The table will list the Common agents you have installed. Select a Common agent and click **Next**.

A C C	Install the new c	ommon agent at ti	ne location listed b	elow	
	C:\Program File:	s\IBM\TPC\ca		E	rowse
	Agent port	9510			
		ta di	Windows service	info	1
	Port	Version	Location	Data agent	Fabric age
12 -					
A ALT					
100 00					

Figure 49. Common agent Selection panel

Click the **Windows service info** button to enter a Common agent service name, user ID, and password information that the installation program will use to create a Windows service for the Common agent. This is optional. If you do not specify a Windows service account, by default, **itcauser** is created. Click **OK**.

🕲 IBM Tivoli Storage Pro	ductivity Center - Installer	_ 🗆 X
	Common agent service information (Optional)	
	Enter the information to create the Windows service for the common agent.	
IBM.	Common agent service name	
	Common agent service logon account information	
	User ID	
	Password	
1 Wash		
11 15		
1112-		
NILL+		
	<u> </u>	

Figure 50. Common agent service information panel

12. The Tivoli Integrated Portal installation panel is displayed. This panel lets you select an existing IBM Tivoli Integrated Portal to use or install the IBM Tivoli Integrated Portal program.

🕙 IBM Tivoli Storage Produ	ictivity Center - Installer	
IBM.	Tivioli Integrated Portal (TIP) TIP provides TPC with the ability for Single Sign-On authentication, launch o applications in context, and reports to be viewed from Tivoli Common Repo Select an existing TIP install to be used with TPC or specify the install direct where TPC is to install TIP.	ther rting. ory
	C:\Program Files\IBM\Tivolitip	Browse
	Existing TIP Installs: CXIBMtivolittipA TIP Administrator ID wasAdmin Password ******	
	< Back Next > Ca	ncel

Figure 51. Tivoli Integrated Portal installation panel

Enter the following information:

# Specify the location to install TIP

Accept the default or enter a location to install Tivoli Integrated Portal.

- **Port** Enter the port number for Tivoli Integrated Portal or accept the default (16310). Tivoli Integrated Portal uses 10 port numbers. For example, if the default port 16310 is accepted, Tivoli Integrated Portal uses the following ports: 16310, 16311, 16312, 16313, 16315, 16316, 16318, 16320, 16322, and 16323. If you enter a port number other than the default number, ensure that you have the following ports available for Tivoli Integrated Portal:
  - base port
  - base port +1
  - base port +2
  - base port +3
  - base port +5
  - base port +6
  - base port +8
  - *base port* +10
  - base port +12
  - base port +13

where *base port* is the port value entered in the **Port** field.

# Reuse an existing TIP install

Select this option if you want to use an existing IBM Tivoli Integrated Portal. Under **Existing TIP installs**, select a IBM Tivoli Integrated Portal to use. Enter the following information:

# **TIP Administrator ID**

Enter the IBM Tivoli Integrated Portal administrator ID.

#### Password

Enter the IBM Tivoli Integrated Portal password of the administrator ID.

Click Next.

**13**. The authentication selection panel is displayed. If a valid IBM Tivoli Integrated Portal instance exists on the system and it uses either the OS-based authentication or LDAP-based authentication, then IBM Tivoli Storage Productivity Center will use that existing authentication method. Otherwise, select the authentication method to use.



Figure 52. Authentication selection panel

Single sign-on is a method of access control that enables a user to log in once and gain access to the resources of multiple software systems without being prompted to log in again. The single sign-on feature requires a centralized user and group repository, such as an LDAP-compliant directory, that all participating applications can access. The user's credentials are passed between applications in a secure manner. If you do not want to use LDAP or Active Directory, you can select OS authentication. Select the authentication method to use and click **Next**.These are the options:

# **OS** Authentication

This uses the operating system for user authentication. If you select this option, go to step 17.

# LDAP/Active Directory

If you select LDAP or Microsoft Active Directory for authentication, you must have an LDAP or Active Directory already installed. If you select this option, go to step 14. Click **Next**.

14. If you selected **LDAP/Active Directory**, there is more information that Tivoli Storage Productivity Center needs to be collected.

🕲 IBM Tivoli Storage Prod	uctivity Center - Installer	×
TIBM Tivoli Storage Prod	uctivity Center - Installer         Lightweight Directory Access Protocol (LDAP)         Specify the LDAP server information required for TPC to use LDAP authentication. The Bind Distinguished Name and Bind Password options are optional if the LDAP server supports anonymous binds and user or group creation from TIP is not required.         LDAP Server Hostname         LDAP Port Number         389         The following are optional if anonymous binds are allowed:	X
	Bind Distinguished Name Bind Password Sind Password Sind Password Cancel	

Figure 53. LDAP Server information panel

Enter this information and click Next.

# **LDAP Server Hostname**

The fully-qualified host and domain name of the machine where your LDAP-based directory is running.

#### LDAP Port Number

The port number on your LDAP server where the LDAP process is listening for communications.

# Bind Distinguished Name

The distinguished name used to bind to the LDAP-based directory when performing a user or group search. This name is optional because some LDAP-based Directories allow anonymous binds and others require you to bind with a specific name and password.

**Note:** Depending on how the LDAP server is set up, the Bind DN and password might or might not be optional. If the LDAP server allows for anonymous binds, then the Bind DN and password are optional.

If you want the ability to create or modify LDAP users and groups from the Tivoli Integrated Portal admin panel, then the Bind DN and password are required.

#### **Bind Password**

The password associated with the Bind Distinguished Name.

Enter this information and click Next.

**15.** The Lightweight Directory Access Protocol (LDAP user and group information) panel is displayed.

🕲 IBM Tivoli Storage Proc	ductivity Center - Installer	_ 🗆 🗙
TEM &	ductivity Center - Installer Lightweight Directory Access Protocol (LDAP) Specify the LDAP user and group information required for TPC to use LDAP authentication. Relative Distinguished Name for usernames L Attribute to use for usernames L IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	
	Attribute to use for groups cn < <u>Back</u> <u>N</u> ext > <u>C</u> ancel	

Figure 54. LDAP user and group information panel

Enter this information and click Next.

# **Relative Distinguished Name for usernames**

Tells IBM Tivoli Storage Productivity Center where to start a search in the directory when performing user authentication.

#### Attribute to use for usernames

Tells IBM Tivoli Storage Productivity Center which attribute in a user's directory entry contains the user's name for authentication.

# **Relative Distinguished Name for groups**

Tells IBM Tivoli Storage Productivity Center where in the directory to start a search when performing a group search for authorization.

#### Attribute to use for groups

Tells IBM Tivoli Storage Productivity Center which attribute in a group's directory entry contains the group's name for authorization.

**16.** The Lightweight Directory Access Protocol (LDAP TPC Administrator user and group information) panel is displayed.

🕲 IBM Tivoli Storage Prod	luctivity Center - Installer	_ 🗆 🗙
IBM.	Lightweight Directory Access Protocol (LDAP) Specify the LDAP TPC Administrator user and group that will have the TPC Administrator privileges.	
	LDAP TPC Administrator username	
	LDAP TPC Administrator group	
	< <u>B</u> ack <u>N</u> ext > <u>C</u> ancel	

Figure 55. LDAP TPC Administrator user and group information panel

Enter information for these fields:

# LDAP TPC Administrator username

The user ID that IBM Tivoli Storage Productivity Center will configure as the IBM Tivoli Storage Productivity Center superuser during installation. This user name should already exist in the directory before you start the IBM Tivoli Storage Productivity Center installation and should be a member of your designated LDAP IBM Tivoli Storage Productivity Center Administrator group in the directory.

**Note:** If you install IBM Tivoli Storage Productivity Center on a Windows system and have IBM Tivoli Storage Productivity Center authenticate users against an LDAP-based repository, then the LDAP TPC Administrator username must **not** contain a space or blank character in it. See the WebSphere Application Server APAR PK77578.

Ensure that you use the correct case when entering the values for the LDAP TPC Administrator username and LDAP TPC Administrator group. If you use the incorrect case when entering these values, then you will not be able to login to Tivoli Storage Productivity Center for Replication with the user name you expected to use.

#### LDAP TPC Administrator password

Password for the administrator.

# LDAP TPC Administrator group

The group that IBM Tivoli Storage Productivity Center will map to the IBM Tivoli Storage Productivity Center superuser role during installation. This group should already exist in the directory before you start the IBM Tivoli Storage Productivity Center installation and should have the designated LDAP IBM Tivoli Storage Productivity Center Administrator as a member.

#### Note:

Ensure that you use the correct case when entering the values for the LDAP TPC Administrator username and LDAP TPC Administrator group. If you use the incorrect case when entering these values, then you will not be able to login to Tivoli Storage Productivity Center for Replication with the user name you expected to use.

- 17. The Summary Information panel is displayed. Review the information. Click **Install**.
- **18**. You will see the installing panel. When Tivoli Integrated Portal has finished installing, Tivoli Storage Productivity Center will start the Tivoli Storage Productivity Center for Replication installation.
- **19.** Tivoli Storage Productivity Center starts the IBM Tivoli Storage Productivity Center for Replication installation program.
  - a. The Welcome panel is displayed. Click Next.
  - b. The System prerequisites check panel is displayed. The installation wizard checks whether the prerequisites are installed, then confirms whether your operating system is supported and is at the appropriate fix pack or update level. Click **Next**.
  - c. The License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select I accept the terms of the license agreement. Click Next.
  - d. The Directory Name panel is displayed. Accept the default installation directory by clicking **Next**, or specify a different installation directory and click **Next**.
  - e. The IBM Tivoli Storage Productivity Center for Replication Administrator ID and Password panel is displayed. Enter the administrator user ID and password. This ID is usually the operating system administrator user ID. If you use a different ID, create it beforehand and ensure that it has administrator rights.

**Note:** There is a limitation on the number of characters for the user name and password on AIX. At the time this document was written, AIX did not properly validate passwords that are longer than eight characters.

- f. The Default ports panel is displayed. Accept the defaults. Click Next.
- g. The settings panel is displayed. Review the settings and change them if needed by clicking **Back**. Otherwise, click **Install** to begin the installation.
- h. You will see the status panel. Wait for installation to complete.
- i. You will see the summary information panel. Review the information and click **Finish**.
- j. Tivoli Storage Productivity Center for Replication is installed with no license. You must install the Two Site or Three Site Business Continuity (BC) license. For information about installing the license, see "Installing the Two Site or Three Site Business Continuity license" on page 197.
- 20. The successfully installed panel is displayed. Click Finish.
- **21.** After you have installed Tivoli Storage Productivity Center, you can use the Configuration Utility to learn how to configure your system. Follow these steps to go to the Configuration Utility:
  - a. Open the Tivoli Storage Productivity Center GUI.
  - b. Go to Tivoli Storage Productivity Center > Configuration Utility.

22. For IBM Tivoli Storage Productivity Center for Replication configuration, see the Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/ v4r1/index.jsp. Click **Tivoli Storage Productivity Center for Replication** > **Configuring**.

# Creating the database schema

This topic provides information on how to create the database schema for IBM Tivoli Storage Productivity Center. You must create a database schema before you can use Tivoli Storage Productivity Center. If you are using a remote database for Tivoli Storage Productivity Center, you must install the database schema on that remote computer after you have installed DB2. This option also allows you to specify the type of table space you want to use to store your data on DB2.

**Note:** The DB2 database schema name for Tivoli Storage Productivity Center cannot be longer than eight characters.

To create the database schema, complete the following steps:

- 1. If you are installing the database on AIX or Linux, source the db2profile.
- 2. Start the Tivoli Storage Productivity Center installation program. For information about starting the installation program, see "Starting the installation program" on page 168.
- 3. The Select a language panel is displayed. Select a language and click OK.
- The Software License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select I accept the terms of the license agreement. Click Next.
- 5. The Select the type of installation you want to run panel is displayed. Select **Custom installation**. Enter the Tivoli Storage Productivity Center Installation Location or accept the default:

C:\Program Files\IBM\TPC (for Windows) /<usr or opt>/IBM/TPC (for UNIX or Linux)

Click Next.

- 6. The Select one or more components to install panel is displayed. Select **Create database schema**. Click **Next**.
- 7. The Database administrator information panel is displayed. Enter the database administrator user ID and password. This user ID and password were specified when you installed DB2.
- 8. The New database schema information panel is displayed.

	New database scho Enter the database with the instance a	New database schema information Enter the database information that the product will use when comn with the instance and creating the required repository tables.				
IBM•	DB user ID	db2adm	in l	⊃assword	*****	
	C Use local datab	ase				
	Port	Di	atabase	Path	Instance	
	C Use remote data	abase localhos	st	Database name Port	TPCDB 50000	
	C:\PROGRA~1	\IBM\SQLLIB!	31\java\db2jcc	.jar	JDBC driver	
1 section	Create local dat	abase		Database name	TPCDB	
NET		l	C	atabase creation de	etails	
VER :						
		< Back		Next >	Cancel	1

Figure 56. New database schema information panel

Select **Create local database** and enter the database name or accept the default (TPCDB). Click **Next**.

If you click **Database creation details**, you will see the Database schema creation information panel. This allows you to change the database schema.

Do not change the default values unless you are a knowledgeable DB2 administrator. For information about tablespace allocation, see "Estimating tablespace allocation" on page 606. Also refer to your DB2 documentation.

Make your changes and click **OK**. Click **Next** on the New database schema information panel.

🕲 IBM Tivoli Storage Pro	oductivity Center - Installer	8			. 🗆 🗙	
TEM.	Database schema creatio Enter the information to c remote) computer.	n information reate the database schema of	n the specified	d (local or		
	Schema name	TPC				
	Database Drive	c:	Browse	200 MB 💌		
	Tablespace	Container directory		Size		
	Normal	C:\DB2\TPCDB\TPC	Browse	200 MB 💌		
	Key	C:\DB2\TPCDB\TPC	Browse	200 MB 💌		
	Big	C:\DB2\TPCDB\TPC	Browse	350 MB 💌		
	Temp	C:\DB2\TPCDB\TPC	Browse	200 MB 💌		
	Temporary user	C:\DB2\TPCDB\TPC	Browse	200 MB 💌		
Wife	System managed (Si Log location	System managed (SMS) C Database managed (DMS) C Automatic Storage g location				
		Browse	Size	20 MB 💌		
	-	ОК		Cancel	1	

Figure 57. Database schema creation information panel

Note:

- If you installed Agent Manager on this computer, you will see **IBMCDB** listed. Do **not** use this database; it is for Agent Manager.
- If you are installing on AIX, the default location of the database schema should be changed to a file system with adequate space. The DB2 administrator and the Tivoli Storage Productivity Center installer must have authority to modify the database. The default is for Tivoli Storage Productivity Center to create a database in a directory homed off of root.
- 9. The Summary Information panel is displayed. Review the information. Click **Install**.
- 10. You will see the installing panel. Wait for installation to complete.
- 11. The successfully installed panel is displayed. Click Finish.

# Installing the servers using a local database

This procedure provides information on how to install the IBM Tivoli Storage Productivity Center servers using a local database.

To install the IBM Tivoli Storage Productivity Center servers, complete the following steps:

- 1. Start the IBM Tivoli Storage Productivity Center installation program. For information about starting the installation program, see "Starting the installation program" on page 168.
- The Software License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select I accept the terms of the license agreement. Click Next.

**Note:** 8 GB of RAM is required. If you have 4-8 GB of RAM, you can still install Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication. However, you will get a warning message. You should

run only Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication because of system load. For information about how to disable Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication after installation, see "Disabling Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication" on page 341.

- **3**. Go to the Select the type of installation you want to run panel. Select **Custom installation**. Click **Next**.
- 4. On the Select one or more components to install panel, select **Tivoli Storage Productivity Center Servers**. Click **Next**.
- 5. The Database administrator information panel is displayed. Enter a database administrator user ID and password. Click **Next**.
- 6. The New database schema information panel is displayed. Select **Create local database**. Click **Next**.

DB user ID	db	2admin	Password	******
C Use local (	database			
F	Port	Database	Path	Instance
C Use remot	ie database		Database name	TPCDB
Host name	e To	calhost	Port	50000
C:\PROG	RA~1\IBM\S(	QLLIB91\java\db	2jcc.jar	JDBC driv
Create loc	al database		Database name	TPCDB
			Database creation de	etails
		10.		

Figure 58. New database schema information panel

If you click **Database creation details**, you will see the Database schema creation information panel. This panel allows you to change the default space assigned t the database. You do not need to change these values and you can accept the default values. If you do change this information, click **OK**.

**Note:** The DB2 database schema name for Tivoli Storage Productivity Center cannot be longer than eight characters.

IBM Tivoli Storage Pr	oductivity Center - Installer	in da mara di su			_ 0		
TRM.	Database schema creation information Enter the information to create the database schema on the specified (local or remote) computer.						
	Schema name	TPC					
	Database Drive	<u>с:</u>	Browse	200 MB 💌			
	Tablespace	Container directory		Size			
	Normal	C:\DB2\TPCDB\TPC	Browse	200 MB 💌			
1 miles	Key	C:\DB2\TPCDB\TPC	Browse	200 MB 💌			
	Big	C:\DB2\TPCDB\TPC	Browse	350 MB 💌			
	Temp	C:\DB2\TPCDB\TPC	Browse	200 MB 💌			
1111-	Temporary user	C:\DB2\TPCDB\TPC	Browse	200 MB 💌			
UME -	<ul> <li>System managed (SM Log location</li> </ul>	S) C Database n O Automatic Storage	C Database managed (DMS)				
		Browse	Size	20 MB 💌			
		ОК		Cancel	1		

Figure 59. Database schema creation information panel

7. The Data server, Device server, Data agent, and Agent information panel is displayed.

🕲 IBM Tivoli Storage Pro	ductivity Center - Instal	ler					
	Data server, Device server, Data agent, and Agent Information						
iem.	Enter the server name and port that the Data agent and Fabric agent, and GUI will use to communicate with the server.						
	Data server name	mdm-b26-w2k3.bea	Data server port	9549			
A	Device server name	mdm-b26-w2k3.bea	Device server port	9550			
	Enter an OS user group whose members will be TPC administrators in the administrators group.						
	TPC superuser	Administrators	Secu <u>r</u> ity role	s			
	Enter a password that the Fabric agents will use to communicate with the Device server.						
	Host authentication password						
1 Junio	Enter a password that will be used to create the Data Server Account.						
1/1/1	Data Server Account Pa	assword					
	WAS admin ID	Passv	vord				
an alta	NAS discovery						
	Data agent <u>o</u> ptions						
	< <u>B</u> a	ck <u>N</u> e	xt >	<u>C</u> ancel			

Figure 60. Data server, Device server, Data agent, and Agent information panel

Enter the following information:

#### **Data Server Name**

Enter the fully-qualified host name of the Data server.

#### **Data Server Port**

Enter the Data server port. The default is 9549.

#### **Device server Name**

Enter the fully qualified host name of the Device server.

#### **Device server Port**

Enter the Device server port. The default is 9550.

#### **TPC Superuser**

Enter an operating system group name to associate with the TPC superuser role. This group must exist in your operating system before you install Tivoli Storage Productivity Center. Membership in this group provides full access to the Tivoli Storage Productivity Center product. You can assign a user ID to this group on your operating system and start the Tivoli Storage Productivity Center GUI using this user ID.

**Note:** If you select LDAP authentication later in the Tivoli Storage Productivity Center installation, then the value you enter for LDAP TPC Administrator group overrides the value you entered here for the TPC superuser. For more information about security roles, see "Planning for IBM Tivoli Storage Productivity Center authorization" on page 18.

#### Host authentication password

This is the password used by the Fabric agent to communicate with the Device server. This password must be specified when you install the Fabric agent.

#### Data Server Account Password

For Windows only. You supply this password. When you supply this password, the Tivoli Storage Productivity Center installation program creates a user ID and the password you supplied to create the Data server account on Windows. This user ID and password is used by the Data server service.

The display name for the Data Server is:

IBM Tivoli Storage Productivity Center - Data Server

#### WAS admin ID and Password

This is the WebSphere administration user ID and password required by the Device server to communicate with embedded WebSphere, if this user ID does not exist.

**Note:** If you select LDAP authentication later in the Tivoli Storage Productivity Center installation, then the values you enter for LDAP TPC Administrator username and password override the value you entered here for WAS Admin ID and password.

#### Click Next.

#### If you click the Security roles button:

The Advanced security roles mapping panel is displayed. Enter the operating system group for each Tivoli Storage Productivity Center role you want to make an association with. You do not have to assign security roles at installation time. You can assign these roles after you have installed Tivoli

Storage Productivity Center. Click **OK**. Click **Next** on the Data server, the Device server, Data agent, and Agent information panel.

**Note:** If you select LDAP authentication later in the Tivoli Storage Productivity Center installation, then the values you enter here for Security Roles Mapping are deleted and you will have to reset the mappings after the installation is complete using the **Role-to-Group Mappings** node.

IBM Tivoli Storage Pro	oductivity Lenter - Installer				
	Advanced security roles mapping				
IBM.	Product supports "Role Based" security for each of its manager components. can assign a group to a role mapping for any of the following roles supported default, the TPC superuser role will have an Administrators group authority or Windows, and a system or root group authority on UNIX or Linux.				
	User role OS group User role OS group				
	TPC superuser Administrators TPC administrator				
	Data administrator Data operator				
P P	Disk administrator Disk operator				
	Fabric administrator Fabric operator				
1925	Tape administrator Tape operator				
With :					
	OK Canad	1			
	OK Cance				

Figure 61. Advanced security roles mapping panel

8. The Agent Manager information panel is displayed.

🕲 IBM Tivoli Storage Pro	ductivity Center - Installer		_ 🗆 🗙			
	Agent manager information					
IBM.	Enter the information that the product will use to register its Data server, Device server, Data agent, or Fabric agent with the agent manager.					
	Hostname or IP address	mdm-b26-w2k3.beaverton.ibm.com				
A	Port (Secured)	9511				
	Port (Public)	9513				
	Enter the Data server and Device s the agent manager.	server registration information as specified on				
	User ID	manager				
2114	Password					
1 Unit	Enter the common agent registration password as specified on the agent manager.					
11 15 +	Password					
APR .						
	< <u>B</u> ack	Next > Cancel				

Figure 62. Agent Manager information panel

Complete the following information:

# Hostname or IP address

Fully qualified host name or IP address of the Agent Manager server.

#### Port (Secured)

Port number of the Agent Manager server. The default is 9511.

#### **Port (Public)**

The public communication port. The default is 9513.

# Enter the Data server and the Device server registration information as specified on the Agent Manager

#### User ID

This is the resource manager registration user ID. This user ID is used to register the Data Server or the Device server with the Agent Manager. The default is **manager**.

#### Password

This is the resource manager registration password. This password is used to register the Data Server or the Device server with the Agent Manager. The default is **password**.

# Enter the Common agent registration password as specified on the Agent Manager

#### Password

This is the Common agent registration password used by the Common agent to register with the Agent Manager. This was specified when you installed the Agent Manager. The default is **changeMe**.

#### Click Next.
**9**. The IBM Tivoli Integrated Portal Information panel is displayed. This panel lets you select an existing IBM Tivoli Integrated Portal to use or install the IBM Tivoli Integrated Portal program.

🕙 IBM Tivoli Storage Prod	uctivity Center - Installer	
IBM.	Tivioli Integrated Portal (TIP) TIP provides TPC with the ability for Single Sign-On authentication, applications in context, and reports to be viewed from Tivoli Commo Select an existing TIP install to be used with TPC or specify the inst where TPC is to install TIP.	launch other on Reporting. all directory
	C:\Program Files\IBM\Tivoli\tip         Port         16310         C Reuse an existing TIP install         Existing TIP Installs:	Browse
	C:\IBMtivoIRtipA TIP Administrator ID wasAdmin Password ****** < Back Next >	Cancel

Figure 63. TIP Information panel

Enter the following information:

## Specify the location to install TIP

Accept the default or enter a location to install Tivoli Integrated Portal.

- **Port** Enter the port number for Tivoli Integrated Portal or accept the default (16310). Tivoli Integrated Portal uses 10 port numbers. For example, if the default port 16310 is accepted, Tivoli Integrated Portal uses the following ports: 16310, 16311, 16312, 16313, 16315, 16316, 16318, 16320, 16322, and 16323. If you enter a port number other than the default number, ensure that you have the following ports available for Tivoli Integrated Portal:
  - base port
  - base port +1
  - base port +2
  - base port +3
  - base port +5
  - base port +6
  - base port +8
  - *base port* +10
  - *base port* +12
  - *base port* +13

where *base port* is the port value entered in the **Port** field.

# Reuse an existing TIP install

Select this option if you want to use an existing IBM Tivoli Integrated Portal. Under **Existing TIP installs**, select a IBM Tivoli Integrated Portal to use. Enter the following information:

# **TIP Administrator ID**

Enter the IBM Tivoli Integrated Portal administrator ID.

# Password

Enter the IBM Tivoli Integrated Portal password of the administrator ID.

Click Next.

10. The authentication selection panel is displayed. If a valid IBM Tivoli Integrated Portal instance exists on the system and it uses either OS-based authentication or LDAP-based authentication, then IBM Tivoli Storage Productivity Center will use that existing authentication method. Otherwise, select the authentication method to use.



Figure 64. Authentication selection panel

Single sign-on is a method of access control that enables a user to log in once and gain access to the resources of multiple software systems without being prompted to log in again. The single sign-on feature requires a centralized user and group repository, such as an LDAP-compliant directory, that all participating applications can access. The user's credentials are passed between applications in a secure manner. If you do not want to use LDAP or Active Directory, you can select OS authentication. Select the authentication method to use and click **Next**.These are the options:

# LDAP/Active Directory

If you select LDAP or Microsoft Active Directory for authentication, you must have an LDAP or Active Directory already installed. If you select this option, go to step 11. Click **Next**.

# **OS** Authentication

This uses the operating system for user authentication. If you select this option, go to step 13 on page 230. Click **Next**.

11. If you selected **LDAP/Active Directory** in step 10, there is more information that Tivoli Storage Productivity Center needs to collect.

🕲 IBM Tivoli Storage Prod	uctivity Center - Installer 📃 🗖 🗙
IBM.	Lightweight Directory Access Protocol (LDAP) Specify the LDAP server information required for TPC to use LDAP authentication. The Bind Distinguished Name and Bind Password options are optional if the LDAP server supports anonymous binds and user or group creation from TIP is not required.
	LDAP Server Hostname LDAP Port Number 389 The following are optional if anonymous binds are allowed:
	Bind Distinguished Name Bind Password
	< <u>B</u> ack <u>N</u> ext > <u>C</u> ancel

Figure 65. LDAP Server information panel

Enter this information and click Next.

#### LDAP Server Hostname

The fully-qualified host and domain name of the machine where your LDAP-based directory is running.

#### LDAP Port Number

The port number on your LDAP server where the LDAP process is listening for communications.

## **Bind Distinguished Name**

The distinguished name used to bind to the LDAP-based directory when performing a user or group search. This name is optional because some LDAP-based Directories allow anonymous binds and others require you to bind with a specific name and password.

**Note:** Depending on how the LDAP server is set up, the Bind DN and password might or might not be optional. If the LDAP server allows for anonymous binds, then the Bind DN and password are optional. If you want the ability to create or modify LDAP users and groups from the Tivoli Integrated Portal administrative panel, then the Bind DN and password are required.

#### **Bind Password**

The password associated with the Bind Distinguished Name.

🕲 IBM Tivoli Storage Produ	uctivity Center - Installer	_ 🗆 ×
IBM.	Lightweight Directory Access Protocol (LDAP) Specify the LDAP user and group information required for TPC to use LDAP authentication.	
	Relative Distinguished Name for usernames Attribute to use for usernames uid Relative Distinguished Name for groups	
	Attribute to use for groups cn	
	< <u>B</u> ack <u>N</u> ext > <u>C</u> ancel	

Figure 66. LDAP user and group information panel

Enter this information and click Next.

## **Relative Distinguished Name for usernames**

Tells IBM Tivoli Storage Productivity Center where in the directory to start a search when performing user authentication.

#### Attribute to use for usernames

Tells IBM Tivoli Storage Productivity Center which attribute in a user's directory entry contains the user's name for authentication.

#### **Relative Distinguished Name for groups**

Tells IBM Tivoli Storage Productivity Center where in the directory to start a search when performing a group search for authorization.

#### Attribute to use for groups

Tells IBM Tivoli Storage Productivity Center which attribute in a group's directory entry contains the group's name for authorization.

12. The LDAP TPC Administrator user and group information panel is displayed.

🕲 IBM Tivoli Storage Prod	luctivity Center - Installer	_ 🗆 🗡
IEM.	Lightweight Directory Access Protocol (LDAP) Specify the LDAP TPC Administrator user and group that will have the TPC Administrator privileges.	
	LDAP TPC Administrator username	
	< Back Next > Cancel	

Figure 67. LDAP TPC Administrator user and group information panel

Enter information for these fields:

# LDAP TPC Administrator username

The user ID that IBM Tivoli Storage Productivity Center will configure as the IBM Tivoli Storage Productivity Center superuser during installation. This user name should already exist in the directory before you start the IBM Tivoli Storage Productivity Center installation and should be a member of the LDAP IBM Tivoli Storage Productivity Center Administrator group in the directory.

**Note:** If you install Tivoli Storage Productivity Center on a Windows system and have Tivoli Storage Productivity Center authenticate users against an LDAP-based repository, then the LDAP Tivoli Storage Productivity Center Administrator username must **not** contain a space or blank character in it. See the WebSphere Application Server APAR PK77578.

Ensure that you use the correct case when entering the values for the LDAP TPC Administrator username and LDAP TPC Administrator group. If you use the incorrect case when entering these values, then you will not be able to login to Tivoli Storage Productivity Center for Replication with the user name you expected to use.

## LDAP TPC Administrator password

Password for the administrator.

# LDAP TPC Administrator group

The group that IBM Tivoli Storage Productivity Center will map to the IBM Tivoli Storage Productivity Center superuser role during installation. This group should already exist in the directory before

you start the IBM Tivoli Storage Productivity Center installation and should have the LDAP IBM Tivoli Storage Productivity Center Administrator as a member.

# Note:

Ensure that you use the correct case when entering the values for the LDAP TPC Administrator username and LDAP TPC Administrator group. If you use the incorrect case when entering these values, then you will not be able to login to Tivoli Storage Productivity Center for Replication with the user name you expected to use.

- **13**. The Summary Information panel is displayed. Review the information. Click **Install**.
- 14. You will see the installing panel. When Tivoli Integrated Portal has finished installing, Tivoli Storage Productivity Center will start the Tivoli Storage Productivity Center for Replication installation.
- **15.** Tivoli Storage Productivity Center starts the IBM Tivoli Storage Productivity Center for Replication installation program.
  - a. The Welcome panel is displayed. Click Next.
  - b. The System prerequisites check panel is displayed. The installation wizard checks whether the prerequisites are installed, then confirms whether your operating system is supported and is at the appropriate fix pack or update level. Click **Next**.
  - c. The License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select I accept the terms of the license agreement. Click Next.
  - d. The Directory Name panel is displayed. Accept the default installation directory by clicking **Next**, or specify a different installation directory and click **Next**.
  - e. The IBM Tivoli Storage Productivity Center for Replication Administrator ID and Password panel is displayed. Enter the administrator user ID and password. This ID is usually the operating system administrator user ID. If you use a different ID, create it beforehand and ensure that it has administrator rights.

**Note:** There is a limitation on the number of characters for the user name and password on AIX. At the time this document was written, AIX did not properly validate passwords that are longer than eight characters.

- f. The Default ports panel is displayed. Accept the defaults. Click Next.
- g. The settings panel is displayed. Review the settings and change them if needed by clicking **Back**. Otherwise, click **Install** to begin the installation.
- h. You will see the status panel. Wait for installation to complete.
- i. You will see the summary information panel. Review the information and click **Finish**.
- j. Tivoli Storage Productivity Center for Replication is installed with no license. You must install the Two Site or Three Site Business Continuity (BC) license. For information about installing the license, see "Installing the Two Site or Three Site Business Continuity license" on page 197.
- **16**. After you have installed Tivoli Storage Productivity Center, you can use the Configuration Utility to learn how to configure your system. Follow these steps to go to the Configuration Utility:
  - a. Open the Tivoli Storage Productivity Center GUI.

- b. Go to Tivoli Storage Productivity Center > Configuration Utility.
- For IBM Tivoli Storage Productivity Center for Replication configuration, see the Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/ v4r1/index.jsp. Click Tivoli Storage Productivity Center for Replication > Configuring.

# Installing the servers using a remote database

This section provides information on how to install the Data Server and Device server using a remote database.

# Preparing to install the Data Server and Device server using a remote database:

This topic provides information on the preparation steps required before installing the Data Server and Device server using a remote database.

Before installing the Data Server and Device server using a remote database, follow these steps:

- 1. Install DB2 on the remote computer if you have not already done so.
- **2**. Ensure that the DB2 instance is running on the database host computer before you run the installation program.
- 3. Ensure that the required JDBC drivers (db2jcc.jar and db2jcc\_license\_cu.jar) are copied from the remote database server to the local computer. The JDBC drivers are located in the Java subdirectory where you installed DB2 UDB on the database host computer.
- 4. Run the IBM Tivoli Storage Productivity Center installation program on the remote computer. Use the installation program to create the database schema and temporarily install an additional Tivoli Storage Productivity Center component. You need to install an additional component so that you can later run the uninstallation program to free the database for use by the Tivoli Storage Productivity Center servers. For example:
  - a. Run the installation program on the remote computer.
  - b. Select the **Custom installation** option.
  - c. Select the Create database schema and GUI options.
  - d. Complete the installation.

See "Installing the IBM Tivoli Storage Productivity Center family" on page 165 for more information about how to install the product.

5. Run the Tivoli Storage Productivity Center uninstallation program on the remote computer. Select to uninstall **Create database schema** and the other component you installed (for example, the **GUI** option). Complete the uninstallation process. See "Uninstalling the IBM Tivoli Storage Productivity Center family using the uninstallation program" on page 383 for more information about how to uninstall the product.

# Installing the Data server and the Device server using a remote database:

This procedure provides information on how to install the Data server and the Device server using a remote database.

**Note:** The DB2 database schema name for Tivoli Storage Productivity Center cannot be longer than eight characters.

To install the Data server and the Device server using a remote database, complete the following steps:

- Start the IBM Tivoli Storage Productivity Center installation program on your local computer. For information about starting the installation program, see "Starting the installation program" on page 168.
- The Software License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select I accept the terms of the license agreement. Click Next.

**Note:** 8 GB of RAM is required. If you have 4-8 GB of RAM, you can still install Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication. However, you will get a warning message. You should run only Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication because of system load. For information about how to disable Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication after installation, see "Disabling Tivoli Storage Productivity Center or Tivoli Storage Productivity Center or Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication after installation, see "Disabling Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication" on page 341.

- **3**. Go to the Select the type of installation you want to run panel. Select **Custom Installation**. Click **Next**.
- 4. On the Select one or more components to install panel, select **Tivoli Storage Productivity Center Servers**.
- **5**. The Database administrator information panel is displayed. Enter a database administrator user ID and password. Click **Next**.

🕲 IBM TotalStorage Productivity Center - Installer						
IIM.	Existing database so Enter the informati	chema informatio on to use an exis	n ting database :	schema for the r	repository.	
	DB user ID	db2inst1	Passw	ord 👬	***	
	C Use local datab:	ase			1	
	Port	Database	Schema	Instance	Version	
	Ose remote data	abase				
1 Long	Host name	papa.storage.t	tucs Port	5	0000	
11.12+	Database name	TPCDB	Schem	a name 🛛 🗖	PC	
111-	C:\PROGRA~1\I	3M\SQLLIB\java\d	lb2jcc.jar		JDBC driver	
ANID9		< <u>B</u> ack	<u>N</u> ext >		<u>C</u> ancel	

6. The Existing database schema information panel is displayed.

Figure 68. Existing database schema information panel

Select **Use remote database**. Enter the database name, schema name, fully qualified host name or IP address of the remote database server, and its port. Click **JDBC driver** to locate and open the JDBC driver, db2jcc.jar, copied from the database host computer. Click **Next**, and the Remote database manager pop-up message dialog is displayed. Ensure that the remote DB2 instance is running on the database host computer. Click **OK**.

7. The Data server, the Device server, Data agent, and Agent information panel is displayed. Enter the following information:

🕲 IBM Tivoli Storage Productivity Center - Installer 💦 📃 🔀						
	Data server, Device serv	ver, Data agent, and Agent	nformation			
IBM.	Enter the server name communicate with the s	and port that the Data ager server.	t and Fabric agent, and	GUI will use to		
	Data server name	mdm-b26-w2k3.bea	Data server port	9549		
	Device server name	mdm-b26-w2k3.bea	Device server port	9550		
	Enter an OS user group administrators group.	o whose members will be <sup>-</sup>	FPC administrators in th	ie		
	TPC superuser	Administrators	Security role:	S		
	Enter a password that the Fabric agents will use to communicate with the Device server					
	Host authentication pa	ssword				
1 1115-	Enter a password that	will be used to create the D	ata Server Account.			
1111	Data Server Account Pa	assword				
Charles -	WAS admin ID	Passv	vord			
AN ADAT			NAS discovery			
			Data agent <u>o</u> ptions			
	< <u>B</u> a	ck <u>N</u> e	xt >	<u>C</u> ancel		

Figure 69. Data server, the Device server, Data agent, and Agent information panel

# Data Server Name

Enter the fully qualified host name of the Data Server.

#### **Data Server Port**

Enter the Data Server port. The default is 9549.

#### **Device server Name**

Enter the fully qualified host name of the Device server.

#### **Device server Port**

Enter the Device server port. The default is 9550.

#### **TPC Superuser**

Enter an operating system group name to associate with the TPC Superuser role. This group must exist in your operating system before you install Tivoli Storage Productivity Center. Membership in this group provides full access to the Tivoli Storage Productivity Center product. You can assign a user ID to this group on your operating system and start the Tivoli Storage Productivity Center GUI using this user ID.

**Note:** If you select LDAP authentication later in the Tivoli Storage Productivity Center installation, then the value you enter for LDAP TPC Administrator group overrides the value you entered here for the TPC superuser. For more information about security roles, see "Planning for IBM Tivoli Storage Productivity Center authorization" on page 18.

#### Host authentication password

This is the password used by the Fabric agent to communicate with the Device server. This password must be specified when you install the Fabric agent.

#### Data Server Account Password

For Windows only. You supply this password. When you supply this password, the Tivoli Storage Productivity Center installation program creates a user ID and the password you supplied to create the Data server account on Windows. This user ID and password is used by the Data server service.

The display name for the Data Server is:

IBM Tivoli Storage Productivity Center - Data Server

#### WAS admin ID and Password

This is the WebSphere administration user ID and password required by the Device server to communicate with embedded WebSphere, if this user ID does not exist.

**Note:** If you select LDAP authentication later in the Tivoli Storage Productivity Center installation, then the values you enter for LDAP TPC Administrator username and password override the value you enter here for WAS Admin ID and password.

# Click Next.

If you want to associate operating system groups with Tivoli Storage Productivity Center security roles, click **Security roles**. Enter the operating system group for each Tivoli Storage Productivity Center role you want to make an association with. You do not have to assign security roles at installation time. You can assign these roles after you have installed Tivoli Storage Productivity Center. Click **OK**. Click **Next** on the Data server, the Device server, Data agent, and Agent information panel.

**Note:** If you select LDAP authentication later in the Tivoli Storage Productivity Center installation, then the values you enter here for Security Roles Mapping will be deleted and you will have to reset the mappings after the installation is complete through the **Role-to-Group Mapping** node.

8. The Agent Manager information panel is displayed. Complete the following information:

🕲 IBM Tivoli Storage Pro	ductivity Center - Installer		_ 🗆 🗙
	Agent manager information		
IBM.	Enter the information that the proc server, Data agent, or Fabric ager	luct will use to register its Data server, Device It with the agent manager.	
	Hostname or IP address	mdm-b26-w2k3.beaverton.ibm.com	
A	Port (Secured)	9511	
	Port (Public)	9513	
	Enter the Data server and Device the agent manager.	server registration information as specified on	
	User ID	manager	
	Password		
1 haven	Enter the common agent registrat manager.	ion password as specified on the agent	
11.10+ 1	Password		
11/1 -			
	< <u>B</u> ack	<u>N</u> ext ≻ <u>C</u> ancel	

Figure 70. Agent Manager information panel

# Hostname or IP address

Fully qualified host name or IP address of the Agent Manager server.

## Port (Secured)

Port number of the Agent Manager server. The default is 9511.

## **Port (Public)**

The public communication port. The default is 9513.

# Enter the Data server and the Device server registration information as specified on the Agent Manager

# User ID

This is the resource manager registration user ID. This user ID is used to register the Data Server or the Device server with the Agent Manager. The default is **manager**.

#### Password

This is the resource manager registration password. This password is used to register the Data Server or the Device server with the Agent Manager. The default is **password**.

# Enter the Common agent registration password as specified on the Agent Manager

#### Password

This is the Common agent registration password used by the Common agent to register with the Agent Manager. This was specified when you installed the Agent Manager. The default is **changeMe**.

Click Next.

**9**. The IBM Tivoli Integrated Portal Information panel is displayed. This panel lets you select an existing IBM Tivoli Integrated Portal to use or install the IBM Tivoli Integrated Portal program. Enter the following information:

# Specify the location to install TIP

Accept the default or enter a location to install Tivoli Integrated Portal.

- **Port** Enter the port number for Tivoli Integrated Portal or accept the default (16310). Tivoli Integrated Portal uses 10 port numbers. For example, if the default port 16310 is accepted, Tivoli Integrated Portal uses the following ports: 16310, 16311, 16312, 16313, 16315, 16316, 16318, 16320, 16322, and 16323. If you enter a port number other than the default number, ensure that you have the following ports available for Tivoli Integrated Portal:
  - base port
  - base port +1
  - base port +2
  - base port +3
  - base port +5
  - base port +6
  - *base port* +8
  - *base port* +10
  - *base port* +12
  - *base port* +13

where *base port* is the port value entered in the **Port** field.

# Reuse an existing TIP install

Select this option if you want to use an existing IBM Tivoli Integrated Portal. Under **Existing TIP installs**, select a IBM Tivoli Integrated Portal to use. Enter the following information:

#### **TIP Administrator ID**

Enter the IBM Tivoli Integrated Portal administrator ID.

#### Password

Enter the IBM Tivoli Integrated Portal password of the administrator ID.

Click **Next** to continue.

**10**. The authentication selection panel is displayed. If a valid IBM Tivoli Integrated Portal exists on the system, the authentication method that exists with the program will be used. Otherwise, select the authentication method to use.

The single sign-on feature is the method of access control that enables a user to authenticate once and gain access to the resources of multiple, trusted applications. To have a single sign-on environment, there must be a centralized authentication repository such as Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory. The LDAP or Active Directory must be accessed by all applications within a single sign-on environment. The user's ID and password are passed between applications in an encrypted manner. If you do not want to use LDAP or Active Directory, you can select OS authentication. Select the authentication method to use and click **Next**. These are the options:

# LDAP/Active Directory

Use LDAP or Active Directory for the centralized authentication repository. If you select **LDAP/Active Directory**, go to step 11.

## **OS** Authentication

Use operating system authentication. If you select **OS Authentication**, go to step 14.

11. If you selected **LDAP/Active Directory** in step 10, there is more information that Tivoli Storage Productivity Center needs to collect. The LDAP Server information panel is displayed. Enter this information and click **Next**.

### LDAP Server Hostname

The fully-qualified host and domain name of the machine where your LDAP-based directory is running.

#### LDAP Port Number

The port number on your LDAP server where the LDAP process is listening for communications.

# Bind Distinguished Name

The distinguished name used to bind to the LDAP-based directory when performing a user or group search. This name is optional because some LDAP-based Directories allow anonymous binds and others require you to bind with a specific name and password.

# **Bind Password**

The password associated with the Bind Distinguished Name.

**12.** The LDAP user and group information panel is displayed. Enter this information and click **Next**.

#### **Relative Distinguished Name for usernames**

Tells IBM Tivoli Storage Productivity Center where in the directory to start a search when performing user authentication.

#### Attribute to use for usernames

Tells IBM Tivoli Storage Productivity Center which attribute in a user's directory entry contains the user's name for authentication.

#### **Relative Distinguished Name for groups**

Tells IBM Tivoli Storage Productivity Center where in the directory to start a search when performing a group search for authentication or authorization.

## Attribute to use for groups

Tells IBM Tivoli Storage Productivity Center which attribute in a group's directory entry contains the group's name for authentication or authorization.

**13**. The LDAP TPC Administrator user and group information panel is displayed. Enter information for these fields:

# LDAP TPC Administrator username

The user ID that Tivoli Storage Productivity Center will configure as the Tivoli Storage Productivity Center superuser during installation. This user name should already exist in the directory before you start the Tivoli Storage Productivity Center installation and should be a member of your designated LDAP Tivoli Storage Productivity Center Administrator group in the directory.

**Note:** If you install Tivoli Storage Productivity Center on a Windows system and have Tivoli Storage Productivity Center authenticate users

against an LDAP-based repository, then the LDAP Tivoli Storage Productivity Center Administrator username must **not** contain a space or blank character in it. See the WebSphere Application Server APAR PK77578.

Ensure that you use the correct case when entering the values for the LDAP TPC Administrator username and LDAP TPC Administrator group. If you use the incorrect case when entering these values, then you will not be able to login to Tivoli Storage Productivity Center for Replication with the user name you expected to use.

#### LDAP TPC Administrator password

Password for the administrator.

# LDAP TPC Administrator group

The group that Tivoli Storage Productivity Center will map to the Tivoli Storage Productivity Center superuser role during installation. This group should already exist in the directory before you start the Tivoli Storage Productivity Center installation and should have the designated LDAP IBM Tivoli Storage Productivity Center Administrator as a member.

#### Note:

Ensure that you use the correct case when entering the values for the LDAP TPC Administrator username and LDAP TPC Administrator group. If you use the incorrect case when entering these values, then you will not be able to login to Tivoli Storage Productivity Center for Replication with the user name you expected to use.

- 14. The Summary Information panel is displayed. Review the information. Click **Install**.
- **15.** You will see the installing panel. When Tivoli Integrated Portal has finished installing, Tivoli Storage Productivity Center will start the Tivoli Storage Productivity Center for Replication installation.
- **16.** Tivoli Storage Productivity Center starts the IBM Tivoli Storage Productivity Center for Replication installation program.
  - a. The Welcome panel is displayed. Click Next.
  - b. The System prerequisites check panel is displayed. The installation wizard checks whether the prerequisites are installed, then confirms whether your operating system is supported and is at the appropriate fix pack or update level. Click **Next**.
  - c. The License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select I accept the terms of the license agreement. Click Next.
  - d. The Directory Name panel is displayed. Accept the default installation directory by clicking **Next**, or specify a different installation directory and click **Next**.
  - e. The IBM Tivoli Storage Productivity Center for Replication Administrator ID and Password panel is displayed. Enter the administrator user ID and password. This ID is usually the operating system administrator user ID. If you use a different ID, create it beforehand and ensure that it has administrator rights.

**Note:** There is a limitation on the number of characters for the user name and password on AIX. At the time this document was written, AIX did not properly validate passwords that are longer than eight characters.

- f. The Default ports panel is displayed. Accept the defaults. Click Next.
- g. The settings panel is displayed. Review the settings and change them if needed by clicking **Back**. Otherwise, click **Install** to begin the installation.
- h. You will see the status panel. Wait for installation to complete.
- i. You will see the summary information panel. Review the information and click **Finish**.
- j. Tivoli Storage Productivity Center for Replication is installed with no license. You must install the Two Site or Three Site Business Continuity (BC) license. For information about installing the license, see "Installing the Two Site or Three Site Business Continuity license" on page 197.
- 17. The successfully installed panel is displayed. Click Finish.
- **18**. After you have installed Tivoli Storage Productivity Center, you can use the Configuration Utility to learn how to configure your system. Follow these steps to go to the Configuration Utility:
  - a. Open the Tivoli Storage Productivity Center GUI.
  - b. Go to Tivoli Storage Productivity Center > Configuration Utility.
- For IBM Tivoli Storage Productivity Center for Replication configuration, see the Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/ v4r1/index.jsp. Click Tivoli Storage Productivity Center for Replication > Configuring.

# Installing the IBM Tivoli Storage Productivity Center GUI

This procedure provides information on how to install the GUI. The GUI is installed where ever you might want to control IBM Tivoli Storage Productivity Center.

IBM Tivoli Storage Productivity Center also supports a Java Web based GUI which gives you the option of not installing the GUI wherever you wish to use IBM Tivoli Storage Productivity Center. For information about the Java Web based GUI, see "Configuring Java Web Start to start the IBM Tivoli Storage Productivity Center GUI" on page 323.

To install the GUI, complete the following steps:

- 1. Start the IBM Tivoli Storage Productivity Center installation program.
- 2. On the Select the type of installation panel, select **Custom installation**.
- 3. Go to the Select one or more components panel, select GUI. Click Next.
- 4. The Summary Information panel is displayed. Review the information. Click **Install**.
- 5. You will see the installing panel. Wait for installation to complete.
- 6. The successfully installed panel is displayed. Click Finish.

# Installing the IBM Tivoli Storage Productivity Center CLI

This procedure provides information on how to install the CLI.

To install the IBM Tivoli Storage Productivity Center CLI, complete the following steps:

- 1. Start the IBM Tivoli Storage Productivity Center installation program.
- 2. On the Select the type of installation panel, select **Custom installation**.

- 3. Go to the Select one or more components panel, select CLI. Click Next.
- 4. The Summary Information panel is displayed. Review the information. Click **Install**.
- 5. You will see the installing panel. Wait for installation to complete.
- 6. The successfully installed panel is displayed. Click Finish.

# Adding an installation license

If you have installed a package on your system, for example, IBM Tivoli Storage Productivity Center Basic Edition, and want to add another package to your system (for example, IBM Tivoli Storage Productivity Center Standard Edition), all you have to do is add the installation license on your system. This topic provides information on how to add the installation license.

To check the type of license you have, look for .SYS2 files in the installation directory:

#### TPCBE0401.SYS2

Indicates you have a Tivoli Storage Productivity Center Basic Edition license.

# TPCSE0401.SYS2

Indicates you have a IBM Tivoli Storage Productivity Center Standard Edition license.

# TPCDATA0401.SYS2

Indicates you have a IBM Tivoli Storage Productivity Center for Data license.

# TPCDISK0401.SYS2

Indicates you have a IBM Tivoli Storage Productivity Center for Disk license.

For example, if you want to add the IBM Tivoli Storage Productivity Center Standard Edition package to your system, complete the following steps:

- 1. If you are adding a license on AIX or Linux, source the db2profile.
- 2. Start the Tivoli Storage Productivity Center installation program from the DVD or image for the license you want to add.
- **3.** The Select a language panel is displayed. Select a language from the list box and click **OK**. This is the language used to install the license.
- The Software License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select I accept the terms of the license agreement. Click Next.
- 5. The Select the type of installation panel is displayed. Select **Installation Licenses**. Click **Next**.
- 6. The Database administrator information panel is displayed. Enter the database administrator user ID and password. Click **Next**.
- 7. The Existing database schema information panel is displayed. Enter the information for where the database is located. Click **Next**.
- 8. The successfully installed panel is displayed. Click Finish.
- 9. Stop the Tivoli Storage Productivity Center GUI.
- 10. Stop the Device server and Data Server.
- 11. Start the Data Server and the Device server.
- 12. Start the Tivoli Storage Productivity Center GUI.

# Installing the agents

This section describes how to install the Data agents and Fabric agents locally or remotely. This section also describes how to install the Storage Resource agents using commands.

**Note:** The Storage Resource agents are not installed using the installation wizard. The Storage Resource agents are deployed using the IBM Tivoli Storage Productivity Center user interface. You cannot have a Data agent and Storage Resource agent on the same system that point to the same Data server. (You can have a Data agent and Storage Resource agent on the same server if they are pointing to different Data servers.) For information about deploying Storage Resource agents, see "Storage Resource agent deployments" on page 295.

The agents are composed of the Common agent and one or more Data agent and Fabric agent. When you uninstall the Data agent and Fabric agent, the last agent to be uninstalled will also uninstall the Common agent.

If you are installing the Data agent and Fabric agent, you must have previously installed the Agent Manager and have registered the Device server and Data Server with the Agent Manager. For information about registering the Device server and Data Server with the Agent Manager, see "Agent Manager Registration" on page 294.

For information about installing the Data agent and Fabric agent in silent mode, see "setup\_agents.iss options file" on page 620.

If you are using IPv6 machines, see "Planning for Internet Protocol Version 6" on page 34.

## Note:

- If the default port is not used for the agent port, then the Tivoli Storage Productivity Center agents need to be installed using custom installation.
- If the default ports were not used when the Tivoli Storage Productivity Center servers were installed, then the agents need to be installed using custom installation.
- Do not install Fabric agents on VMware systems.
- For HACMP: A Data agent must be installed on each node of the cluster and all agents in a cluster must be configured to use the same listening port. To perform a scan on a cluster resource group, you must configure the cluster resource group to have at least one IP address that is accessible from the Tivoli Storage Productivity Center server.

The Fabric agent can be installed on any number of nodes in a cluster.

To install the Data agents and Fabric agents, you must log in as a user with the following authority:

## **On Windows systems**

You must have Administrator authority and the following rights:

- · Act as part of the operating system
- Log on as a service

# On UNIX or Linux systems

You must be logged in as the root user.

# Installing the Storage Resource agents locally

This section describes how to install the Storage Resource agents locally.

You would typically install the Storage Resource agents using the Tivoli Storage Productivity Center GUI. However, if you need to install the Storage Resource agents locally, you can do so with limited support.

For example, if you use this method of installation, you will get a return code of zero for a successful installation and a nonzero return code for an unsuccessful installation. If you have an unsuccessful installation, you will need to go through the log files to determine what the problem was for the failure.

The **-force** option can be used when you have a Storage Resource agent pointing to multiple servers. If one server has installed an agent, and another server wants to install an agent in the same location, the second server can use the **-force** option to install the agent.

If you use this method of installation, make sure that when you specify a directory to install the Storage Resource agent into, do not specify an ending slash mark (\). For example, do not specify C:\agent1\. This will cause the installation to fail.

If you run the agent as a non-daemon service (on-demand service), you must make sure that at least one protocol is valid for a successful connection from the server to the agent. See Table 23 for the required parameters for each protocol.

Protocol	Description
SSH	Requires the user ID and password or user ID, certificate, and passphrase.
Windows (SMB)	Requires the user ID and password.
REXEC	Requires user ID and password.
RSH	Requires the user ID.

Table 23. Parameters required for each protocol

The disk 1 or disk2 image contains the installation images for the Storage Resource agents. The images are located in the following directory:

<CD\_installation\_image\_location>/data/sra/<operating\_system>

See Table 24 for the Storage Resource agent installation images.

Table 24. Storage Resource agent installation images

Operating system	Operating system name
AIX	aix_power
Linux x86	linux_ix86
Linux Power	linux_power
Linux s390	linux_s390
Windows	windows

To install the Storage Resource agents locally, follow these steps:

 Go to the installation image location: cd <CD installation image location> 2. Run the following command:

```
bin/Agent -install [-force]
-serverPort <server_secure_port>
-serverIP <server_IP_address>
-installLoc <Agent_install_location>
```

Parameters when agent is run as a daemon service:

-agentPort <agent\_port>
-commtype daemon

Parameters when agent is run as a non-daemon service: See Table 23 on page 242 to determine which parameter is required for each protocol:

```
-userID <user_ID>
-password <paddword>
-certFile <certificate_file>
-passphrase <passphrase>
```

Optional parameter:

-debug MAX

# Where:

- -force This forces the agent to be installed. There are two different situations in which this parameter should be specified:
  - If an earlier installation failed and there is residue on the system which causes further installations to fail. You need to make sure that all the parameters provided are valid, such as the installation location, port, and so forth.
  - If the agent is already installed from one server and you now need to install the agent pointing to another server.

When you specify this parameter, various checks will be overwritten and the port is verified after the agent service stops.

#### -serverPort <server\_secure\_port>

The default port for the Data server is 9549.

#### -serverIP <server\_IP\_address>

The IP address of the server. If the server can be reached through multiple IP addresses, then multiple IP addresses can be specified with IP addresses separated with a comma.

#### -installLoc <Agent\_install\_location>

Location where the agent will be installed.

#### -debug MAX

This is an optional parameter for debugging purposes.

Specify these parameters when the agent is run as a daemon service:

#### -agentPort <agent\_port>

If the agent is run as a daemon service, then the agent port must be specified.

#### -commtype daemon

If the agent is run as a daemon service, then this parameter must be specified.

Specify these parameters when the agent is run as a non-daemon service (on-demand service):

### -userID <user\_ID>

The user ID defined on the agent system. This is the user ID that the server can use to connect to the agent system.

#### -password <password>

Password for the user ID.

# -certFile <certificate\_file>

The certificate used for SSH communication between the server and agent. This certificate needs to be stored on the server system.

#### -passphrase <passphrase>

The passphrase defined for the certificate used in SSH communication.

If the installation fails, see the return codes in the Information Center. Search for **Return codes used by Storage Resource agent**.

# Using typical installation for the agents

This section describes how to install the IBM Tivoli Storage Productivity Center agents using typical mode.

To install the Tivoli Storage Productivity Center agents using typical mode, follow these steps:

- 1. Start the Tivoli Storage Productivity Center installation program. For information about starting the installation program, see "Starting the installation program" on page 168.
- 2. The Select a language panel is displayed. Select a language from the list box and click **OK**. This is the language that is used for installing this product.
- 3. The Software License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select I accept the terms of the license agreement. Click Next.
- 4. The select the type of installation panel is displayed. On the Select the type of installation you want to run panel, select **Typical installation** and **Agents**. Click **Next**.

	Select the type of installa	tion you want to run		
	Typical installation	non journant to run		
IBM.	This will install the Data and CLI. A new databas database during install	a server and Device se se will be created, and ation. The database a	erver, Data agent and Fa the schema will be cre nd schema will be reus	abric agent, GUI ated on the sed for upgrade.
	Servers	Clients		
	Agents	🗖 Register w	ith the agent manager	
	📉 👩 Custom installation	100		
	Computer. You will have computer.	a server and Device se on this computer. Rer loose any server, ager a choice to create the	river, Jata agent and Fa note agents are installe t, or client to be installe database and schema	aon: agent, 601 ad on other d on this a on this
MICH	C:\Program Files\IBM\T	TPC	TPC Installation	Location

Figure 71. Select the type of installation panel

5. The User ID and password panel is displayed. Enter the user ID and password that has administrator and database administrator authority.

**Note:** If you have a server on machine A (the server must be registered with the Agent Manager) and you install the agent on machine B, then you must provide the following information:

- a. A user ID for machine B (on which you are installing the agent). A user ID will be created if it does not exist.
- b. The password for this user ID must be the same password as the host authentication password on the Tivoli Storage Productivity Center server machine (machine A).

Enter the server name, server port, and agent port or accept the defaults. Click **Next**.

Note: The default server port is 9549.

**6**. The Agent Manager information panel is displayed. Complete the following information:

Hostname or IP address

Fully qualified host name or IP address of the Agent Manager server.

# Port (Secured)

Port number of the Agent Manager server. The default is 9511.

# Port (Public)

The public communication port. The default is 9513.

Enter the Common agent registration password as specified on the Agent Manager.

# Password

This is the Common agent registration password used by the

Common agent to register with the Agent Manager. This was specified when you installed the Agent Manager.

Click Next.

- 7. The Summary Information panel is displayed. Review the information. Click **Install**.
- 8. You will see the installing panel. Wait for installation to complete.
- 9. The Successfully installed panel is displayed. Click Finish.

# Using custom installation for the agents

This section describes how to install the IBM Tivoli Storage Productivity Center agents using custom installation.

# Installing the agents locally:

This topic provides information on how to install the agents locally on a server to be managed.

To install the Data agent and Fabric agent, complete the following steps:

- 1. Start the IBM Tivoli Storage Productivity Center installation program. For information about starting the installation program, see "Starting the installation program" on page 168.
- 2. The Select a language panel is displayed. Select a language and click OK.
- **3**. The Software License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select **I accept the terms of the license agreement**. Click **Next**.
- 4. The Select the type of installation panel is displayed. Select **Custom installation**. Click **Next**.
- 5. The select one or more components to install panel is displayed. Select **Data Agent, Fabric Agent, and Register with the Agent Manager**. Click **Next**.

🕲 IBM Tivoli Storage Pro	🕲 IBM Tivoli Storage Productivity Center - Installer 📃 🔲				
	Select one or more components to insta This program will install or upgrade var example, if version number 3.1.0.39 is of that the version of the component is aim installation, all installed components w software. You can choose to install add	II on the local or remote computer. ious components displayed below. For displayed next to the component, this means, eady installed on this computer. In this ill be upgraded to the current version of itional components which are not installed.			
	<ul> <li>Create database Schema</li> <li>Data Server</li> <li>GUI</li> <li>Data Agent</li> <li>Remote Data Agent</li> <li>Register with the agent manager</li> <li>Register Launch Information With Or</li> </ul>	Device Server  CLI  Fabric Agent  Remote Fabric Agent  ther Applications			
< Back Next > Cancel					

Figure 72. Select one or more components to install panel

6. The Data server, Device server, Data agent, and Agent Information panel is displayed.

🕲 IBM Tivoli Storage Pro	ductivity Center - Instal	ler			
	Data server, Device serv	er, Data agent, and Agent I	nformation		
IBM.	Enter the server name communicate with the	and port that the Data agen server.	t and Fabric agent, and	GUI will use to	
	Data server name	mdm-b26-w2k3.bea	Data server port	9549	
	Device server name	mdm-b26-w2k3.bea	Device server port	9550	
	Enter an OS user group administrators group.	) whose members will be 1	FPC administrators in th	ne	
	TPC superuser	Administrators	Secu <u>r</u> ity role:	S	
	Enter a password that t	he Fabric agents will use t	o communicate with the	Device server.	
	Host authentication pa	ssword			
1 1115	Enter a password that	will be used to create the D	ata Server Account.		
1/1/1	Data Server Account Pa	assword			
	WAS admin ID	Passv	vord		
2 N LOHA			NAS discovery		
	Data agent <u>o</u> ptions				
	< <u>B</u> a	ck <u>N</u> e	xt >	<u>C</u> ancel	

Figure 73. Data server, Device server, Data agent, and Agent Information panel

Enter the following information:

#### **Data Server Name**

Enter the fully qualified host name of the Data Server.

# **Data Server Port**

Enter the Data Server port. The default is 9549.

#### **Device Server Name**

Enter the fully-qualified host name of the Device server.

#### **Device Server Port**

Enter the Device server port. The default is 9550.

#### **TPC Superuser**

Enter an operating system group name to associate with the TPC Superuser role. This group must exist in your operating system before you install Tivoli Storage Productivity Center. Membership in this group provides full access to the Tivoli Storage Productivity Center product. You can assign a user ID to this group on your operating system and start the Tivoli Storage Productivity Center GUI using this user ID.

**Note:** If you select LDAP authentication later in the Tivoli Storage Productivity Center installation, then the value you enter for LDAP TPC Administrator group overrides the value you entered here for the TPC Superuser.

### Host Authentication Password

This is the password used for the Fabric agents to communicate with the Device server.

#### Data Server Account Password

For Windows only. You supply this password. When you supply this password, the Tivoli Storage Productivity Center installation program creates a user ID and the password you supplied to create the Data server account on Windows. This user ID and password is used by the Data server service.

The display name for the Data Server is:

IBM Tivoli Storage Productivity Center - Data Server

#### WAS admin ID and Password

This is the user ID and password required by the Device server to communicate with embedded WebSphere. This is only used at installation time.

**Note:** If you select LDAP authentication later in the Tivoli Storage Productivity Center installation, then the values you enter for LDAP TPC Administrator username and password override the value you entered here for WAS Admin ID and password.

# Click Next.

## If you click the Security roles button:

The Advanced security roles mapping panel is displayed. Enter the operating system group for each Tivoli Storage Productivity Center role you want to make an association with. The operating group must exist before you can associate a Tivoli Storage Productivity Center role with a group. Click **OK**. Click **Next**.

**Note:** You do not have to assign security roles at installation time. You can assign these roles after you have installed Tivoli Storage Productivity Center.

If you select LDAP authentication later in the Tivoli Storage Productivity Center installation, then the values you enter here for Security Roles Mapping will be deleted and you will have to assign roles to individuals after the installation is complete (use the **Role-to-Group Mapping** node).

# If you click the NAS discovery button:

The NAS discovery information panel is displayed. Enter the NAS filer login default user name and password. If you want to enter the SNMP communities to be used for NAS discovery, click **Add**, enter the community name, then click **OK**. Click **Next** on the Data server, the Device server, Data agent, and Agent information panel.

If you click **Data Agent Options**, you will be able to select whether or not you want the agent to perform an initial scan when first brought up. You can also select whether or not the agent can run scripts sent by the server. Make your selections and click **OK**.



Figure 74. Data Agent Options panel

The options are:

## Agent should perform a scan when first installed

Clear the check box for this option if you do not want Data Manager to perform an initial scan of your storage upon installation. This option is checked by default and gathers default statistics.

#### Agent may run scripts sent by server

Leave this option checked if you want to store scripts in the server's \scripts directory that will run on all agents. When a script needs to be run on a particular agent, the server will access that script from its local \scripts directory and send it to the appropriate agent.

If you clear the check box for this option, the agents will ignore scripts sent by the server. You will have to store a copy of every script in every agent's \scripts directory.

The default \scripts directory for an agent behaves as described below:

If a script with the same name exists on both the server and the agent, the script stored on the agent will take precedence. This is useful if you want to run a special version of a script on one agent that is different from the version you are running on all the other agents.

The following example demonstrates the advantage of storing scripts at the server level. To monitor a computer's file system free space, you can store a script on the server that runs when any computer on the network meets a specified low file system free space threshold condition. But you could also store a special script on one computer that defined a different threshold for that computer. This script would take precedence over the script stored on the server.

The default directory for the \scripts directory is as follows: C:\Program Files\IBM\TPC\data\scripts (for Windows) /opt/IBM/TPC/data/scripts (for UNIX or Linux)

7. The Agent Manager information panel is displayed.

🕲 IBM Tivoli Storage Pro	ductivity Center - Installer		_ 🗆 🗙		
	Agent manager information				
IBM.	Enter the information that the product will use to register its Data server, Device server, Data agent, or Fabric agent with the agent manager.				
	Hostname or IP address	mdm-b26-w2k3.beaverton.ibm.com			
	Port (Secured)	9511			
	Port (Public)	9513			
	Enter the Data server and Device server registration information as specified on the agent manager.				
	User ID	manager			
	Password				
1 have	Enter the common agent registration password as specified on the agent manager.				
11 11 -	Password				
line .					
	< <u>B</u> ack	Next > Cancel			

Figure 75. Agent Manager information panel

Enter the following information:

# Hostname or IP Address

Enter the fully qualified host name of the Agent Manager.

#### Port (Secured)

The port number of the Agent Manager. The default port is 9511.

# **Port (Public)**

This is the public port. The default port is 9513.

## Password

This is the password used by the Common agent to register with the Agent Manager. The default value is **changeMe**. Use the password specified when you installed the Agent Manager. Click **Next**.

8. The Common agent selection panel is displayed. You can install a new Common agent or use an existing Common agent. Select Install new Common agent at the location listed below for a new Common agent. Enter a directory or accept the default directory where the Common agent will be installed. Enter the port that the Data agent and Fabric agent will use to listen and communicate with the Common agent. The default port is 9510. You can also specify to download the truststore certificate from the Agent Manager. Click Next.

IBM Tivoli Storage Pr	oductivity Center - In	staller			
	Common agent sele	ection			
IBM.	Select the installation agent already insta	on of a new commo lled on your comput common agent at th	n agent or choose er for the Data age e location listed b	an existing commo ent and Fabric ager elow	on It
	C:\Program File	s\IBM\TPC\ca		В	rowse
	Agent port	9510			
			Windows service	info	T.
	Port	Version	Location	Data agent	Fabric agent
(I)					
		Back	Next >	c	ancel

Figure 76. Common agent Selection panel

If you have an existing Common agent already installed, select **Select existing Common agent from the list below**. The table will list the common agents you have installed. Select a Common agent and click **Next**.

9. If you want to enter Windows service information, click **Windows Service Info**. The Common agent Service Information panel is displayed. This information is optional. You can enter a Common agent service name, user ID and password that the installation program will use to create a Windows service for the Common agent. Enter the information and click **OK**. Click **Next** on the Common agent information panel.

**Note:** For Windows, if you are using domains, you must enter the domain name for user ID in the format <domain>\<account>.

🕲 IBM Tivoli Storage Pro	ductivity Center - Installer	_ 🗆 🗙			
	Common agent service information (Optional)				
IBM.	Enter the information to create the Windows service for the common agent.				
	Common agent service name				
	Common agent service logon account information				
	User ID				
	Password				
	<u>O</u> K <u>C</u> ancel				

Figure 77. Common agent Service Information panel

- 10. The Summary Information panel is displayed. Review the information. Click **Install**.
- 11. You will see the installing panel. Wait for installation to complete.
- 12. The successfully installed panel is displayed. Click Finish.

## Installing the agents remotely (from the server computer):

This section describes how to install the Data agent and Fabric agent remotely from the IBM Tivoli Storage Productivity Center server. Installing agents remotely from a non-Tivoli Storage Productivity Center server is not supported.

## Preparing to install the agents remotely:

This section provides information on how to prepare your system before installing the agents remotely.

You will need to know the following information:

- To remotely install the Data agents and Fabric agents, you must run the installation program on the computer that has the Data server and Device server.
- You must know the name or IP address of the computers on which you want to install the agent.

Before you remotely install an agent, keep in mind the following items:

- You must install the Data agent before installing the Fabric agent to a remote computer. The Common agent is installed with the Data agent, and the Fabric agent requires that the Common agent be installed and running on the target computer. Install the Data agent first. Then install the Fabric agent.
- You must ensure that the computers on which you want to install the agent are available.

• When installing to a foreign Windows domain, the domain from which you are installing has to trust the foreign domains, and your login must be an administrator on the local computer (the computer from which you are installing) and a domain administrator on the foreign domains. Setting up the trust between domains is a complex task that should be done by your administrator before remotely installing Data agents.

**Note:** If you do not have administrator rights to the foreign domains, the installation will be able to find the other domains but might *not* be able to list the computers for that domain.

- The IBM Tivoli Storage Productivity Center server must be registered with the Agent Manager.
- You must supply a user ID and password that has administrative privileges on the target computer. The user ID must be a local administrative account on the target computer (not a domain administrative account).

To prepare for installing the Data agents remotely, complete the following steps:

- 1. If you are installing a Data agent remotely on a Linux system, you must set the /etc/ssh/sshd\_config file parameter **PasswordAuthentication** to **yes**. To set the parameter, follow these steps:
  - a. Go to the following directory: /etc/ssh.
  - b. Use a text editor such as **vi** to edit the /etc/ssh/sshd\_config file. Change the **PasswordAuthentication** parameter to **yes**.
  - c. Stop the daemon by running the following command: /etc/init.d/sshd stop.
  - d. Start the daemon by running the following command: /etc/init.d/sshd start.
- If you are installing a Data agent remotely on a Solaris 10 system, you must set the following parameters in file/etc/ssh/sshd\_config:

PasswordAuthentication yes PermitRootLogin yes

To stop **sshd**, you have to kill it; there is no stop command. To start the **sshd**, enter the following:

/usr/lib/ssh/sshd

# Installing the Data agent and Fabric agent remotely:

This topic describes how to install the Data agent and Fabric agent remotely.

Steps 1-10 apply to installing the Common agent and Data agent. Steps 11-16 apply to installing the Fabric agent.

To install the Data agent and Fabric agent remotely, complete the following steps:

- 1. Start the IBM Tivoli Storage Productivity Center installation program. Run **setup.exe** (for Windows) or **setup.sh** (for UNIX) to start the installation program.
- 2. The Select a language panel is displayed. Select a language and click OK.
- The Software License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select I accept the terms of the license agreement. Click Next.
- 4. The Select the type of installation you want to run panel is displayed. **Custom installation** is already selected. Click **Next**.
- 5. The Select one or more components to install panel is displayed. Select both **Remote Data Agent** and **Remote Fabric Agent**. Click **Next**.

- 6. The Data server, the Device server, Data agent and Agent Information panel is displayed. If the Data Server is installed on the local computer, then Click **Next**. Otherwise, enter the Data server name and Data server port fields. Click **Next**.
- 7. The Select the Remote Agents to Install panel is displayed. Use this window to:
  - Specify Windows computers on which to install agents (when installing from a Windows computer, only). These Windows computers can be in the current domain or in another domain within your environment.
  - Specify non-Windows computers on which to install agents. You can add multiple computers at the same time.
  - View a list of the computers on which you want to install agents.
  - Remove a computer from the list of target computers.

The following information is provided:

# Add Agents from MS Directory (button)

This applies to Windows domains.

If you are installing from and to Windows computers, click this button to specify Windows computers on which you want to install the agents.

- You can select computers from the current domain or from foreign domains.
- The remote installation is more likely to succeed if the remote domain to which you are pushing trusts the domain of the installation computer. Otherwise, you will have to log in as an administrator on the remote domain.

When you click on this button, the Add Agents from MS Directory panel is displayed. Use this panel to specify Windows computers on which to install the agents. When you first access this window, the installation program will find and list all the computers within your current domain. Complete the following fields on this panel:

## **Remote Agent Machines**

This list box provides a complete listing of the computers detected for the current domain that do not already have a Data agent installed.

Use the columns on this window to sort and filter the computers that appear in this list:

- To sort the names in a column, place the mouse over a column name and click one of the arrows that appears.
- To filter the names that appear in a column, click the box below the column name and enter a filter.

The filter supports UNIX shell wild carding or shell globbing. The most common wild card characters you can use are:

- \* includes any number of characters, including 0
- ? includes exactly one character
- \*[a-n] includes any number of characters, plus any one character ending through a - n.
- **Select** Click the check box next to the computer on which you want to install an agent.

#### Host Name

Displays the names of the computers detected in the current domain.

## Domain

Displays the domain of the computers listed on the window. You can only display the computers from one domain at a time. To list the computers from another domain, click the filter box below the column name and enter the name of another domain.

**Note:** If you do not have administrator rights to the foreign domains, the installation will be able to find the other domains but may **not** be able to enumerate the computers for that domain.

#### Virtual Node

Indicates whether the computer is a virtual node.

**OK** Click this button to add the computers you entered to the **Computers Targeted for a Remote Install** list on the Remote Agents to Install window.

A computer you selected for a target install will not appear in the **Computers Targeted for a Remote Install** list after you click **OK** if:

- The installation program cannot establish communication with a target computer.
- The current computer does not have the proper authority to install on the remote computer.
- The computer you entered has already been targeted for an installation.

## Manually Enter Agents (button)

Click this button to manually specify Windows and non-Windows (UNIX, Linux) computers on which you want to install agents. You can specify multiple computers on which to install agents at the same time. Keep in mind the following items:

- The current computer must be able to resolve the IP address of a remote computer and be able to communicate with that computer.
- The user ID and password you enter must have administrative authority on the remote computer.
- You can add multiple computers in a single installation if they share the same user ID and password. If computers do not share the same user ID and password, you must add them individually.

When you click this button, the Manually Enter Agents panel is displayed. Complete the following fields on this panel:

#### **Remote Agent Machines**

Enter the network names or IP addresses of the computers to which you want to install agents. Type one name per line.

When adding multiple computers, separate each computer name or IP address with a carriage return. For example:

9.45.179.8 9.23.180.5 storagebox1 storagebox2 storagebox3 9.41.20.144

You can copy and paste one computer per line. To copy and paste one computer per line:

- a. Highlight the computer you want to copy and press Ctrl+C.
- b. Click the cursor on a row in the Manually Enter Agents window.
- c. Press Ctrl+V.

# **Remove Selected Entries**

Click this button to remove the highlighted computers in the **Remote Agent Machines** list box.

## User and Password

Use the fields in this section to specify the user and password for the hosts that you want to manually add. This is recommended when you want to add multiple hosts at the same time that share the same user ID and password. The user ID and password that you enter must have administrative privileges on the target computers.

**OK** Click this button to add the computers you entered to the **Computers Targeted for a Remote Install** list on the "Select the remote agents to install" window.

A computer you selected for a target install will not appear in the **Computers Targeted for a Remote Install** list after you click **OK** if:

- The installation program cannot establish communication with a target computer.
- The current computer does not have proper authority to install on the remote computer.
- The default user ID and password is incorrect.
- The computer you entered has already been targeted for an installation.

The "Select the remote agent to install" window has these fields:

# Add Agents from MS Directory (button)

Use this button to add more agents to list of remote agents to install.

# Manually Enter Agents (button)

Use this button to add more agents to list of remote agents to install.

# Computers Targeted for a Remote Agent Install (table of computers for remote agent install)

This list box provides a complete listing of the computers on which you selected to install agents. Computers will appear in this list if:

- The computer was selected on either the Add Agents from MS Directory or Manually Enter Agents windows.
- The current computer can communicate with the listed target computer.
- The current computer has the proper authority to install agents on the listed target computer.

The following columns appear in the list box.

- Host Name the network name of a target computer.
- IP Address the IP address of a target computer

Right-click on a column name (in the header line) to filter or sort the listed computers.

**Note:** If you filter the names in the computer list, the computers you selected for an agent installation that do not match the filter criteria will not appear in the list. Note that agents will still be installed to the unlisted computers whose names do not match the filter.

## Remove (button)

Click this button to remove the highlighted computers from the list of computers on which you want to install an agent.

### Click Next.

- **8**. The Windows Service Account panel is displayed (for Windows only, not required for UNIX or Linux). You have two options:
  - Create a local account for the agent service (creates a new service account under which the server will run).
  - Use this account for the agent service (provide a user name and password to use an existing service account).

#### Click Next.

**9**. The agent status panel is displayed. The Data Manager will run a mini-probe on all the computers you selected to determine what necessary applications are installed and if the agent is already installed on any computer. Make sure that the server can ping the agent and the agent can ping the server. These are the column headings:

# OS Type

Displays the operating system of the target computer.

## Computer

Displays a list of computers where the agent will be installed.

**Status** Displays the current status of the agent install on the remote computer.

# Directory

Displays the directory where the agent will be installed. If an agent is already installed on a computer, you will not be able to edit this field. If you can edit the field, this means that an agent has not yet been installed, and you can edit the directory where the agent will be installed. If any Common agent exists, the path cannot be changed. **Port** Displays the port number on which the agent is listening. You can change the listener port for a remote probe on this panel. So if you have a firewall, you can select the port that the program uses to communicate back to the installation program.

# Space Required

Displays the space required to install the agent.

# Space Available

Displays the available space on the computer.

10. Click Install. The agents will be installed on the specified computers. This window is automatically updated as the agent is installed on the target computers. The Status column will display the installation status (for example, "Copying software", "Initializing Install", and so forth) for each computer on which an agent is being installed.

**Note:** The installation process automatically creates a Service account on a Windows computer where a NetWare Client is installed. Tivoli Storage Productivity Center will use this new account to log into the NetWare server and avoid security conflicts with other services using NetWare. Tivoli Storage Productivity Center will not create a Service account on a computer that is a domain controller.

A confirmation window is displayed with the message "Installation completed." Click **OK**. A window appears that lists the computers where an agent has been installed.

**Note:** You can double-click on a computer name (in the heading) to view the installation log for that computer.

The messages generated during the installation are stored in files located in:

- C:\Program Files\IBM\TPC\ca\subagents\TPC\Data\log\ directory (this is the default) on the target Window computers.
- /opt/IBM/TPC/ca/subagents/TPC/Data/log/ directory (this is the default) on the target UNIX or Linux computers.

The name of the installation log file will be dataAgentInstall.log. Click **Done**.

11. A pop-up window opens with the following message:

Server validation and retrieval of agent list can take several minutes.

Click OK.

- 12. The Remote Fabric agent information panel is displayed. This list is a list of common agents that are known to the Agent Manager. You can select one or more remote common agents to deploy the Fabric agents under the **Deploy** column heading. Make your selection and click **Next**.
- **13.** A confirmation panel is displayed listing where the Fabric agent will be installed. Click **Next**.
- 14. The status panel for deploying the Fabric agent is displayed. Wait for the deployment to complete.
- 15. The deployment complete panel is displayed. Click Next.
- 16. The deployment of the Fabric agent has now completed.

#### Installing the Fabric agents remotely:

This topic describes how to install the Fabric agents remotely.

If you are installing the Fabric agents remotely, note the following requirements:

- The Agent Manager must be running.
- The Device server must be installed on the computer you are running the installation program from, and must be registered with the Agent Manager.
- A Common agent must be running on the computer where you want to install the Fabric agent. This would be the case if you had already installed the Data agent on this computer.

To install the Fabric agents remotely, complete the following steps:

- 1. Start the IBM Tivoli Storage Productivity Center installation program.
- 2. The Select a language panel is displayed. Select a language and click OK.
- **3**. The Software License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select **I accept the terms of the license agreement**. Click **Next**.
- 4. Go to Select the type of installation you want to run panel. Select **Custom installation**. Click **Next**.
- 5. The Select one or more components to install panel is displayed. Select **Remote Fabric Agent**. Click **Next**.
- 6. The List of Remote Hosts panel is displayed. The remote hosts listed have common agents installed on them, and are running under the operating systems that support the Fabric agent. You can select some or all of the remote hosts that you want to deploy your agents to. Make your selection and click **Next**.
- 7. The Confirmation panel is displayed showing the list of remote hosts you have selected. Read the information and click **Next**.
- 8. A Progress panel is displayed. When the agents have been deployed, click **Next** to continue.
- **9**. The Summary Information panel is displayed which shows a list of successful and failed deployments. Click **Finish** to exit the installation wizard.
- **10.** Make sure that the server can ping the agent and the agent can ping the server.

# Installing the agents on Virtual I/O Server

Install Data agents, Fabric agents, and Storage Resource agents on Virtual I/O Servers to collect information about those servers. You can view the information gathered by agents in the Reporting sections of the IBM Tivoli Storage Productivity Center user interface.

## Note:

- The agent software is part of the Virtual I/O Server software package V1.5.2. You cannot install the software on a lower version of the Virtual I/O Server.
- This section applies to installing the Data agents and Fabric agents only. For information about installing the Storage Resource agents, see "Storage Resource agent deployments" on page 295.

Use the **cfgsvc** command to install the Data agent and Fabric agent. You must log into the Virtual I/O Server as the **padmin** user ID when running this command. For information about deploying the Storage Resource agents, see

The **cfgsvc** command installs and configures the agent specified. After installing and configuring the agent, you can start and stop the agent using the **startsvc** and **stopsvc** commands.

If you use the default parameters to install the agents, this command will install both the Data agent and Fabric agent. The parameters for the **cfgsvc** command are:

►►—cfgsvc—TPC— -attr=—attribute value— -ls—

**TPC** Required parameter. This installs and configures the Tivoli Storage Productivity Center agents.

#### -attr=attribute\_value

Identifies an attribute value associated with the configuration of an agent. The attribute values are:

- **S** Required attribute. Specify the Tivoli Storage Productivity Center server host name or IP address to which this agent is associated.
- A Required attribute. Specify the Agent Manager host name or IP address.

#### devAuth

Required attribute. The devAuth password is the password that the Fabric agent authenticates with the Device server.

**caPass** Required attribute. Specify the Common agent password. The default Common agent password is changeMe if you have Agent Manager 1.2 installed. For Agent Manager 1.3.2, a default password is no longer provided.

#### amRegPort

Optional attribute. Specify the Agent Manager registration port. The default value is 9511.

#### amPubPort

Optional attribute. Specify the Agent Manager public port. The default value is 9513.

#### dataPort

Optional attribute. Specify the Tivoli Storage Productivity Center Data server port. The default value is 9549.

## devPort

Optional attribute. Specify the Tivoli Storage Productivity Center Device server port. The default value is 9550.

#### newCA

Optional attribute. The value can be **true** or **false**. The default value is **true**.

**oldCA** Optional attribute. The value can be **true** or **false**. The default value is **false**.

#### daScan

Optional attribute. This runs a Data agent scan after installation. The value can be **true** or **fals**e. The default value is **true**.

#### daScript

Optional attribute. This runs the Data agent script after installation. The value can be **true** or **false**. The default value is **true**.

#### daInstall

Optional attribute. This installs the Data agent. The default value can be **true** or **false**. The default value is **true**.
#### faInstall

Optional attribute. This installs the Fabric agent. The default value can be **true** or **false**. The default value is **true**.

**-ls** Lists all the attributes that can be modified for a particular agent configuration.

To install and configure Tivoli Storage Productivity Center agents on a Virtual I/O Server, follow these steps:

- 1. Log in to the Virtual I/O Server using the **padmin** user ID. Upon logging into the Virtual I/O Server, you are placed into a restricted Korn shell.
- 2. Run the **cfgsvc** command with your specified attributes. For example:

cfgsvc TPC -attr S=<TPC\_server\_hostname> A=<Agent\_Manager\_hostname> devAuth=<host\_authentication\_password> caPass=<common\_agent\_password>

The installation wizard appears.

**3**. Type the number next to the language that you want to use for the installation wizard and enter **0**. The license agreement panel appears.

```
Initializing InstallShield Wizard.....
Launching InstallShield Wizard.....
Select a language to be used for this wizard.
[] 1 - Czech
[x] 2 - English
[] 3 - French
[] 4 - German
[] 5 - Hungarian
[]6 - Italian
[] 7 - Japanese
[] 8 - Korean
[]9 - Polish
[] 10 - Portuguese (Brazil)
[] 11 - Russian
[] 12 - Simplified Chinese
[] 13 - Spanish
[] 14 - Traditional Chinese
To select an item enter its number, or 0 when you are finished: [0]
```

4. Read the license agreement panel. At the end of the license agreement panel, you will see the following:

```
Please choose from the following options:
[ ] 1 - I accept the terms of the license agreement.
[ ] 2 - I do not accept the terms of the license agreement.
To select an item enter its number, or 0 when you are finished: [0]
```

Type **1** to accept the terms of the license agreement. Type **2** to reject the terms of the license agreement and exit the installation wizard without installing any agents. If you accepted the license agreement, the agents are installed on the Virtual I/O Server according to the attributes you specified in the **cfgsvc** command.

- 5. Check the log files to see if the installation has shown any problems. See "Default log file locations" on page 501.
- 6. Start the agents by running the **startsvc** command.
- 7. Start the Tivoli Storage Productivity Center user interface and run a discovery for the agents on the Virtual I/O Server.

- **8**. Define and run probes, scans, and ping jobs to gather information about the Virtual I/O Server.
- **9**. View the storage information gathered by the monitoring jobs through the topology Viewer and reports that you can generate through Fabric Manager and Data Manager.

#### Example

To install and configure the agents, enter the following command: cfgsvc TPC -attr S=<TPC\_server\_hostname> A=<Agent\_Manager\_hostname> devAuth=<host\_authentication\_password> caPass=<common\_agent\_password>

To list all the attributes associated with an agent configuration, enter the following command:

cfgsvc TPC -ls

# Installing IBM Tivoli Storage Productivity Center in silent mode

IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication do not support silent, unattended installations except for the Data agents and Fabric agents. By modifying the appropriate parameters in the options file, you can run the script to install or uninstall the Data agents and Fabric agents.

#### Note:

- Doing a remote deployment of the agent in silent mode is not supported. Also, you cannot use silent mode installation to install the Language Pack.
- Agent Manager and agents only use IPv4 communication. See "Planning for Internet Protocol Version 6" on page 34.

To install the Data agent or Fabric agent in silent mode, complete the following steps:

- 1. Review the options file and make the appropriate changes in the file. See "setup\_agents.iss options file" on page 620. Save the file.
- 2. Run the following command:
  - For Windows: setup.exe -silent -options "<directory>\setup\_agents.iss" -is:log <log\_file>
  - For Linux or UNIX: ./setup.sh -silent -options "<directory>/setup\_agents.iss" -is:log <log\_file>

#### <directory>

This is the directory where you placed the **setup\_agents.iss** file.

<log\_file>

This is the name you provide for the InstallShield log file. This can be a full directory path name or just the name of the log file.

**Note:** You will not receive any success or error messages in the command prompt window while this command is running. When the command is finished running, it will return you to a command prompt window. To see if the Tivoli Storage Productivity Center installation was successful or not, check the log files.

**3**. Check the log files so you will know if the Tivoli Storage Productivity Center silent installation succeeded or failed.

Component	Log file
Data agent	<install_dir>\log\subagents\TPC\Data\install\ dataAgentInstall.log <install_dir>\log\subagents\TPC\Data\install\ dataAgentInstallIS.log</install_dir></install_dir>
Fabric agent	<install_dir>\log\subagents\TPC\Fabric\install\ fabricAgentInstallIS.log</install_dir>
InstallShield	When you specify the <b>-is:log</b> < <b>log_file</b> > parameter, you can specify a full directory path name or just the log file name. If you specify a full directory path name, the path name indicates the location of the log file. If you specify just the log file name, the log file will be in the directory where you issues the InstallShield command ( <b>setup.exe</b> or <b>setup.sh</b> ).

# Installing the Language Pack

The Language Pack allows you to see messages, online help, and text in a different language other than English in IBM Tivoli Storage Productivity Center.

Before you install the Language Pack, you must first have successfully installed Tivoli Storage Productivity Center. You can install the Language Pack for the components in the table below.

Data Server	Fabric agent
the Device server	GUI
Data agent	CLI

You can install the Language Pack for the languages in the table below.

Czech	Hungarian	Russian
German	Italian	Brazilian Portuguese
Spanish	Japanese	Simplified Chinese
French	Korean	Traditional Chinese

**Note:** When installing Tivoli Storage Productivity Center on a system with the Turkish locale on Windows 2003, you must have the correct regional and language options set for the agent installation to succeed.

This restriction applies only to the agent and Agent Manager communication; not for the Tivoli Storage Productivity Center servers. To install Tivoli Storage Productivity Center for a Turkish locale, follow these steps:

- 1. Ensure that the Agent Manager is installed on a machine where the language and regional settings are **not** Turkish. (The language could be the default language of English or any other language but not Turkish.)
- 2. Ensure that the agent machine's language and regional settings are not Turkish.
- 3. Install the Tivoli Storage Productivity Center agent.
- 4. Change the locale of the Agent Manager and agent machines to Turkish (Language and Regional settings).

To set the regional and language options on Windows, follow these steps:

a. Go to **Start > Settings > Control Panel**.

- b. Click Regional and Language Options.
- c. Select the Turkish language in all three tabs:
  - Regional Options
  - Languages
  - Advanced also check the box for "Default user account settings"

Click Apply.

5. Do not enter NLV characters in the Tivoli Storage Productivity Center GUI.

You must have administrator authority on Windows or root authority on UNIX or Linux to install the Language Pack.

To install the Language Pack, complete the following steps:

- 1. Log onto the system with administrator authority on Windows or root authority on UNIX or Linux.
- Insert the Language Pack CD or go to the directory where you have downloaded the Language Pack. Run the following program: TPCLP.exe (for Windows) ./setup.sh (for UNIX or Linux)
- **3**. The Select a Language panel is displayed. Select a language from the list box and click **OK**.
- 4. The Welcome panel is displayed. Click Next.
- 5. The Select one or more languages panel is displayed. Select one or more languages and one or more Tivoli Storage Productivity Center components to install. Click **Next**.
- 6. The Summary panel is displayed indicating the choices you have made on the previous panel. Review the information. Click **Install**.
- 7. You will see the Installing status panel displayed. Wait for installation to complete.
- 8. The Installation successful panel is displayed. Click Finish.

For the changes to take effect, you must stop and restart the Device server, Data Server, Data agent, Fabric agent, and GUI (or whatever component you installed the Language Pack for). For information about stopping and restarting the components, see "Starting and stopping the IBM Tivoli Storage Productivity Center services" on page 464.

To install the Storage Resource agents in a different language, see "Data/Storage Resource Agent Upgrades" on page 311. Select the Options tab to apply the appropriate language for the agent.

To check for the files that have been installed for the Language Pack, see the following table.

Table 25. Language Pack files

Component	Directory	Language Pack files
Data Server	<tpc_install_dir>\data\server\lib</tpc_install_dir>	TSRMsrv_ <locale>.zip where locale is the abbreviation for the language you installed</locale>

Table 25. Language Pack files (continued)

Component	Directory	Language Pack files
the Device server	<tpc_install_dir>\device\apps\was\ profiles\deviceServer\installedApps\ DefaultNode\DeviceServer.ear\ DeviceServer.war\ WEB-INF\lib</tpc_install_dir>	deviceSrv_ <locale>.jar where locale is the abbreviation for the language you installed</locale>
GUI	<tpc_install_dir>\gui</tpc_install_dir>	TSRMgui_ <locale>.jar where locale is the abbreviation for the language you installed</locale>
Data agent	<tpc_install_dir>\ca\subagents\TPC\ Data\agent\lib</tpc_install_dir>	TSRMagt_ <locale>.zip where locale is the abbreviation for the language you installed</locale>
Fabric agent	<tpc_install_dir>\ca\subagents\TPC\ Fabric\lib</tpc_install_dir>	deviceAgt_ <locale>.jar where locale is the abbreviation for the language you installed</locale>
CLI	<tpc_install_dir>\cli\libs</tpc_install_dir>	tpccli_ <locale>.jar where locale is the abbreviation for the language you installed</locale>

The run-time jar files and their installed locations are shown below.

Table 26. Run-time jar files and installed locations

Run-time jar files	Installed location
TSRMagt_ <locale>.zip</locale>	<tpc_install_dir>/ca/subagents/TPC/Data/agent/lib</tpc_install_dir>
TSRMgui_ <locale>.jar</locale>	<tpc_install_dir>/gui</tpc_install_dir>
TSRMsrv_ <locale>.zip</locale>	<tpc_install_dir>/data/server/lib</tpc_install_dir>
deviceAgt_ <locale>.jar</locale>	<tpc_install_dir>/ca/subagents/TPC/Fabric/lib</tpc_install_dir>
deviceSrv_ <locale>.jar</locale>	<tpc_install_dir>/device/apps/was/profiles/ deviceServer/installedApps/DefaultNode/ DeviceServer.ear/DeviceServer.war/WEB-INF/lib</tpc_install_dir>
tpccli_ <locale>.jar</locale>	<tpc_install_dir>/cli/libs</tpc_install_dir>

The <locale> can be one of the following abbreviations:

cs - Czech	it - Italian	pt_BR - Brazilian Portuguese
de - German	ja - Japanese	zh_CN - Simplified Chinese
es - Spanish	ko - Korean	zh_TW - Traditional Chinese
fr - French	pl - Polish	
hu - Hungarian	ru - Russian	

# Chapter 3. Configuring IBM Tivoli Storage Productivity Center

After you have successfully installed IBM Tivoli Storage Productivity Center, you must configure it. You can use the Configuration Utility to learn how to configure and use Tivoli Storage Productivity Center. This section also describes each node under Administrative Services > Configuration.

The Data server hosts the control points for product scheduling functions, configuration, event information, reporting, and graphical user interface support. It will coordinate communication with and data collection from agents that scan file systems and databases to gather storage demographics and populate the database with results. Automated actions can be defined to drive functions like data deletion, IBM Tivoli Storage Manager backup or archiving, or event reporting when defined thresholds are encountered. The Data server will be the primary contact point for all user interface functions. It will also include functions that schedule data collection and discovery for the Device server.

The Device server will discover, gather information from, analyze performance of and control storage subsystems and SAN fabrics. It will coordinate communication with and data collection from agents that scan SAN fabrics.

# **Configuration overview**

After you have installed IBM Tivoli Storage Productivity Center, you must configure your system to get the information you want. This section provides information about the agents required, the jobs that must be run, and the alerts you can set.

To enable data gathering from the devices and servers that will be managed and monitored, different configuration steps are required to enable these different functions in Tivoli Storage Productivity Center.

Tivoli Storage Productivity Center uses four different types of agents to gather data about the devices and servers that will be managed and monitored. Different combinations of these agents are required to effectively enable the functions of Data Manager, Fabric Manager, Disk Manager, and Tape Manager. In addition to these manager functions, the topology viewer is greatly affected by the proper discovery of all the managed entities in the management scope of Tivoli Storage Productivity Center.

# Agents

The agents are:

#### Storage Management Initiative Specification (SMI-S) providers

SMI-S providers or Common Information Model (CIM) agents are provided by the vendor of the storage device, fabric switch, or tape library. For storage, they are needed for storage asset information, provisioning, alerting, and performance monitoring. For the fabric switch, they are used for performance monitoring. The CIM agents are also used for certain switch models to collect topology information, port state information, zoning information, zone control, and alerting. For tape libraries, they are used for asset and inventory information. Each vendor of the storage, fabric switch, or tape library supplies unique CIM agent code for their family of devices. These agents implement an SMI-S provider to provide a communication transport between Tivoli Storage Productivity Center and the managed devices. After a CIM agent is installed and configured, Tivoli Storage Productivity Center can be configured to communicate with it.

When setting up your CIM agents for managing devices, read the CIM agent documentation first. This documentation can provide guidelines for how many devices the CIM agent can be configured to manage. If the CIM agent documentation does not include such guidelines, limit three subsystems per CIM agent.

#### Data agents

The Data agents are installed on all the computer systems that you want Tivoli Storage Productivity Center to manage. These agents collect information from the server they are installed on. Asset information, file and file system attributes, and any other information needed from the computer system is gathered. Data agents can also gather information on database managers installed on the server, Novell NDS tree information, and NAS device information. In Tivoli Storage Productivity Center, you can create ping, probe, and scan jobs to run against the servers that have Data agents installed.

### Storage Resource agents

Storage Resource agents are a type of agent that can collect information from computer systems (host systems) on which they are installed. Information is collected through probe jobs. These agents are designed to be more lightweight and easier to install or deploy than the Data agents.

#### Fabric agents

Fabric agents are installed on computer systems that have fiber connectivity (through HBAs) into the SAN fabrics you want to manage and monitor. Fabric agents use scanners to collect information. The scanners communicate through the HBA to collect fabric topology information, port state information, and zoning information. They also can identify other SAN-attached devices (if they are in the same zone). Fabric agents are discovered during the agent installation process and do not need to be discovered separately. A best practice is to have two agents connected to each switch for redundancy.

## **Out-of-band agents**

The out-of-band agents are used to collect topology information from fabric switches through the IP network using SNMP queries to the switches. A best practice is to have Tivoli Storage Productivity Center communicating with the out-of-band agent (SNMP agent) on each switch in each SAN fabric you are managing.

## Jobs

Tivoli Storage Productivity Center uses data collection jobs to provide information about your environment. The types of data collection jobs are:

#### **Discovery** jobs

Discovery jobs locate data sources and collect basic information about these data sources. When a discovery job is run against a storage subsystem CIM agent or tape library CIM agent, the job locates all the storage subsystems or tape libraries for this CIM agent and retrieves basic information that the

CIM agent holds for these systems. When a discovery job is run against a fabric switch CIM agent, the job retrieves basic available information about the fabric and switches.

#### Probe jobs

Probe jobs collect detailed statistics on all the assets of the managed infrastructure, such as computers, disk controllers, hard disks, clusters, fabrics, storage subsystems, LUNs, tape libraries, file systems, and so on. Probe jobs can also discover information about new or removed disks and file systems. Probe jobs can be directed against any element in the managed infrastructure.

There are four types of probe jobs: for computers, fabrics, storage subsystems, and tape libraries.

Computer probe jobs collect local host information such as file systems, directories, clusters, hard disks and so on. Storage subsystem probe jobs collect information about the storage subsystems, such as disk, volumes, LUNs and so on. Fabric probe jobs collect information about the fabric. Tape library probe jobs collect information about the tape libraries.

When probing storage subsystems that are registered with the same CIM agent, do not probe more than three storage subsystems within the same probe job because the increased load on the agent would increase the likelihood of time-outs. Instead, spread the storage subsystems across multiple probe jobs with different starting times.

#### Scan jobs

Scan jobs collect statistics about the actual storage consumption. Scan jobs are always directed against a Data agent and deliver very detailed information about the file systems, files, and databases of a computer.

#### **Ping jobs**

Ping jobs gather statistics about the availability of the managed computers. Ping jobs generate TCP/IP pings and consider the computer available if it gets an answer. Like scan jobs, ping jobs can be directed against computers only.

#### Performance monitoring jobs

Performance monitoring jobs collect statistics about the performance of storage subsystems and switches. Performance monitoring jobs can be run against storage subsystems, SAN Volume Controllers, and switches and always need a CIM agent to communicate with the elements.

## Alerts

You can define alerts so that Tivoli Storage Productivity Center notifies you when a specified event occurs. Such events are the triggering conditions for the alert. The specific triggering conditions that you can use to define an alert depend on the sort of storage resource that you are monitoring.

The alerts you can define are:

#### Computer

Use this alert to be notified when a condition is detected on a computer during a probe job.

Examples of computer alerts are when RAM is increased or decreased, virtual memory is increased or decreased, or when a new disk is detected or not found, and so on.

This is a Data Manager alert.

#### Filesystem

Use this alert to be notified when a condition is detected on a file system during a probe job.

Examples of file system alerts are when the file system is not found or reconfigured or is low on free space.

This is a Data Manager alert.

#### Directory

Use this alert to be notified when a condition is detected on a directory during a scan job.

Examples of directory alerts are when the directory is not found or when a user or directory storage quota is exceeded.

This is a Data Manager alert.

# Hypervisor

Use this alert to be notified when a hypervisor is discovered or missing, or a virtual machine is added or deleted from a VMware system.

This is a Data Manager alert.

#### Instance

Use this alert to be notified when a condition is detected for a database.

Examples of instance alerts are when a new database or tablespace is discovered for a specific RDBMS, and so on.

This is a Data Manager for Databases alert.

#### Database-tablespace

Use this alert to be notified when a condition is detected for a database-tablespace.

Examples of database-tablespace alerts are when Tivoli Storage Productivity Center detects that free space is low, or the database or table space is offline or dropped for a specific RDBMS, and so on.

This is a Data Manager for Databases alert.

**Table** Use this alert to be notified when a condition is detected for a table in a database.

Examples of table alerts are when a managed table is dropped or exceeds its storage quota, and so on.

This is a Data Manager for Databases alert.

#### Storage subsystem

Use this alert to be notified when a condition is detected on a storage subsystem during a probe job.

Examples of storage subsystem alerts are when a storage subsystem is discovered or not found, a subsystem cache is increased or decreased, a disk is detected or not found, a subsystem goes offline or online, a port is discovered or missing, a back-end controller goes offline or online, a volume goes offline or online, a pool goes offline or online, a pool is missing or discovered, a node goes offline or online, an SAN Volume Controller node is missing or discovered, a disk utilization percentage threshold is reached, and so on.

This is a Disk Manager alert.

#### Fabric

Use this alert to be notified when a condition is detected on a fabric during a probe job.

Examples of fabric alerts are if a fabric is missing or discovered, a fabric goes online or offline, a zone is missing or discovered, a zone set is missing or discovered, and so on.

This is a Fabric Manager alert.

#### Switch

Use this alert to be notified when a condition is detected on a switch during a probe job.

Examples of switch alerts is if a switch is missing or discovered, a switch goes online or offline, a switch blade is missing or discovered, a switch blade goes online or offline, a total port data rate threshold is reached, a total port packet rate threshold is reached, and so on.

This is a Fabric Manager alert.

#### **Endpoint device**

Use this alert to be notified when a condition is detected on an endpoint device during a probe job. Endpoint devices are devices discovered by the Fabric Manager but cannot be identified as a specific device type, such as a computer or subsystem.

Examples of endpoint device alerts are when an endpoint device is missing or discovered, a peripheral entity to node association is missing or discovered, or the version for an endpoint device changes.

This is a Fabric Manager alert.

Once you have defined alerts, you can choose to be notified through different methods.

#### **SNMP** trap

Generate an SNMP trap message to any console or terminal to indicate the occurrence of an alert.

#### **TEC** event

Send alerts to the IBM Tivoli Enterprise Console. The Tivoli Enterprise Console administrator can write correlation and automation rules to analyze Data Manager events and perform responses such as send further notification, create or update trouble tickets, run programs, and so on.

#### Login notification

Send alerts to a specified user upon logging in to the system.

#### Windows Event Log, UNIX Syslog

Record alerts to the OS Event Log. If you already have an administrator monitoring OS logs, this is an easy way to have all of your priority messages centralized for quick notification and viewing.

#### Run script

Run a script in response to an alert.

E-mail Send alerts through e-mail to e-mail addresses that you specify.

## Database connection alerts

Database connection alerts notify the Tivoli Storage Productivity Center administrator when the database connection used by the Tivoli Storage Productivity Center server is lost unexpectedly and when the database connection is restored. The database connection alerts are always enabled and configured to add the alert to the alert log and send an e-mail to the data administrator.

The database connection alerts are:

- DB connection failed
- DB connection successful

You cannot create, configure, delete, disable, edit, or rename these alerts. You can, however, change the destination for the database connection alerts. Expand **Administrative Services** → **Configuration**. Left-click **Alert Disposition**. In the right pane, under Email, you can change all of the fields.

# **Configuration Utility**

Use the Configuration Utility to help you learn about how to configure your IBM Tivoli Storage Productivity Center system.

# Configuration utility tasks

The configuration utility is a teaching tool that helps guide you through the steps and prerequisite steps required to configure your system.

All of the functions in the configuration utility exist on their own within the IBM Tivoli Storage Productivity Center GUI. However, the configuration utility provides you with a single place for new users to find all these common functions and information to help you decide what agents you need and which jobs to run to get the information you want. It provides links into the Tivoli Storage Productivity Center GUI to display reports, add agents, create jobs, create alerts, and so on.

If you are a new user of Tivoli Storage Productivity Center, use the configuration utility to learn what the common functions are and to help you with the task of deciding what agents you need and which jobs to run to get the information you want.

If you are an experienced Tivoli Storage Productivity Center user, you can go to the GUI directly to perform all of the configuration tasks. However, you might also want to use the configuration utility to provide you with a quick summary review of your system.

Depending on what information you want to see and collect, you will go to a different tab in the configuration utility for information and configuration.

#### How to manage the servers and agents

This section describes how to use the configuration utility to manage your servers and agents.

To manage your servers and agents, complete the following steps:

- Expand IBM Tivoli Storage Productivity Center → Configuration Utility → Services tab.
- 2. You can see a list of the Data server, Device server, Data/Storage Resource Agents, CIM agents, in-band Fabric agents, and out-of-band Fabric agents. You can add agents, enable agents, and run discovery jobs.

# Show managed devices

This section describes how to use the configuration utility to show the devices (storage subsystems, switches, or tape libraries) that are managed by the CIM agent.

To show the devices, complete the following steps:

- Expand IBM Tivoli Storage Productivity Center → Configuration Utility → Services tab.
- 2. Under the CIMOM section, click **Show Managed Devices**. A dialog box displays the managed devices.

# How to display availability reports

This section describes how to use the configuration utility to display availability reports.

To display availability reports of storage assets, complete the following steps:

- Expand IBM Tivoli Storage Productivity Center → Configuration Utility → Data Manager tab.
- 2. You can run ping jobs to collect information about the availability of storage assets in your environment.

# How to monitor your storage assets, storage subsystems, and fabrics

This section describes how to use the configuration utility to monitor your storage assets, storage subsystems, and fabrics in your enterprise.

To monitor your storage assets, storage subsystems, and fabrics, complete the following steps:

- For information collected from the Data Manager, expand IBM Tivoli Storage Productivity Center → Configuration Utility → Data Manager tab.
- 2. For information collected from the Disk Manager, expand **IBM Tivoli Storage Productivity Center** → **Configuration Utility** → **Disk Manager** tab.
- 3. For information collected from the Fabric Manager, expand **IBM Tivoli Storage Productivity Center** → **Configuration Utility** → **Fabric Manager** tab.
- 4. You are linked to the existing probe functions or can run probe jobs.

# How to collect statistics on the usage and trending of your actual storage consumption

This section describes how to use the configuration utility to collect statistics on the usage and trending of your actual storage consumption.

To collect statistics on the usage and trending, complete the following steps:

- Expand IBM Tivoli Storage Productivity Center → Configuration Utility → Data Manager tab.
- 2. You can run scan jobs to collect information about storage usage.

# How to view and create alert definitions for storage-related events

This section describes how to use the configuration utility to view and create alert definitions for storage-related events.

To view and create alerts for storage-related events, complete the following steps:

- 1. Expand IBM Tivoli Storage Productivity Center → Configuration Utility → Data Manager tab.
- 2. You can view alerts and create new alert definitions.

## How to enable a storage subsystem for provisioning

This section describes how to use the configuration utility to enable a storage subsystem for provisioning.

Before you can create volumes on the storage subsystem and assign them to hosts, make sure that you have a CIM agent for the storage subsystem, perform a CIMOM discovery job, and run a probe job.

To enable a storage subsystem for provisioning, complete the following steps:

- Expand IBM Tivoli Storage Productivity Center → Configuration Utility → Disk Manager tab.
- 2. See the CIMOM Discovery and Storage Subsystem Probes section on the Disk Manager tab.

## How to monitor storage subsystem performance

This section describes how to use the configuration utility to monitor storage subsystem performance.

For any of the storage subsystems that you are managing with Disk Manager, you can create a Storage Subsystem Performance Monitor job. This requires a CIM agent that is SNIA SMI-S V1.1 compliant. The CIM agent for the storage device must be defined to IBM Tivoli Storage Productivity Center and be up and running. A CIMOM discovery job needs to be run after you have defined the CIM agent to Tivoli Storage Productivity Center.

To view subsystem performance reports and create subsystem performance monitoring jobs, complete the following steps:

- Expand Tivoli Storage Productivity Center → Configuration Utility → Disk Manager tab.
- 2. You can view subsystem performance reports and create performance monitoring jobs. You can also view alerts and create alert definitions related to the storage subsystems.

# How to manage fabric reports, fabric zoning, and monitor switch performance

This section describes how to use the configuration utility to manage and monitor your fabric.

You can have in-band Fabric agents installed on systems in each fabric that you will be managing, CIM agents that are configured to manage each fabric, and out-of-band Fabric agents that communicate with each switch in the fabric. It is a good practice to have multiple agent types configured. CIM agents are the preferred agent type for Brocade and McDATA fabrics. To collect zoning information for Brocade, either CIM agents or out-of-band agents are required, or both. For Cisco switches, out-of-band agents are required for VSAN information. Zoning information is provided only by the in-band Fabric agents for Cisco and QLogic switches.

Before you can run a switch performance monitoring job in IBM Tivoli Storage Productivity Center, you must have a switch CIM agent installed and configured in Tivoli Storage Productivity Center. This CIM agent must be SMI-S V1.1 compliant. For more information about the supported agent types for switch performance management and fabric zone configuration, see "Collecting data with the Fabric Manager" on page 77.

To manage your fabric and switches, complete the following steps:

- Expand IBM Tivoli Storage Productivity Center → Configuration Utility → Fabric Manager tab.
- 2. You can view the fabrics and switches managed by Tivoli Storage Productivity Center. You can also run fabric discovery, probe, and performance monitoring jobs. You can also change your zoning configuration for the fabric.

# How to create alert definitions

This section describes how to use the configuration utility to create alert definitions.

You can create alert definitions to notify you of an alert condition. When you receive an alert notification, you can take the appropriate action when a certain condition occurs on storage subsystems, computers, file systems, directories, fabrics, switches, or endpoint devices.

To create an alert definition, complete the following steps:

- Expand IBM Tivoli Storage Productivity Center → Configuration Utility → Disk Manager tab. The Alerting section helps you create Data Manager alert definitions.
- If you want to see the alerts for the Disk Manager fabric, click the Disk Manager tab to the Alerting section. You can create storage subsystem alert definitions.
- **3**. If you want to see the alerts for the fabric, click the **Fabric Manager** tab to the Alerting section. You can create fabric, switch, and endpoint device alert definitions.

## How to manage tape library reports

This section describes how to use the configuration utility to manage tape library reports.

A CIM agent must be installed and configured to collect information from the tape libraries. After the CIMOM discovery job completes, you can create a tape library probe job that collects asset information (drives, media changers, I/O ports, cartridges, slots, and so forth).

To manage your tape library reports, complete the following steps:

- Expand IBM Tivoli Storage Productivity Center → Configuration Utility → Tape Manager tab.
- 2. You can display information about your tape library, run a CIMOM discovery job for your tape libraries, and run probe jobs for your tape libraries.

#### Learning how to manage element managers and external tools

This section describes how to use the Configuration Utility to add and manage element managers and external tools.

Element managers are programs that allow you to configure and maintain your storage devices. An example of an element manager is DS8000 Storage Manager, which is the default element manager that is provided with IBM System Storage DS8000. Examples of external tools are Web-based user interfaces and local

executable files. For example, you might add the address of a Web site that you frequently access or an application that you often use (a text editor, a spreadsheet application, and so on). You can add and manage connections to element managers and external tools from the Configuration Utility.

To learn how to add and manage connections to element managers and external tools, complete the following steps:

- 1. Expand **IBM Tivoli Storage Productivity Center** → **Configuration Utility** → **Element Manager** tab.
- 2. See the following sections on the Element Manager tab:
  - **DS8000 Element Manager**. This section shows the element managers that have been added for DS8000.
  - Other Device Element Manager. This section shows element managers that have been added for devices other than DS8000. For example, element managers for other DS series systems, IBM Tivoli Storage Enterprise Storage Server, and IBM System Storage SAN Volume Controller.
  - **External Tools**. This section shows external tools such as Web-based interfaces and local executable files that have been added.
  - Advanced Settings. This section defines default settings for the element managers and external tools that are defined in the preceding sections. For example, you can define the default Web browser that you want to use to start Web-based element managers and external tools.

# How to access IBM Tivoli Storage Productivity Center for Replication through IBM Tivoli Storage Productivity Center

This section describes how to access IBM Tivoli Storage Productivity Center for Replication through the IBM Tivoli Storage Productivity Center GUI.

Complete the following steps:

- Expand IBM Tivoli Storage Productivity Center → Configuration Utility → Replication Manager tab. For information about how to administer IBM Tivoli Storage Productivity Center for Replication, see the online help.
- 2. On the Replication Manager tab, you will see these buttons:

## **Replication Health Overview**

The **Replication Health Overview** button displays the Health Overview panel for IBM Tivoli Storage Productivity Center for Replication. This panel provides the following information:

- Overall session status: indicates the session status, which can be normal, warning, or severe.
- Overall storage system status: indicates the connection status of the storage system.
- Management server status: indicates the status of the standby server if you are logged on to the local server. If you are logged on to the standby server, this status indicates the status of the local server.

#### **Replication Sessions Overview**

The **Replication Sessions Overview** button lists all sessions defined within the IBM Tivoli Storage Productivity Center for Replication environment including their state and status.

#### **Replication Storage Systems Overview**

The **Replication Storage Systems Overview** button displays the Storage Systems panel. The Storage Systems panel lists all the known

storage systems, and indicates whether the storage systems are communicating normally with the active and remote servers, if enabled.

#### **Replication Paths Overview**

The **Replication Paths Overview** button displays the ESS/DS Paths panel. The ESS/DS Paths panel summarizes all the known ESS/DS series paths, listing them by storage system.

#### **Replication Management Servers Overview**

The **Replication Management Servers Overview** button displays the Management Servers panel. The Management Servers main panel displays the status of the management servers configuration, lists the management servers in operation (up to two), and enables you to define a standby server, or to define the local server as a standby server to an alternate server. This panel has two variations, depending on whether or not you have defined a standby.

#### **Replication Administration**

The **Replication Administration** button displays the Administration panel. The Administration panel displays a list of IBM Tivoli Storage Productivity Center for Replication users and groups and their access privileges, and allows administrators to take actions on users and groups.

#### **Replication Advanced Tools**

The **Replication Advanced Tools** button displays the Advanced Tools panel. The Advanced Tools panel enables you to create a diagnostic package and change the automatic refresh rate of the GUI.

When you click on a button, a new browser window is opened to the IBM Tivoli Storage Productivity Center for Replication page.

# **Configuration nodes**

This section is organized to help you associate the information in the IBM Tivoli Storage Productivity Center GUI with an explanation of each node.

Expand **Administrative Services > Configuration**. You will see these nodes:

#### **Role-to-Group Mappings**

One of the first tasks you should perform after installing IBM Tivoli Storage Productivity Center is to assign roles to individuals who will use the product. From the **Role-to-Group Mapping** node, you can map Tivoli Storage Productivity Center roles, such as Tape Operator or Fabric Administrator, to user groups that you create in your operating system or in your LDAP-compliant repository. For information about this task, see "Role-to-Group Mappings" on page 279.

#### License Keys

This section provides information on how to administer the database licenses for Data Manager. For information about this task, see "License keys" on page 281.

#### **Alert Disposition**

Use this information to configure IBM Tivoli Storage Productivity Center so that SNMP traps and Tivoli Enterprise Console (TEC) events can be sent to other consoles. For information about this task, see "Alert disposition" on page 287.

#### **Log-File Retention**

You can specify the number of runs and the length of time to maintain the log files generated by IBM Tivoli Storage Productivity Center. For information about this task, see "Log-File Retention" on page 288.

#### Quota and Constraint e-mail Address Rules

You can specify rules for generating e-mail addresses of quota and constraint violators based on their user ID name, first name, or last name as they are registered within the operating system. For information about this task, see "Quota and Constraint e-mail Address Rules" on page 289.

#### Scan/Probe Agent Administration

This topic provides information to assign agents to perform scan and probe jobs. For information about this task, see "Scan/Probe Agent Administration" on page 289.

#### Manual NAS/Netware Server Entry

This section provides information on how to configure IBM Tivoli Storage Productivity Center to support network-attached storage or NetWare. For information about this task, see "Manual NAS/NetWare Server Entry" on page 290.

#### **Agent Manager Registration**

If you are using the Agent Manager (with Data agents and Fabric agents), you must register the Device server and Data server with the Agent Manager. For information about this task, see "Agent Manager Registration" on page 294.

#### **History Aggregator**

This topic provides information about specifying how Data Manager handles data aggregation for statistical reporting purposes. For information about this task, see "History Aggregator" on page 295.

### Storage Resource Agent Deployments

Deploy or install Storage Resource agents through the user interface rather than a separate installation wizard. For information about this task, see "Storage Resource agent deployments" on page 295.

#### Data/Storage Resource Agent Upgrades

This topic provides information on how to configure IBM Tivoli Storage Productivity Center for a Data agent or Storage Resource agent upgrade. For information about this task, see "Data/Storage Resource Agent Upgrades" on page 311.

#### **NetWare Tree Logins**

You must specify a fully-qualified login ID and password for each of the Novell Directory Services trees (NDS trees) discovered by licensed agents. For information about this task, see "NetWare Tree Logins" on page 311.

#### **Resource History Retention**

You can specify how long to keep a history of the statistical elements collected by the system. For information about this task, see "Resource History Retention" on page 311.

#### **Removed Resource Retention**

You can specify the number of days to keep information such as directories, file systems, and disks that have been removed from the system and can no longer be found. For information about this task, see "Removed Resource Retention" on page 312.

### **Resource History Retention for Databases**

You can specify how long to keep a history of the database-related statistical elements collected by the system. For information about this task, see "Resource History Retention for Databases" on page 313.

### **Removed Resource Retention for Databases**

You can specify how long to keep information in the enterprise repository that is related to a database entity that has been removed from the system and can no longer be found. For information about this task, see "Removed Resource Retention for Databases" on page 313.

### **Configuration History Settings**

You can specify how often the system captures snapshots of your configuration and when to delete them. For information about this task, see "Configuration History Settings" on page 314.

# **Role-to-Group Mappings**

One of the first tasks you should perform after installing IBM Tivoli Storage Productivity Center is to assign roles to individuals who will use the product. From the **Role-to-Group Mapping** node, you can map Tivoli Storage Productivity Center roles, such as Tape Operator or Fabric Administrator, to user groups that you create in your operating system or in your LDAP-compliant repository.

For example, on a Windows computer you can create user groups using the Administrative Tools control panel. When a user name is used to authenticate with Tivoli Storage Productivity Center, the user's group membership determines the authorization level.

# **Role-based authorization**

Operating system groups or LDAP groups (for example, groups contained in your LDAP-compliant repository) are associated with predefined roles. When a user ID is authenticated to Tivoli Storage Productivity Center through the GUI, CLI, or APIs, membership in an operating system or LDAP group determines the user's authorization level.

Table 27 shows the association between roles and authorization level.

If you select OS authentication for your Tivoli Storage Productivity Center installation, then you do not have to create any of the groups before installation. The Tivoli Storage Productivity Center superuser role automatically gets mapped to the Administrators group on Windows, to the system group on AIX, or to the root group on Linux.

**Note:** If you plan to select LDAP authentication during your Tivoli Storage Productivity Center installation, then the group you intend to map to the Tivoli Storage Productivity Center Superuser role must exist in the LDAP-compliant directory before you start your Tivoli Storage Productivity Center installation.

Table 27. Roles and author	rization levels
----------------------------	-----------------

Role	Authorization level
Superuser	Has full access to all Tivoli Storage Productivity Center functions.
Productivity Center administrator	Has full access to operations in the Administration section of the GUI.

Role	Authorization level
Disk administrator	Has full access to Tivoli Storage Productivity Center disk functions.
Disk operator	Has access to reports only for Tivoli Storage Productivity Center disk functions. This includes reports on tape devices.
Fabric administrator	Has full access to Tivoli Storage Productivity Center for Fabric functions.
Fabric operator	Has access to reports only for Tivoli Storage Productivity Center for Fabric functions.
Data administrator	Has full access to Tivoli Storage Productivity Center for Data functions.
Data operator	Has access to reports only Tivoli Storage Productivity Center for Data functions.
Tape administrator	Has full access to Tivoli Storage Productivity Center tape functions.
Tape operator	Has access to reports only for tape functions.

Table 27. Roles and authorization levels (continued)

### Notes:

- 1. If a user has multiple roles, the authorization level is a combination of the levels for each of the roles.
- 2. If a user is not a member of any of the roles listed, no access is granted to that user.
- **3**. For enterprise-rollup reports, you need superuser or Tivoli Storage Productivity Center administrator authority to do the following:
  - Add, remove, or modify the Tivoli Storage Productivity Center subordinate server that the master server is monitoring.
  - Create or run probe jobs that include Tivoli Storage Productivity Center subordinate servers.

Any Tivoli Storage Productivity Center user can generate enterprise-rollup reports.

4. When you create and save role-to-group mappings in Tivoli Storage Productivity Center, these mappings get propagated into Tivoli Integrated Portal, where the groups are given the operator authorization. Occasionally, you might find that after creating and saving the role-to-group mappings in Tivoli Storage Productivity Center, you are unable to access Tivoli Integrated Portal as a valid user (in a valid group that is mapped to the operator authorization in Tivoli Integrated Portal). If this occurs, stop and restart the Tivoli Integrated Portal server.

# How to associate a user and group with IBM Tivoli Storage Productivity Center

This section provides information on how to associate a user and group with IBM Tivoli Storage Productivity Center.

## Creating a system group on Windows:

You must first create an operating system group on your computer, and then assign the users to the group. Then you can use the GUI to associate the group with the IBM Tivoli Storage Productivity Center role. For Windows, first create the users you want to have access to the various Tivoli Storage Productivity Center roles. Complete the following steps:

- 1. Go to Start → Settings → Control Panel → Administrative Tools → Computer Management → Local Users and Groups.
- 2. Right-click on Users and click New Users.
- **3.** The New User panel is displayed. Enter a user name, description (optional), and password (twice). Click **Create**.
- 4. Repeat steps 3 and 4 for each new user you want to create. Then create a system group on Windows:
  - a. Go to Start → Settings → Control Panel → Administrative Tools → Computer Management → Local Users and Groups.
  - b. Right-click on Groups and click New Group.
  - c. The New Group panel is displayed. Enter a Group Name and Description (optional). Click **Add**.
  - d. The Select Users or Groups panel is displayed. Enter or select the users or groups you want to add to the new group you have created. Click Add. Then click Create.

### Creating a system group on UNIX or Linux:

For UNIX or Linux, to add new users to the system, follow the steps in this topic.

Complete the following steps:

- 1. Create a new user's name.
- 2. The new user must have a home directory allocated for them.
- **3**. That user must be placed in the group file. Refer to your UNIX or Linux documentation for information about how to create a system group.

#### Associating the user groups to IBM Tivoli Storage Productivity Center roles:

After you have created the operating system group and assigned users to that group, you must assign the groups to IBM Tivoli Storage Productivity Center roles.

Complete the following steps:

- 1. Open the Tivoli Storage Productivity Center GUI.
- 2. Go to Administrative Services → Configuration → Role-to-Group Mappings.
- **3.** On the right pane, click **Edit** for the role you want to associate with the group you have created.
- 4. The Edit Group dialog is displayed. Enter the group you want to associate with the Tivoli Storage Productivity Center role. Click OK. This associates the operating system group with the Tivoli Storage Productivity Center role.
- 5. Click **File** → **Save** to save the mappings.

# License keys

This section provides information on how to administer the database licenses for Data Manager.

You must have the following permissions set to monitor the databases with Data Manager:

Table 28. Database permissions

Database	Permissions
DB2	db2admin
Microsoft SQL Server	public
Oracle	DBA
Sybase	SA level

**Note:** To monitor Oracle databases with IBM Tivoli Storage Productivity Center, the Oracle user needs DBA authority. A non-DBA Oracle user with "create session", "select any dictionary", and "analyze any" roles can still monitor the Oracle database through Tivoli Storage Productivity Center. However, Tivoli Storage Productivity Center will not able to obtain free space information for database objects. During the database registration, when a non-DBA Oracle user is used with the roles mentioned in the preceding list, the following warning message displays:

RDBMS login does not have dba privilege. Freespace will not be calculated for system objects.

Clicking **OK** continues with the registration process. This message also appears in the scan logs when scan jobs are run.

Through the License Keys node, you can administer the license keys for Data Manager for Databases. Specifically, you can:

- Assign Data Manager for Databases licenses to your Data agents.
- Edit, add, and delete the instances within your organization that you want to monitor.
- View the number of Data Manager for Databases licenses.
- View the number of Data Manager for Databases licenses that are not currently assigned (unused) to agents.

Before you can use Data agents to manage the storage for your instances, you must do the following:

- 1. Assign Data Manager and Data Manager for Databases licenses to the agents that will be monitoring RDBMS instances.
- 2. Register the instances on the machines that contain licensed agents.

## Assigning Data Manager database licenses to installed agents

This topic describes how to assign Data Manager database licenses to an agent.

To assign a Data Manager database license to an agent, complete the following steps:

- 1. Expand Administrative Services → Configuration → License Keys. The License Editor window is displayed.
- Click the icon to the left of IBM Tivoli Storage Productivity Center for Data -Databases. The Tivoli Storage Productivity Center for Data - Databases License Editor window is displayed. The field and button descriptions for the Licensing tab are:

#### Select All

Click this button to select all the Licensed boxes.

Deselect All

Click this button to remove all the licenses for Data Manager - Databases.

#### Computer

Displays all the computers on which a Data Manager agent is installed.

#### OS Type

Displays the operating system of the machine where the agent is installed.

#### Domain

Displays the domain of a machine where the agent is installed.

#### Tree Name

For NetWare only.

#### Licensed

Contains a check box that indicates whether a computer is licensed for use with Data Manager - Databases.

If you have unused Data Manager - Databases licenses, continue to the next step. To unassign licenses from agents, see "Unassigning Data Manager -Databases license" on page 287.

- **3**. Click the check box in the **Licensed** column next to the computer containing the instance you want to monitor.
- 4. Click File → Save to save the updated license settings. If an instance is registered on the machine where you licensed the agent, you are ready to set up your Data Manager Databases jobs to monitor its storage. If an instance is not registered on the machine where you licensed the agent, see "Registering instances on machines that contain licensed agents."

## Registering instances on machines that contain licensed agents

This topic describes how to register instances on machines that contain licensed agents.

- 1. Click the **RDBMS Logins** tab on the IBM Tivoli Storage Productivity Center for Data Databases License Editor window.
- 2. The RDBMS Logins window is displayed. Use this window to edit, add, and delete the instances within your organization that you want to monitor. The field and button descriptions for the RDBMS Logins tab are:
  - **Edit** Highlight a row and click this button to edit the login information for the corresponding instance. The RDBMS Login Editor window is displayed.

#### Add New

Click this button to add login information for a new instance. The RDBMS Login Editor window is displayed.

- **Delete** Highlight a row for an instance and click this button to delete that instance from Data Manager - Databases. Once you delete an instance, all the previously-gathered statistics for that instance are automatically deleted from the database repository and that instance will no longer be available for selection in the reporting section of the navigation tree.
- **3**. Click **Add New** to add a new instance. The RDBMS Login Editor window is displayed. Use this window to enter information about the instance that you want Data Manager Databases to monitor.

**Note:** In an Oracle Parallel Server (OPS) or Real Application Cluster (RAC) environment, you only need to register one of the instances within that

environment. OPS and RAC are resource-sharing systems that increase availability and performance by partitioning the workload across multiple servers of a cluster (nodes).

4. Select the name of the machine where the instance is running from the **Host Name** list box.

Note: You can only register instances on machines that contain licensed agents.

5. Enter the following information in the next field:

#### For Oracle

Enter the Oracle SID and host for the instance.

#### For Microsoft SQL/Server

Enter the name of the instance you want to register in the **Instance** field.

#### For Sybase

Enter the server name in the **Server** field.

## For IBM UDB

Enter the name of the instance you want to register in the **Instance** field.

6. Enter a user ID that has the appropriate database privileges within the instance in the **User** field. See "License keys" on page 281.

#### For Oracle

- The following privileges are required for this user ID:
- CREATE SESSION
- SELECT ANY DICTIONARY
- ANALYZE ANY

## For Microsoft SQL Server

The login ID that Data Manager uses to log into Microsoft SQL Server instances that you want to probe must have "permit" access.

- 7. Enter a password for the User ID in the Password field.
- 8. Enter the port on which the instance is listening in the **Port** field.

## For Oracle

The default port is 1521.

#### For Microsoft SQL/Server

The default port is 1433. You must also provide the fully-qualified path to the JDBC driver in the **JDBC Driver** field.

#### For Sybase

The default port is 5000.

#### For IBM UDB

When monitoring multiple UDB instances within your environment, you must ensure that the port numbers you choose are open (unique for each instance) for JDBC and Java connections to those instances. To open up a port, run the following DB2 command on the machine where the instance is located:

#### db2jstrt

The default port number is 6789. You can change this default by indicating the port number you want to use when running the **db2jstrt** command. For example:

db2jstrt 6790

If you enter an incorrect port number, an error will occur. To verify the port number for an instance, do the following:

#### **UNIX or Linux**

View the etc/services file to confirm the correct port number.

AIX Run the following command: ps -ef | grep db2jd

The output from this command indicates the port on which the instance is listening. Use this port number when running the **db2jstrt** command.

#### Windows

Use the information in the IBM DB2 configuration tools to confirm the port number.

9. Click File → Save to save the instance configuration information. You can now run a probe job against the registered instances. You must run a probe job against an instance before you can select any databases or tablespaces against which you want to run a scan job.

#### How to configure Microsoft SQL Server 2000:

Use this information to configure IBM Tivoli Storage Productivity Center so that you can logon to the Microsoft SQL Server 2000 database.

To configure Tivoli Storage Productivity Center so that you can logon to the Microsoft SQL Server 2000 database, follow these steps:

- 1. Install the Data agent and JDBC driver on the Microsoft SQL Server system.
- 2. Ensure that the jar files installed with the JDBC package are located in the same directory. The jar files are mssqlserver.jar, msbase.jar, and msutil.jar. There is no particular location required for installing driver.
- Open the RDBMS Login Editor. Expand Administrative Services > Configuration > License Keys. In the right pane, click RDBMS Logins tab.
- 4. Click **Add New**. The RDBMS Login Editor opens. Enter the following information:

#### Database

Microsoft SQL/Server.

#### Instance name

Name of the instance.

**User** User ID to logon to the Microsoft SQL Server.

#### Password

Password for the user ID.

#### JDBC Driver

Enter the JDBC driver. For Microsoft SQL Server 2000, specify the file name with double backslash characters. For example:

C:\\Program Files\\MSSQL2000\\lib\\mssqlserver.jar

5. Click Save.

#### Configuring Microsoft SQL Server 2005 or 2008:

**Port** 1433

Before you can monitor a Microsoft SQL Server 2005 or Microsoft SQL Server 2008 database, you must make some configuration changes to the Microsoft SQL Server.

Before monitoring the Microsoft SQL Server database, follow these steps:

- Install the Microsoft SQL Server and provide the required information on the installation panels. See the Microsoft SQL Server 2005 Installation and Configuration Guide for detailed information. For the installation and configuration guide, see http://msdn.microsoft.com/en-us/library/ ms143516.aspx.
- 2. For Microsoft SQL Server 2005 and 2008, make sure that the Microsoft SQL Server is using Mixed Mode authentication.
- **3.** After the installation, go to the SQL Server Configuration Manager and make sure you set the Dynamic TCP/IP port to the default port 1433. (See the Microsoft SQL Server 2005 Installation and Configuration Guide for detailed information.) To, configure the Microsoft SQL Server, follow these steps:
  - a. Open the SQL Server Configuration Manager.
  - b. Go to SQL Server 2005/2008 Network Configuration.
  - c. Select Protocols for MSSQLINST (name of the instance).
  - d. Right-click TCP/IP.
  - e. Select Enable: Yes.
  - f. Go to the **IP Addresses / IP All** and add **TCP Dynamic Ports : 1433** (default port).
- 4. Launch the Microsoft SQL Server setup.exe.
- 5. Go to **Installation/Search** for product updates. You will be redirected to the Microsoft update Web site that will scan the computer for the components that need to be updated.
- 6. When finished, select Express Install to install the components found.
- 7. Install the Microsoft CoreXML Services (MSXML) 6.0 SP 2. Reboot the system.
- 8. For Microsoft SQL Server 2008 only: Install the Microsoft SQL Server 2008 Management Objects from the following Microsoft SQL Server 2008 Feature Pack link: http://www.microsoft.com/downloads/. Search for Management Objects.
- For Microsoft SQL Server 2008 only: Install the Microsoft SQL Server 2005 Backward Compatibility Components from the link specified in step 8. Search for 2005 Backward Compatibility.
- 10. Install the Data agent and JDBC driver on the Microsoft SQL Server system.
- Open the RDBMS Login Editor. Expand Administrative Services > Configuration > License Keys. In the right pane, click RDBMS Logins tab.
- **12.** Click **Add New**. The RDBMS Login Editor opens. Enter the following information:

#### Database

Microsoft SQL/Server.

#### Instance name

Name of the instance (mssqlinst).

**User** User ID to logon to the Microsoft SQL Server.

#### Password

Password for the user ID.

**Port** 1433

## JDBC Driver

Enter the JDBC driver. For Microsoft SQL Server 2005 and 2008, open the Microsoft SQL Server 2005/2008 JDBC Driver package and install the driver to the desired location. After the package is unpacked, in the RDBMS logon panel, enter the absolute path to the JDBC Driver (suggested version 1.2):

%MS\_SQL\_DRIVER\_HOME%/sqljdbc\_1.2/enu/sqljdbc.jar

13. Click Save.

# **Unassigning Data Manager - Databases license**

This topic describes how to unassign a Data Manager - Databases license.

To unassign a license, complete the following steps:

- 1. Expand Administrative Services 

  Configuration 

  License Keys.
- 2. The License Editor window is displayed.
- **3**. Click the icon to the left of **IBM Tivoli Storage Productivity Center for Data - Databases**. The IBM Tivoli Storage Productivity Center for Data Databases License Editor window is displayed. Use the **Licensed** column in this window to view the agents to which licenses are currently assigned.
- 4. Clear the **Licensed** check box next to a machine to remove the license for the agent on that machine.
- 5. Click **File** → **Save**. When you remove the license for an agent, the following occurs:
  - All the data gathered by that agent for the instance it monitors is removed from the database repository.
  - You can no longer run monitoring, alerting, or policy management jobs against the instance on the machine where the agent was located.
  - The number of unused licenses increases by one.

# **Alert disposition**

You can configure IBM Tivoli Storage Productivity Center so that SNMP traps and Tivoli Enterprise Console (TEC) events can be sent to other consoles.

# Configuring IBM Tivoli Storage Productivity Center to send SNMP traps and IBM Tivoli Enterprise Console events

This topic provides information on how to configure IBM Tivoli Storage Productivity Center to send SNMP traps, Tivoli Enterprise Console events, or e-mail notifications that are generated when an event specified in an alert is detected. From this node, you can also specify the number of days after which records in the alert log are deleted.

To enable SNMP traps and Tivoli Enterprise Console event alert notifications, consider the following:

## **SNMP** traps

System administrators must set up their SNMP trap ringer with the provided MIB files in order to receive SNMP traps from Tivoli Storage Productivity Center. These files are located in the following directories on the product installation CD:

- Fabric: device\snmp\fabric.mib
- Data: data\snmp\tivoliSRM.mib

#### **TEC events**

Send an alert to the Tivoli Enterprise Console. The Tivoli Enterprise

Console administrator can write correlation and automation rules to analyze Tivoli Storage Productivity Center events according to the event definitions specified in the tivoliSRM.baroc and fabric.baroc files. It also performs responses such as sending further notification, creating or updating trouble tickets, running programs, and so forth.

The tivoliSRM.baroc and fabric.baroc files must be loaded into the current active rule base of the Tivoli Enterprise Console server. This allows Tivoli Enterprise Console events sent by Tivoli Storage Productivity Center to display on the console. These files are located in the following directories on the product installation CD:

- Device Server: device\conf\manager\fabric.baroc
- Data Server: data\tec\tivoliSRM.baroc

### Port 162

Tivoli Storage Productivity Center uses port 162 to listen for SNMP traps. This is the default port. For switches, you must configure the switch to send SNMP traps to the Device server IP address. If you need to change the default port number, use the **setdscfg** command. The attribute to set is **SNMPTrapPort**.

To configure Tivoli Storage Productivity Center to send traps and Tivoli Enterprise Console events, follow these steps:

- 1. Open the Tivoli Storage Productivity Center GUI.
- 2. Go to Administrative Services -> Configuration -> Alert Disposition.
- **3**. On the right pane, you can enter information for two SNMP destinations and one Tivoli Enterprise Console event destination. For the SNMP destination, enter the community name, host, and port information. For the Tivoli Enterprise Console event destination, enter the server and port information. You can also enter information for e-mail information. Click **File -> Save**.

# **Log-File Retention**

You can set the retention period for log files.

You can specify the number of runs and the length of time to maintain the log files generated by IBM Tivoli Storage Productivity Center. We recommend that you set the value for **Maximum number of runs to keep of each schedule** to be less than or equal to the value in the **Maximum number of days' worth of log files to keep** (**regardless of schedule**) field. This will help avoid the situation where entries for job runs remain in the user interface, but the corresponding log files are deleted.

To set the retention period, complete the following steps:

- 1. Go to Administrative Services → Configuration → Log-File Retention.
- 2. In the Maximum number of runs to keep of each schedule field, enter the maximum number of runs (job entries) for a scheduled job that you want to display in the user interface. The default is 5 runs per job. For example: if you enter 10 in this field and then run a probe job for 11 times, job log and job information entries for the first job run are deleted from the filesystem and database repository. Additionally, only the ten most recent runs of the job appear under the IBM Tivoli Storage Productivity Center > Monitoring > Probes > [probe\_jobname] node in the navigation tree.
- 3. In the **Maximum number of days ' worth of log files to keep (regardless of schedule)** field, enter the maximum number of days to keep a log file for a job run. A log file is generated for each run of a job and is stored in the

appropriate log directory. Every log file that is older than the number of days you specify here will be deleted. The default is 90 days.

# **Quota and Constraint e-mail Address Rules**

You can specify rules for generating e-mail addresses of quota and constraint violators based on their user ID name, first name, or last name as they are registered within the operating system.

The user names are obtained as follows:

- For Windows: Full name field, from LDAP.
- For NetWare: Surname and Given name fields, from LDAP.
- For UNIX or Linux: User description from the Password file.

To set the rules, complete the following steps:

- 1. Expand Administrative Services → Configuration → Quota and Constraint e-mail Address Rules.
- 2. Click **Add After** or **Add Before** to include elements within an e-mail address template. An e-mail address template describes how to build the user ID that should be notified in the event of a quota violation. This user ID represents the actual quota violator.
- **3.** Select **USERNAME**, **FIRSTNAME**, **LASTNAME**, **Text**, or **Substring** from the pop-up menu to include as an element in the e-mail address rule:
  - USERAME: the login ID of the quota or constraint violator.
  - FIRSTNAME: the first name of the quota or constraint violator.
  - LASTNAME: the last name of the quota or constraint violator.
  - Text: free form text that you want to appear within the e-mail address.
  - Substring: an element in the e-mail address that is a substring of USERNAME, LASTNAME, or FIRSTNAME. For example: LASTNAME + SUBSTRING(USERNAME, 0, 3)

includes the first three characters of the USERNAME. If a user's last name is Smith and username (as defined by file owner information) is 9A0723, then this substring example is equal to "SMITH9A0".

To define a substring, complete the following steps:

- a. Select Substring after clicking Add After or Add Before.
- b. Select the substring variable: **USERNAME**, **LASTNAME**, or **FIRSTNAME**.
- c. Highlight the range for the substring.
- d. Click **OK**. That substring will now appear within the e-mail address template.
- e. Click **File** → **Save** to save the e-mail address rule.

# Scan/Probe Agent Administration

You can assign Data agents to run scan and probe jobs.

Assign the Data agents that should perform scans against the following:

- Volumes and file systems within the licensed NetWare servers of an NDS tree
- · File systems within NAS filers
- IBM Tivoli Storage SAN File Systems

The window associated with this node provides a complete listing of the licensed NetWare volumes, NAS filers, and SAN File System discovered by Data Manager.

# Manual NAS/NetWare Server Entry

You can configure IBM Tivoli Storage Productivity Center to support network-attached storage or NetWare.

Use the Manual NAS/NetWare Server Entry node to:

- Manually enter information about the NetWare and Network Attached Storage (NAS) servers that you want to monitor within your environment. After you enter information about the NetWare or NAS servers, you can assign agents to those servers on the Scan/Probe Agent window.
- View a list of the NetWare server and NAS filers whose information was manually entered into Data Manager.
- Delete NetWare servers and NAS filers whose information entered into Data Manager.

You can manually set up individual NetWare and NAS servers for monitoring by Data Manager using this window, or you can use a "discovery" method for automatically adding multiple servers at the same time.

We recommend using the "discovery" method when working in large environments where you want to add multiple NAS Filers and NetWare servers for monitoring. Use the Manual NAS/NetWare Server Entry window when you want to manually add individual NAS Filers and NetWare servers for monitoring.

For more information about configuring NAS and NetWare, see http://www.redbooks.ibm.com/. Search for **sg247490**.

# Manually adding a NAS filer or gateway

To manually add a NAS filer or gateway:

- 1. Expand Administrative Services -> Configuration -> Manual NAS/Netware Server Entry.
- 2. Click the Add NAS Server button. The Add NAS Server window is displayed.
- **3**. Enter the following information:

#### Network name

Enter the network name of the NAS server you want to add.

When manually adding a NAS Gateway or Filer that is monitored by a Data agent on a UNIX computer, you must add the NAS using the same name that was used when mounting its file systems on that UNIX computer. You can mount file systems using the short name, fully-qualified name, or IP address of a NAS.

For example, if the file systems from a NAS Gateway were mounted to a UNIX computer (where the Data agent is installed) using the short name of the NAS Gateway, you must add the NAS Gateway in IBM Tivoli Storage Productivity Center using the short name of the NAS Gateway. If the file systems from a NAS Gateway were mounted using an IP address, you must add the NAS Gateway in Tivoli Storage Productivity Center using the IP address as its name.

Consider the following example:

- a. The NAS filer named "oxide" was mounted on the UNIX machine where a Data agent is located. The following commands used the short name and IP address to identify the NAS filer during a file system mount:
  - oxide:/vol/john1 81920 22108 74% 123 5% /n3700\_john1
  - 192.168.1.65:/vol/vol0 47566060 28715228 40% 1016085 52% /n3700\_vol0
- b. To add this NAS filer to Tivoli Storage Productivity Center, enter the following values in the **Network Name** field:
  - oxide
  - 192.168.1.65

If file systems from a NAS Gateway or Filer were mounted on a UNIX computer in different ways, you must add that NAS to Tivoli Storage Productivity Center with the names used in both methods. For example, if one file system is mounted using the fully-qualified name of a NAS Gateway and the other file system is mounted using the IP address, you must add that NAS Gateway to Tivoli Storage Productivity Center twice: once with the fully-qualified name and once with the IP address. Note that only one row appears for this NAS on Manual NAS/Netware Server Entry panel, but both file systems are listed on the Scan/Probe Agent Administration panel.

### Data Manager Agent OS Type

Select the operating system of the computer that contains the agent that will gather information about the NAS filer.

### Accessible from

Select the agent that you want to use to "discover" the NAS filer. This list box will only display agents that are:

- Running under the operating system selected in the **Data Manager** Agent OS Type field.
- Located on Windows or UNIX computers that are accessible to the NAS filers (Data Manager's agents are not located on the NAS filers themselves):
  - Windows: agents are located on Windows computers within the same domain as the NAS filers.
  - UNIX: agents are located on UNIX or Linux computers that have NFS imports for the file systems within the NAS filers.

## **SNMP** Community

Enter the name of the SNMP communities that Data Manager should use when communicating with machines in your environment. If you do not enter the name of an SNMP community, the default community **public** is used. Data Manager uses the SNMP protocol to contact and identify NAS filers. This is an optional field.

#### Login ID

(Windows only.) Enter the login ID that Data Manager will use when logging into the NAS filer.

#### Password

(Windows only.) Enter the password that Data Manager will use when logging into the NAS filer.

#### Add as Other NAS

Select this check box to add a NAS server as Other NAS filer. With this

option, you can monitor and report on file system information on the NAS filer or gateway through Windows CIFS or UNIX NFS shares accessible to the scan or probe job for the agent. No controllers, disks, and logical volumes information are collected or reported.

## NAS Server Vendor Name

Enter the vendor name (or manufacturer) hosting the file system of the NAS server. The default vendor is Network Appliance.

- 4. Click **OK** to have the Data Manager verify the filer for which you entered information. During this verification, Data Manager will:
  - Log in to the NAS filer.
  - Gather information about the file systems visible on those filers to the agent. For UNIX or Linux, it gathers information about the file systems that it can actually see (for example, file systems that are mounted to the UNIX boxes). By default, file systems are discovered at the root. For Windows, it finds all the NAS filers that are visible through CIFS.
  - Determine which file systems are visible to which agents.
  - Enter the NAS server information into the repository.
- 5. Expand Administration Services -> Configuration -> Scan/Probe Agent Administration. This window allows you to assign agents to each file system of the NAS server.

**Note:** At any time you can change the login ID and password for a NAS filer on the **Administrative Services -> Configuration -> License Keys -> Filer Logins** window.

## Deleting a manually-added NAS filer

To delete a NAS filer whose information was manually entered into Data Manager, follow these steps:

- 1. Expand Administrative Services -> Configuration -> Manual NAS/Netware Server Entry.
- 2. Highlight a row that represents the device you want to delete.
- **3.** Click **Delete**. Remember that when you delete a device from this window, all information about that device will be removed from the repository.

# Manually adding a NetWare server

To manually add a NetWare server, complete the following steps:

- 1. Expand Administrative Services → Configuration → Manual NAS/Netware Server Entry.
- 2. Click the Add Netware Server button. The Add Netware Server windows is displayed.
- 3. Enter the following information:

### NDS Trees

Select an NDS Tree. The NDS Trees that appear in this list were discovered and saved to the repository by probe jogs that were automatically run upon agent installation.

#### Network Name

Enter the network name of the NetWare server you want to add.

4. Click **OK** to have the Data Manager verify the server for which you entered information. During this verification, the Data Manager will gather information about the volumes and file systems within the specified NetWare server.

# Deleting a manually-added NetWare server

To delete a NetWare server whose information was manually entered into Data Manager, complete the following steps:

- 1. Expand Administrative Services → Configuration → Manual NAS/Netware Server Entry.
- 2. Highlight a row that represents the device you want to delete.
- **3**. Click **Delete**. Remember that when you delete a device from this window, all information about that device will be removed from the repository.

## Editing Data Manager configuration files

IBM Tivoli Storage Productivity Center provides you with the ability to edit Data Manager configuration files to further customize the component's settings according to the standards at your site.

Data Manager has configuration files for customizing the operation of the server and agent components within your environment. These files reside in the <*TPC\_install\_directory*>/config/ directory, where *TPC\_install\_directory* represents the directory where you installed the product. The default installation directory for the server configuration file is:

- (Windows) c:\program files\IBM\TPC\Data\config\
- (UNIX) /opt/IBM/TPC/Data/config/

The default install directory for the server configuration files is:

- (Windows) c:\program files\IBM\TPC\ca\subagents\TPC\Data\
- (UNIX) /opt/IBM/TPC/ca/subagents/Data/config/

**Note for UNIX:** When you make changes to the configuration files for the server component, you must stop and start the server before those changes will take effect.

Edit the agent.config file to configure the Data Manager agents in your environment. This file appears in the agent install directory on every machine where an agent is installed."agent.config file" on page 500 describes the parameters in the file.

Edit the nas.config file to configure the Data Manager NAS feature for your environment.

The nas.config file contains the following:

- On each line not beginning with #, the first blank-delimited field must contain the SNMP Enterprise code of a NAS filer that the agent should discover, probe, or scan.
- The second field contains identifying information about the filer.

Any remote host that cannot be reached by SNMP or whose enterprise code does not match one of these values will be ignored.

For information about the server files to configure, see "server.config file" on page 498, "scheduler.config file" on page 499, and "TPCD.config file" on page 500.

For information about the agent file to configure, see "agent.config file" on page 500.

# Editing the NAS configuration file

This topic provides information on editing the nas.config file for the Data Manager NAS feature.

Edit the nas.config file to configure the Data Manager NAS feature for your environment.

The nas.config file contains the following information:

- On each line not beginning with #, the first blank-delimited field must contain the SNMP Enterprise code of a NAS filer that the agent should discover, probe, or scan.
- The second field contains identifying information about the filer.

Any remote host that cannot be reached by SNMP or whose enterprise code does not match one of these values will be ignored.

# Agent Manager Registration

Use the Agent Manager Registration page to register the Device server and Data server with the Agent Manager.

**Note:** This procedure does not install the Agent Manager. For information about installing the Agent Manager, see "Installing the Agent Manager" on page 131.

To register the Device server and Data server with the Agent Manager, follow these steps:

- 1. Navigate to Administrative Services > Configuration > Agent Manager Registration.
- 2. Click Agent Manager Registration in the right pane.
- **3**. The Agent Manager Registration window is displayed. Enter the following information:

#### Hostname or IP address

Enter the host name for the Agent Manager. If you specify a host name, use the fully qualified host name. It is preferable to use the fully qualified host name rather than an IP address.

Port (Public)

The public port for the Agent Manager. The default port is 9513.

#### Port (Secured)

The secured port for the Agent Manager. The default port is 9511.

#### User ID (for Data server and Device server registration)

This is the user ID used to register the Data server and the Device server with the Agent Manager.

#### Password (for Data server and Device server registration)

This is the password used to register the Data server and the Device server with the Agent Manager.

#### Password (Common agent registration password)

Enter the agent registration password. This is the password used to register the common agents with the Agent Manager. The agent registration password was specified when you installed the Agent Manager. The default password is **changeMe**.

4. Click OK.

5. If the operation is successful, the Device server and Data server will be registered with the Agent Manager and you will see the information in the following table:

Field Name	Description
Agent Manager	IP address of the Agent Manager.
Port (Public)	The public port for the Agent Manager. The default port is 9513.
Port (Secured)	The secured port for the Agent Manager. The default port is 9511.
User ID	The user ID that the Device server and Data server used to register with the Agent Manager.
Unique ID	This is the unique ID returned by the Agent Manager.

# **History Aggregator**

You can configure reports for data aggregation.

You have the option of turning aggregation off, although this is not recommended. To turn off aggregation, access the History Aggregator window, clear the **Enabled** check box, and select **File**  $\Rightarrow$  **Save**.

To configure reports for data aggregation, complete the following steps:

- **2**. The Edit History Aggregator panel is displayed in the right pane. You can specify the following information:
  - How often to run the job
  - How to handle time zones
  - Triggering conditions
  - Triggered actions

# Storage Resource agent deployments

Use this page to manage Storage Resource agent deployments.

# **Deploying Storage Resource agents**

Deploy or install Storage Resource agents through the user interface rather than a separate installation wizard. You can have only one type of agent per host that points to the same server. For example, if you install a Storage Resource agent, and then later install a Data agent on the same host that points to the same Data server, the Storage Resource agent will automatically get uninstalled after the Data agent runs a successful probe job. See "Using Data agents or Storage Resource agents" on page 300 for information about the features available for Data agents and Storage Resource agents.

You can enter host names from a Microsoft directory, enter host names manually, or import a host list file. You can schedule a job to add the Storage Resource agents at a time that is convenient for you. You can also specify the type of alerts to generate if a job fails. Once you enter information for the Storage Resource agent, you can optionally validate the connection to the Data server. This step helps to eliminate most of the possible failure cases once you have submitted the job for Storage Resource agent deployment.

You can define a deployment job to include multiple computers on which to install Storage Resource agents. The computers you include in a deployment job must share the same administrative user ID and password. IBM Tivoli Storage Productivity Center uses these user credentials to log into the computers when installing Storage Resource agents. If the computers in a deployment job do not share the same administrative user credentials, you must create separate deployment jobs for them.

To deploy Storage Resource agents, follow these steps:

- 1. See "Deployment considerations for Storage Resource agents" on page 298 for a list of considerations before deploying Storage Resource agents.
- 2. Open the Tivoli Storage Productivity Center user interface.
- In the navigation tree pane, expand Administrative Services > Configuration > Storage Resource agent Deployments. Right-click Storage Resource agent Deployments and click Create Storage Resource agent Deployments.
- 4. The Create Storage Resource agent Deployment window opens displaying the Computers tab. Enter the following information:

#### Top pane

#### Creator

Pre-defined creator name.

Name Pre-defined name.

### **Description (optional)**

Enter a user-defined description name for the job.

### Enabled

Check this box to enable Storage Resource agent deployments.

#### Add Host List

Click this button to manually enter names and login credentials for the computers on which you want to deploy Storage Resource agents to.

If you click this button, the Login Information window opens. You can enter information in the following ways:

- Click Add Agents from MS Directory to install Storage Resource agents on one or more Windows computers that are members of a Windows domain.
- Click **Get Agent List From file** to install Storage Resource agents on one or more computers listed in a file. The computers listed in the file must share the same administrative user ID and password.
- Enter the computer names or IP addresses in the Remote Agent Machines table.
- Enter the installation locations for the agents.

**Note:** The default path for Linux and UNIX is /opt/IBM/TPC/ in the subfolder agent. The default path for Windows is C:/Program Files/IBM/TPC in subfolder /agent. The path is filled in automatically by the GUI if you do not supply any value and have checked the box for **Validate before save**. Otherwise, if you enter a path, the agent is installed in that path.

- Select Force under the following circumstances:
  - If an earlier Storage Resource agent installation failed and there are damaged agent files on the computer that cause further installations to fail. If you select this option, Tivoli Storage
Productivity Center attempts to overwrite the previous failed deployment on the computer with a new Storage Resource agent.

 If you want an existing Storage Resource agent to communicate with an additional Tivoli Storage Productivity Center server. To do this, you must create the deployment job from the additional Tivoli Storage Productivity Center server to which you want the Storage Resource agent to communicate.

#### Note:

- You cannot change the communication type for a Storage Resource agent (daemon or non-daemon) when you select the Force option. Make sure to select the same communication type as the existing Storage Resource agent when you create a deployment job.
- If a Storage Resource agent exists on a target computer and you do not select Force, an error occurs during validation and the Storage Resource agent is not installed.

#### Enter the following information:

User The user ID that Tivoli Storage Productivity Center should use when logging into the computers listed in the **Remote Agent Machines** section. The value in this field is applied to all the computers that are included in the deployment job. If a computer listed in the **Remote Agent Machines** section uses a different user ID than what you specify in this field, you must create a separate deployment job for that computer.

#### Password

Password for the computers on which to deploy Storage Resource agents.

## Re-type

Re-enter the passwords for the target computers.

## **Certificate Location**

For Storage Resource agents, certificates are required for SSH protocol communication between the server and agent. This certificate needs to be stored on the server. See "Creating a certificate for SSH protocol" on page 302.

#### Passphrase

For Storage Resource agents, enter the passphrase used for SSH protocol communication. See "Creating a certificate for SSH protocol" on page 302.

**Port** Port for the Storage Resource agent. The default is 9510.

#### Change Authentication

Click this button to change the user ID, password, and certificate location for deploying Storage Resource agents. For information, see "Changing authentication for a Storage Resource agent" on page 442.

#### **Edit Selected Entries**

Click this button to edit the host list.

#### Remove

Click this button to remove the Storage Resource agent from Tivoli Storage Productivity Center.

5. Click the When to run tab to enter the following information:

## How often to run

- You can specify a time to run:
- Run now
- **Run once at** (specify a date and time to run)

#### How to handle time zones

- You can specify a time zone to use:
- Use the time zone that the server runs in
- Use this time zone (select a time zone)
- 6. Click the Alert tab to specify the following information:

## **Triggering-Condition**

- The triggering conditions you can specify are:
- Storage Resource agent Deployment Failed

#### **Triggered-Actions**

- You can choose from the following check boxes:
- SNMP Trap
- TEC Event
- Login Notification
- Windows Event Log
- Run Script
- Email

Depending on what action you select, you might have other choices to make. For example, if you select the **Windows Event Log** check box, the **Event Type** field becomes active so that you can specify a severity for the event in the Windows event log.

7. Click File > Save.

## **Deployment considerations for Storage Resource agents**

There are a number of guidelines you must take into consideration when deploying and working with Storage Resource agents in your environment.

### Required authority for deploying Storage Resource agents

You must be logged in to IBM Tivoli Storage Productivity Center with a user ID that has the superuser role to schedule Storage Resource agent deployments. See the Configuration - Role-to-Group Mappings topic for more information about user roles.

### Supported operating systems

Storage Resource agents are not deployable on all the operating systems where you can deploy Data agents. See "Using Data agents or Storage Resource agents" on page 300 to view the operating systems that are supported by Storage Resource agents.

## Communication between the Tivoli Storage Productivity Center server and a Storage Resource agent

The Tivoli Storage Productivity Center server connects to a monitored computer when a Storage Resource agent is deployed and whenever a probe job runs against that agent.

During deployment, the server communicates with the target computer using one of the following protocols:

- Windows server message block protocol (SMB)
- Secure shell protocol (SSH)

- Remote execution protocol (REXEC)
- Remote shell protocol (RSH)

After deployment, the type of communication between the server and agent on that computer depends on whether you deployed the agent as daemon service or non-daemon service. See the *IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication Installation and Configuration Guide* for more information about these protocols.

## Daemon or non-daemon services

You can deploy a Storage Resource agent agent as a daemon or non-daemon service:

- A Storage Resource agent that is deployed as a daemon service runs in the background on the monitored computer and listens for requests from the Tivoli Storage Productivity Center server. Connectivity between the server and agent is established using SSL. The server and agent have their respective certificates and no additional information is required besides those certificates and the security that is provided by the SSL protocol.
- A Storage Resource agent deployed as an on-demand service (non-daemon service) runs as a stand-alone executable file on the monitored computer. Connectivity between the server and agent uses the same protocol that was used during the deployment of the agent.

## Authentication between the Tivoli Storage Productivity Center server and a Storage Resource agent

Tivoli Storage Productivity Center requires the correct authentication information (user ID, password, port, certificate location, or passphrase) for monitored computers each time it communicates with Storage Resource agents running those computers. If the authentication information changes for a host computer on which a Storage Resource agent is deployed, the authentication information for that agent must be updated using the **Change Authentication** or **Update Storage Resource agent List** functions on the Data/Storage Resource agents panel located under the Administrative Services > Data Sources node in the navigation tree.

### Storage Resource agents and Data agents on the same computer

You cannot install a Storage Resource agent on a computer where a Data agent is already installed *and* pointing to the same Data server as that Storage Resource agent. For example, if you install a Storage Resource agent on a computer, and then later install a Data agent that points to the same Data server as that Storage Resource agent, the Storage Resource agent is automatically uninstalled after the Data agent runs a successful probe job.

You can install a Storage Resource agent and a Data agent on the same computer if those agents communicate with different Data servers.

#### Storage Resource agents on computers running Windows 2008

Before you can deploy a Storage Resource agent on a computer that is running the Windows 2008 operating system, you must turn off the firewall on that computer. If you do not turn off the firewall, the deployment fails. To turn off the firewall on a Windows 2008 computer, complete the following steps:

- On the desktop of the Windows 2008 computer, click Start > Administrative Tools.
- 2. Click Windows Firewall with Advanced Security.

- 3. Click Windows Firewall Properties.
- 4. Change the **Firewall state** field to **Off** on the following tabs: **Domain Profile**, **Private Profile**, **Public Profile**.
- 5. Click **OK** to accept the changes and exit.
- 6. Deploy a Storage Resource agent to the Windows 2008 computer.

#### Data collection and Storage Resource agents

You can only run probe jobs against Storage Resource agents. You cannot run other data collection jobs against them such as scans, pings, and performance monitors. See "Reports for Data agents and Storage Resource agents" on page 301 for a list of reports that show the data collected by Storage Resource agents.

## Upgrades and job logs

If you deploy a Storage Resource agent and later decide to upgrade it to a Data agent, the job logs for the probes that are run by the Storage Resource agent are removed from the computer and you are unable to access those job logs through the user interface. The job logs for probes that are run by the Data agent are retained.

#### Time zones for computers monitored by Storage Resource agents

The time zones of computers that are monitored by Storage Resource agents are shown as Greenwich Mean Time (GMT) offsets in Tivoli Storage Productivity Center reports. The time zones of computers that are monitored by Data agents are shown as the local time zone in Tivoli Storage Productivity Center reports. For example, a computer located in Los Angeles shows the following time zones in the By Computer report in Asset reporting.

- If monitored by a Storage Resource agent: (GMT-8:00) GMT-8:00
- If monitored by a Data agent: (GMT-8:00) America/Los\_Angeles Time zone

#### Deployment jobs and computers on which to install Storage Resource agents

You can define a deployment job to include multiple computers on which to install Storage Resource agents. The computers you include in a deployment job must share the same administrative user ID and password. IBM Tivoli Storage Productivity Center uses these user credentials to log into the computers when installing Storage Resource agents. If the computers in a deployment job do not share the same administrative user credentials, you must create separate deployment jobs for them.

#### Additional information about Storage Resource agents

See the *Planning* > *General Planning* > *Planning for Storage Resource agents* section in the *IBM Tivoli Storage Productivity Center Installation and Configuration Guide* for additional planning, configuration, and certificate information about Storage Resource agents.

## Using Data agents or Storage Resource agents

Use a Data agent or a Storage Resource agent to collect storage data about a computer. The storage entity that you want to monitor and the type of information you want to collect can help determine which of these agents to install on a computer.

The following table shows the different features in IBM Tivoli Storage Productivity Center that are available for computers on which Storage Resource agents or Data agents are installed. Use this table to help determine which type of agent best meets your storage monitoring needs.

Feature	Data agent	Storage Resource agent
Is Agent Manager required?	Yes	No
How do you install these agents?	Use the Tivoli Storage Productivity Center installation program to install Data agents on computers. This program is included on the disks provided with the product. See the <i>IBM</i> <i>Tivoli Storage Productivity Center and</i> <i>IBM Tivoli Storage Productivity Center for</i> <i>Replication Installation and Configuration</i> <i>Guide</i> for more information about how to run the installation program.	To install Storage Resource agents, expand Administrative Services > Configuration. Right-click Storage Resource Agent Deployments. Click Create Storage Resource Agent Deployments. You do not need to run the installation program to install Storage Resource agents.
Is the Java Runtime Environment (JRE) required on the computer where the agent is installed?	Yes	No
Is there a list of hardware requirements and operating systems on which these agents can run?	Yes	Yes
What data collection jobs can you run against the computers on which the agents are installed?	Probes, pings, scans	Probes (host systems only)
Can you include computers and file systems that are monitored by agents in monitoring groups?	Yes	No, you cannot include computers and file systems that are monitored by Storage Resource agents in monitoring groups.
What reports show the data that is collected by the agents?	See "Reports for Data agents and Storage Resource agents" to view a list of the reports that show data collected by Data agents.	See "Reports for Data agents and Storage Resource agents" to view a list of the reports that show data collected by Storage Resource agents.

Table 29. Available features for Data agents and Storage Resource agents

## **Reports for Data agents and Storage Resource agents**

You can collect data about the computers on which Data agents and Storage Resource agents are installed. The type of agent determines what kind of information you can collect and which reports display that information.

Use this table to learn:

- The reports that reflect the information collected by data collection jobs
- The data collection jobs that you can run against each agent type

	Table 30. Available data collection	jobs and re	ports for Data	agents and S	Storage Resource	e agents
--	-------------------------------------	-------------	----------------	--------------	------------------	----------

Reports	Data collection job	Data agent	Storage Resource agent
Batch reports	Probes, Scans, Pings	Yes	No
System Reports:			
• Data		2	N 1 4 4 11 1
• Fabric	Probes, Scans	Yes	Yes, but not all <sup>1</sup>
• Disk	Probes	Yes	No

Reports	Data collection job	Data agent	Storage Resource agent
Asset Reports:			
• By Cluster			
By Computer	Probes	Yes	Yes
By Hypervisor	Probes	Yes	No
• By OS Type	Probes	Yes	Yes
By Storage Sybsystem	Probes	Yes	No
• System-wide	Probes, Scans	reports	Yes, but not all -
Availability Reports:			
Ping reports	D:		N.T.
Computer Uptime reports	Pings Probes	Yes Yes	No Yes <sup>3</sup>
Capacity reports	Probes	Yes	Yes
Usage reports	Scans	Yes	No
Usage Violation reports	Scans	Yes	No
Backup reports	Scans	Yes	No
Data Manager for Databases reports	Probes, Scans	Yes	No
Storage Subsystem reports	Probes	Yes	Yes
Storage Subsystem Performance reports	Subsystem Performance Monitors	Yes	No
Rollup Reports:	TPC server probes <sup>4</sup>	Yes	Yes
• Asset			Yes
Database Asset		Yes	NO Ves
Capacity		Yes	No
Database Capacity		Yes	

Table 30. Available data collection jobs and reports for Data agents and Storage Resource agents (continued)

Notes:

1. Only the following Data system reports are available for Storage Resource agents: Disk Capacity Summary, Disk Defects, Storage Capacity, Total Freespace

- 2. Only the following System-wide Asset reports are available for Storage Resource agents: Agents, Computers, Disk/Volume Groups, Disks, File Systems or Logical Volumes, Volumes, Exports or Shares.
- **3.** Computer Uptime reports are not available for Storage Resource agents that are invoked using the non-daemon protocol for data collection. These reports do not contain data for computers on which non-daemon based Storage Resource agents are deployed. To collect computer uptime information using a Storage Resource agent, that agent must use a daemon service for runtime operation.
- 4. Run IBM Tivoli Storage Productivity Center server probes to collect information from subordinate servers for display in the master server's rollup reports. You cannot use Storage Resource agents to collect information about relational databases, so the Database Asset and Database Capacity reports will not display data for those agent types.

## Creating a certificate for SSH protocol

Before you can install the Storage Resource agents using the SSH protocol, you must create a certificate.

## Creating a certificate for SSH protocol (non-Windows)

To create a certificate for SSH protocol, complete the following steps:

1. Telnet to the remote machine using the root user ID.

- Go to the directory where you want to create the certificate: cd to ~/.ssh or ~db2inst1/.ssh
- 3. Enter ssh-keygen. Accept the default names (for example, id\_rsa).
- 4. Enter the passphrase.
- 5. Two files will be created:

id\_rsa This is the private key.

## id\_rsa.pub

This is the public key.

6. Create an authorized\_key file in the same location as id\_rsa.pub by entering the following:

cat id\_rsa.pub >> authorized\_keys

7. Copy the id\_rsa (private key) to your server machine. For example, to copy the id\_rsa file to c:\keys\id\_rsa on the IBM Tivoli Storage Productivity Center server (user responses are in boldface type):

```
# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (//.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
You identification has been save in //.ssh/id_rsa.
Your public key has been save in //.ssh/id rsa.pub.
The key fingerprint is:
# cat id_rsa >> authorized_keys
# 1s -1
total 24
-rw-r-r- 1 root system 1743 Oct 15 09:40 authorized_keys
        1 root system 1743 Oct 15 09:39 id_rsa
-rw---
-rw-r-r- 1 root system 399 Oct 15 09:39 id_rsa.pub
#
```

Note: You must copy the file in binary mode.

- 8. To connect to the remote system using the private key, the following information needs to be entered on the Remote Agent Machines panel when you install the Storage Resource agent:
  - User
  - Certificate Location (c:\keys\id\_rsa)
  - Passphrase

## Setting up an SSH daemon on Windows

On Windows Server 2003, Windows XP, Windows Server 2008, or Windows Vista, you must run the **ssh-host-config** command.

You must be in a Cygwin window or be an xterm user to create the **sshd** service. In most cases you just click on the **cygwin.bat** to bring up the Bash shell.

This requires the following steps:

- 1. Installing Cygwin.
- 2. Setting up your sshd service in Cygwin.
- 3. Creating the certificate.

### Installing Cygwin

To install Cygwin, go to http://cygwin.com. Note that this page contains a

link that displays help for the setup program and a link to download the setup program. Read the help before running the setup program. Then download the Cygwin program by clicking the **Install Cygwin now** link. Start the setup program on your computer by running the **setup.exe** program. Select the appropriate download option (**Install from Internet**, **Download from Internet**, or **Install from Local Directory** ) as described in the help files.

If you are upgrading from an older version of Cygwin to a newer version, you need to remove the **sshd** service before installing the new version of Cygwin.

Accept the default installation options as they are presented to you (Root Directory, Install For, Default Text File Type, and so on). Select a download mirror that is geographically close to your location. Note that some sites require an FTP account before you can install Cygwin. You can either request an account or simply select another mirror.

During the installation process, a Select Packages list is displayed. Expand the plus sign (+) next to the Admin category and select **cygrunsrv** and the **Bin** checkbox. Expand the plus sign (+) next to the Net category and select **openssh**. Expand the plus sign (+) next to the Util category and select **diffutils**. Click **Next** to resume the setup program. The time required to download the packages depends on how busy the mirror is, and on the speed of your internet connection. With **openssh** and **cygrunsrv**, the downloaded files require approximately 70 MB of disk space. Allow 20 to 30 minutes for the download and installation to complete.

#### Setting up your sshd service in Cygwin

Here is an example of the sequence of steps and responses. The responses to the prompts are in boldfaced type.

1. Run the **ssh-host-config** command.

**Note:** With Cygwin you might experience permission problems when running the **ssh-host-config** command. If you have permission problems, run these commands:

chmod +r /etc/passwd chmod +r /etc/group chmod 777 /var \$ ssh-host-config Generating /etc/ssh\_host\_key Generating /etc/ssh host rsa key Generating /etc/ssh\_host\_dsa\_key Generating /etc/ssh config file Should privilege separation be used? (yes/no) no Generating /etc/ssh\_config file Warning: The following functions require administrator privileges! Do you want to install sshd as service? **yes** (If sshd is already installed as a service, answer no.) You appear to be running Windows 2003 Server or later. On 2003 and later systems, it's not possible to use the LocalSystem account, if sshd should allow passwordless logon (e. g. public key authentication). If you want to enable that functionality, it's required to create a new account sshd\_server' with special privileges, which is then used to run the sshd service under. Should this script create a new local account 'sshd\_server' which has the required privileges? (yes/no) yes Please enter a password for new user 'sshd server'. Please be sure that this password matches the password rules given on your system. Entering no password will exit the configuration. PASSWORD=<password> (Specify a password for the sshd\_server account.) User 'sshd\_server' has been created with password '<password>'. If you change the password, please keep in mind to change the password for the sshd service, too. Also keep in mind that the user sshd server needs read permissions on all users' .ssh/authorized\_keys file to allow public key authentication for these users. (Re-)running ssh-user-config for each user will set the required permissions correctly. Which value should the environment variable CYGWIN have when sshd starts? It's recommended to set at least "ntsec" to be able to change user context without password. Default is "ntsec". CYGWIN=ntsec The service has been installed under sshd server account. To start the service, call 'net start sshd' or 'cygrunsrv -S sshd'. Note! If the service doesn't start because of a login failure Host configuration finished. Have fun!

#### 2. Start the **sshd** service:

- a. Open a command prompt window.
- b. Enter **net start sshd** or in a Bash prompt, enter **cygrunsrv -start sshd**.
- c. Verify that the daemon is running.
- d. Enter **ps** -**a**. Examine the output to see if /usr/sbin/sshd is contained in the list of running processes.

To stop the service from a Windows command prompt, enter **net stop sshd**. Alternatively, you can change to the C:\cygwin\bin directory (or open a Bash shell) and enter **cygrunsrv -stop sshd**.

**3**. When you have started the sshd service, test it by entering the following from a Bash shell prompt:

```
ssh localhost -l <user_ID>
    or
ssh <host_name> -l <user_ID>
```

If **localhost** does not work, use the short host name. If you receive a message indicating that the authenticity of localhost cannot be established, answer **Yes** to the question "Are you sure you want to continue connecting?" When prompted for your account password on **localhost**, enter the password you use when logging in to the computer.

- 4. Create the accounts that can log into the computer:
  - a. Create the Windows accounts. Click Start > Settings > Control
     Panel > User Accounts. Make each user a member of the
     Administrators group. Perform this operation for each user you want to add before you create the corresponding Cygwin accounts.
  - b. Make a backup copy of the /etc/passwd file.
  - c. Create the Cygwin user accounts. Run the following command: mkpasswd -1>/etc/passwd
  - d. Verify that a home directory has been created for each account that you have added. Change the ownership of the home directory to its owner (run the **chown** command). If a user's home directory does not exist, create one. For example, enter the following:

mkdir home/<account\_name>;chown <account\_name>/home/<account\_name>

- e. When you add users, you need to stop and start **sshd** before that account is recognized because **sshd** only reads the file /etc/passwd when the service starts.
- f. If you need to create groups of accounts, create the Windows groups first, then create the Cygwin groups. After creating the Windows groups, run the following command:

mkgroup -l>/etc/passwd

When you add groups, you also need to stop an start **sshd** before the new group is recognized.

The Cygwin sshd service should be added as a service that starts automatically. To verify this, click **Start > Settings > Control Panel > Administrative Tools > Services**. Look for **CYGWIN sshd** in the name list. Verify that it is started and configured to start automatically.

## Creating the certificate

To create a certificate for SSH protocol, complete the following steps:

- 1. CD to  $\sim$ /.ssh.
- 2. From the Bash shell prompt, here is an example of the input and output (user responses are in boldface type):

```
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/Administrator/.ssh/id_rsa):
newkev
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in newkey.
Your public key has been saved in newkey.pub.
The key fingerprint is:
3d:4f:55:c9:02:51:c9:2b:dd:d3:0c:59:b8:e9:2e:a2 Administrator@tb124-wi
The key's randomart image is:
+--[ RSA 2048]----+
           0=.0++
            +++
            . ==.
          . +000
        S o o. .
           + .
            ...
           . . .
        E. . .
Administrator@tb124-wi ~/.ssh
$ 1s
authorized keys id rsa id rsa.pub known hosts newkey newkey.pub
Administrator@tb124-wi ~/.ssh
$ cat newkey.pub >> authorized keys
Administrator@tb124-wi ~/.ssh
$
```

**3**. Once the newkey.pub file has been added to the authorized\_keys directory, copy the private key **newkey** to the IBM Tivoli Storage Productivity Center server.

## Replacing a custom certificate for SSL protocol

IBM Tivoli Storage Productivity Center provides default SSL certificates for communication between the Data server and Storage Resource agent. You can replace your custom certificates with the default certificates.

## Overview of replacing a custom certificate for SSL protocol

IBM Tivoli Storage Productivity Center uses SSL certificates for communication between the Data server and Storage Resource agent (daemon service). IBM Tivoli Storage Productivity Center provides default SSL certificates for this communication. If you want to use your own certificates, you can replace the default certificates with your custom certificates.

## Server certificate

The IBM Tivoli Storage Productivity Center Data server uses the TPCDataServer.jks and server.pwd files for communication with the Storage Resource agents. If you are using custom certificates, you need to replace these files.

There are two ways you can replace these certificates:

- Before installation of the Data server
- After installation of the Data server

## Storage Resource agent certificate

The Storage Resource agent uses the certificate files sra.pem and sra.pwd for communication with the Data server. These two files are zipped into

the certs.zip file on the server system for deployment purposes. If you are using custom certificates, you need to replace these files.

There are two ways you can replace the certificates:

- · Before deployment of the agent
- After deployment of the agent

These are the general steps for replacing custom certificates:

- 1. Generate the custom certificates.
- **2**. Stop the Data server (and the Storage Resource agent, if the agent is already deployed) if applicable.
- **3**. Replace the custom certificates on the Data server and Storage Resource agent or on the disk1 installation image.
- 4. Start the Data server (and the Storage Resource agent, if the agent is already deployed) if applicable.

#### How to generate custom certificates

The script file createSRACerts.sh (for Linux or UNIX) or createSRACerts.bat (for Windows) is located in the following directory:

<TPC\_install\_directory>/data/sra/tools/certs

<TPC\_install\_directory> is where the IBM Tivoli Storage Productivity Center servers are installed. The default directory is /opt/IBM/TPC for Linux or UNIX or C:\Program Files\IBM\TPC for Windows.

To generate custom certificates, follow these steps:

1. Create the custom certificates.

The createSRACerts script creates the custom certificates. The syntax is:

► createSRACerts	oryrootCAPassword
►	_store_passwordagent_password
output_directory Directory where the certific sra_certs_out directory in	ates are created. The default is the current working directory.
<i>rootCAPassword</i> Root CA password (root co non-encrypted password is	mmon authority password). The default : s5umEvApR6cafruhustu.
<i>server_key_password</i> Server key password. The c	lefault non-encrypted password is:

Server key password. The default non-encrypted password is drUtaxahaswefraf9uth.

server\_store\_password

Server store password. The default non-encrypted password is: wr4d5Xekaqafehet5u2a.

agent\_password

Agent password. The default non-encrypted password is: jawUchezuthew6azEjef.

**Note:** You will be prompted for the password when the script is run. Provide the value of the rootCAPassword on the command line (if specified on the command line). Otherwise, use the default values in the createSRACerts.sh or createSRACerts.bat script when prompted for the password (twice). The following example creates the SSL certificate using the default output directory and default passwords.

#### createSRACerts

The following examples create the SSL certificates using the directory /tmp on UNIX and C:\temp on Windows. These examples use the default passwords. The passwords are stored in:

/tmp/sra\_certs\_out (for UNIX)
C:\temp\sra\_certs\_out (for Windows)

Here are the examples:

createSRACerts /tmp (for UNIX)
createSRACerts C:\temp (for Windows)

The following examples create SSL certificates in the directory /tmp on UNIX and C:\temp on Windows. These examples use non-default passwords for root CA and server key. The passwords are stored in:

/tmp/sra\_certs\_out (for UNIX)
C:\temp\sra\_certs\_out (for Windows)

Here are the examples creating non-default passwords for the root CA password and server key password:

createSRACerts /tmp newpasswordforrootCA newpasswordforserver (for UNIX)
createSRACerts C:\temp newpasswordforrootCA newpasswordforserver (for Windows)

- Regenerate the certificates again if you have a failure. Delete the files in the out directory before re-running the createSRACerts script.
- **3**. Stop the Data server and Storage Resource agent. If the Data server is installed and running, stop the Data server. Make sure that the JVM for the Data server is not running.

Stop the Storage Resource agent if the certificates for the agent are installed and running.

- 4. Replace the certificates. There are three scenarios:
  - Replacing the certificates after the server is installed.
  - Replacing the certificates before the server is installed.
  - Replacing the certificates after the agent is installed.

### Replacing the certificates after the server is installed

The server certificates are in the following directory: <TPC\_install\_directory>/data/sra/tools/certs/out

These are the server certificates: TPCDataServer.jks server.pwd

For the server certificates, copy the server certificates to the following directory:

<TPC\_install\_directory>/data/sra/certs

The agent certificates are created in the certs.zip file in the following directory:

<TPC\_install\_directory>/data/sra/tools/certs/out/agent

Copy the certs.zip file into the following directory:

<TPC\_install\_directory>/data/sra/<agent\_operating\_system>

Unzip the certs.zip file into the following directory: <TPC\_install\_directory>/data/sra/<server\_operating\_system>

<agent\_operating\_system> is the operating system that the Storage Resource agent is running under. <server\_operating\_system> is the operating system on which the Data server is installed on.

## Replacing the certificates before the server is installed

The server certificates are in the following directory: <disk1\_image\_install\_directory>/data/sra/tools/certs/out

These are the server certificates: TPCDataServer.jks server.pwd

<disk1\_image\_install\_directory> is the location of the disk1 image.

For the server certificates, copy the server certificates into the following directory:

<TPC\_install\_directory>/data/sra/certs

The agent certificates are created in the certs.zip file in the following directory:

<TPC\_install\_directory>/data/sra/tools/certs/out/agent

Copy the certs.zip file into the disk1 image or disk2 image directory:

<disk1 or disk2\_image\_install\_directory>/data/sra/
<agent\_operating\_system>

Disk1 is the location of the disk1 image that was extracted for installation of the server and agents. Disk2 is the location of the disk2 image that was extracted for installation of the agents.

Unzip the certs.zip file into the following directory: <disk1 image install directory>/data/sra/<server operating system>

<agent\_operating\_system> is the operating system that the Storage Resource agent is running under. <server\_operating\_system> is the operating system on which the Data server will be installed on.

#### Replacing the certificates after the agent is installed

The agent certificates are in the certs.zip file that gets created in the following directory:

<TPC\_install\_directory>/data/sra/tools/certs/out/agent

Unzip the certs.zip file into the
<storage\_resource\_agent\_install\_directory>/certs directory.
<storage\_resource\_agent\_install\_directory> is the location where the
Storage Resource agent has been installed.

5. Start the Data server and the Storage Resource agent. If the Data server has stopped for replacement of the certificates, then start the Data server after the replacement of the certificates.

If the Storage Resource agent has stopped for replacement of certificates, then start the Storage Resource agent after the replacement of the certificates.

## **Data/Storage Resource Agent Upgrades**

You can configure IBM Tivoli Storage Productivity Center for a Data agent or Storage Resource agent upgrade.

When you apply maintenance to Tivoli Storage Productivity Center, you have the choice whether to upgrade the Data agent or Storage Resource agent now or to upgrade the agent at a later time. To ensure that all your agents are at the current release level and to manage your network load, schedule upgrades on a regular basis.

To configure Tivoli Storage Productivity Center for a Data agent or Storage Resource agent upgrade, complete the following steps:

- 1. Expand Administrative Services → Configuration → Data/Storage Resource Agent Upgrades.
- 2. Right-click on Data/Storage Resource Agent Upgrades. Click Create Data/Resource Agent Upgrade.
- **3**. The Create Data/Storage Resource Agent Upgrade panel is displayed in the right pane. You have the following tabs:

### Computers

You can select Computer Groups or Computers.

#### When to Run

You can specify how often to run the job or how to handle time zones.

#### Options

You can specify to force an upgrade for an agent, maintenance upgrade for an agent, or language pack to apply to an agent.

Alerts You can specify the triggering conditions and triggering actions.

Enter your information. For more information about upgrading Data agents or Storage Resource agents, see "Upgrading the Data agents" on page 370.

## **NetWare Tree Logins**

You must specify a fully-qualified login ID and password for each of the Novell Directory Services trees (NDS trees) discovered by licensed agents. Data Manager uses this login ID to log into your NDS trees and gather information about the NetWare servers and volumes in those trees.

When you log into the NDS trees, you will see the licensed NDS trees discovered by agents installed in your environment. The login ID you assign to each NDS tree must have permission to enumerate the volumes within the NetWare servers on that tree.

To login to the NDS trees, complete the following steps:

## **Resource History Retention**

You can specify how long to keep a history of the statistical elements collected by the system.

By specifying a number for days, weeks, or months for each element, you can control the amount of data that will be retained and available for historical analysis and charting. The longer you keep the data, the more informative your analysis. You can set retention periods for:

- Directories
- Pings
- Disks
- Performance Monitors
- Filesystems
- · Computer Uptime

**Note:** If you do not select a check box, the data related to that check box is retained permanently. This might cause a large amount of data to accumulate in the database repository over time. If you select a check box and enter a value of 0, the data related to that check box is removed immediately from the database repository.

To set the retention periods, complete the following steps:

- 1. Expand Administrative Services → Configuration → Resource History Retention.
- **2.** The Retain History panel is displayed in the right pane. Enter the information for the retention periods.

## **Removed Resource Retention**

You can specify the number of days to keep information about directories, file systems, disks and so on that have been removed from the system and can no longer be found.

Information is kept in the database repository. To clear the history record for a resource and activate a new period for resource retention, perform a discovery or probe job on the resource.

You can set the retention period for the following:

- Directories
- File systems
- Disks
- Filers
- Subsystems
- Fabric
- Tape
- Hypervisors
- Virtual Machines
- IBM Tivoli Storage Productivity Center Servers: When you remove a data source (agent) from a subordinate server or a storage entity that it monitors, the master server will continue displaying information about that agent or storage entity in rollup reports for a specified amount of time. You can specify how quickly that information is removed by changing this setting.

**Note:** The retention time for cluster resource groups that are monitored by Tivoli Storage Productivity Center is determined by the values you enter in the **Filers** and **Filesystems** fields. If the values in the **Filesystems** and **Filers** fields are different, the field with the higher value (longer retention period) is applied to cluster resource groups.

If you do not select a check box, the data related to that check box is retained permanently. This might cause a large amount of data to accumulate in the database repository over time. If you select a check box and enter a value of 0, the data related to that check box is removed immediately from the database repository.

To set the retention period, complete the following steps:

- 1. Expand Administrative Services → Configuration → Removed Resource Retention.
- 2. The Retain Removed panel is displayed in the right pane. Select the resource and enter the number of days to keep.

## **Resource History Retention for Databases**

You can specify how long to keep a history of the database-related statistical elements collected by the system.

By specifying a number of days, weeks, or months for each element, you can control the amount of data that will be retained and be available for historical analysis and charting. The longer you keep the data, the more informative your analysis.

You can retain the histories for:

- Databases-Tablespaces
- Tables

**Note:** If you do not select a check box, the data related to that check box is retained permanently. This might cause a large amount of data to accumulate in the database repository over time. If you select a check box and enter a value of 0, the data related to that check box is removed immediately from the database repository.

To set the retention period, complete the following steps:

- 1. Expand Administrative Services → Configuration → Resource History Retention for Databases.
- 2. The Retain History panel is displayed in the right pane. Enter the retention period information.

## **Removed Resource Retention for Databases**

You can specify how long to keep information in the enterprise repository that is related to a database entity that has been removed from the system and can no longer be found.

By specifying a number for days, you can indicate how long to keep information for tablespaces and tables that have been removed from the system.

**Note:** If you do not select a check box, the data related to that check box is retained permanently. This might cause a large amount of data to accumulate in the database repository over time. If you select a check box and enter a value of 0, the data related to that check box is removed immediately from the database repository.

To specify a retention period, complete the following steps:

- 1. Expand Administrative Services → Configuration → Removed Resource Retention for Databases.
- 2. The Retain Removed panel is displayed in the right pane. Enter the information for the retention period.

## **Configuration History Settings**

This page allows you to specify how often the system captures snapshots of your configuration and when to delete them. It also gives the number of snapshots in the database, indicates when the last one was taken (and allows you to refresh this setting), and enables you to create and enter a title for a snapshot on demand.

You must configure and save the settings on this page before you can use the Configuration History function.

To specify the configuration history settings, complete the following steps:

- 1. In the Create snapshot every field, type how often (in hours) you want the system to take snapshot views of the configuration.
- 2. To automatically delete snapshots, click the check box to place a check mark before Delete snapshots older than. In the box that follows that field, type how long you want to keep the snapshots (in days) before they are automatically deleted.
- **3.** To optionally refresh the date and time of when the latest snapshot was created, click **Update**.
- 4. To optionally create a snapshot on demand, click **Create Snapshot now**. If you choose, you may type a name for the snapshot in the box below **Title this snapshot** (optional).
- **5.** To change your settings to the default, click **Reset** to defaults. The defaults are create snapshots every 12 hours and delete snapshots older than 14 days.
- 6. Click **File > Save** to save the configuration history settings.

## Configuration: Device server specific

This section provides configuration information that is specific to the Device server.

## **Configuring switches**

This section provides configuration information for switches.

IBM Tivoli Storage Productivity Center is a storage area network (SAN) management application that discovers devices in the SAN and displays a topology of the SAN environment. It is designed to operate using industry-based standards for communicating with fibre channel switches and other SAN devices. This can be done using the simple network management protocol (SNMP) interface for out-of-band agents, the FC-GS-3 interface for in-band agents, CIM agents, or a combination of these agent types. FC-GS-3 refers to the Fibre Channel Generic Services 3 standard. To gather and display the information as expected, the switches must be configured correctly. The configuration varies between vendors and whether in-band agents, out-of-band agents, CIM agents, or a combination of these agent types are used. One of the common sources of customer problems is incorrect configuration of the switches being managed. This leads to missing information and misconceptions that the Tivoli Storage Productivity Center product does not work with certain switches. The switch vendors supported are Brocade, Cisco, CNT, McDATA, and QLogic. Other vendors such as IBM, often sell these switches under their own labels.

WithTivoli Storage Productivity Center in-band discovery, theTivoli Storage Productivity Center for Fabric agent software is installed on SAN-attached hosts. The Fabric agents collect information about the fabric across the fibre channel network by querying the switch and the attached devices through the host bus adapter (HBA) in the system. For the switches to successfully receive and respond to the queries, there are some basic requirements:

- The switch must support the FC-GS-3 standard interface for discovery.
  - Name server
  - Configuration server
  - Unzoned name server
- For zone control functions, the fabric zone server must be supported, except in the case of Brocade switches.

Fabric events are automatically sent from the agent to Tivoli Storage Productivity Center with in-band discovery. There is no need for configuration.

The switch configuration for in-band agents is typically much simpler than for out-of-band, although it requires more involvement on the host side with the HBA and agent software.

SNMP-based out-of-band discovery collects some of the same information that can be obtained in-band, but it does so differently. In out-of-band discovery, Tivoli Storage Productivity Center queries the switch directly rather than going through a Fabric agent and the fibre channel network. It does this using the SNMP protocol to send queries across the IP network to management information bases (MIBs) supported on the switch. Tivoli Storage Productivity Center uses the FC Management MIB (sometimes referred to as the FA MIB) and the FE MIB. The queries are sent only to switches that have been added to Tivoli Storage Productivity Center for use as SNMP agents. SNMP information is collected for a single switch. The out-of-band discovery registers each switch. For the switch to successfully receive and respond to the query, there are some basic requirements:

- The FC Management MIB and FE MIB must be enabled on the switch.
- The switch must be configured to receive SNMPv1 queries and respond in SNMPv1. Some switches are configured to use SNMPv2 or SNMPv3 by default.
- The community string configured in Tivoli Storage Productivity Center must match one of the community strings configured on the switch with read access. Cisco switches must additionally have a community string match for write access. The default community strings in Tivoli Storage Productivity Center are "public" for read access and "private" for write access. Additional community strings can be defined on the switches, but will not be used.
- SNMP access control lists need to include the Tivoli Storage Productivity Center system. Some automatically include all hosts while others exclude all by default.

Another aspect of the SNMP configuration includes trap notification. SNMP traps are generated by the switch and directed to Tivoli Storage Productivity Center as an indication that something in the fabric has changed and that a discovery should occur to identify changes. The default configuration for handling switch traps is to send them from the switch to port 162 on theTivoli Storage Productivity Center system. To successfully generate and receive traps, there are some configuration requirements.

• The trap destination parameter on the switch must be set. This is the host that receives the trap and sends it to Tivoli Storage Productivity Center . This is set on the switch.

- The destination port parameter on the switch must be set. Tivoli Storage Productivity Center listens on port 162 by default. This is on the host.
- The traps must be sent as SNMPv1. This is set on the switch.
- The trap severity level should be set to generate traps for change conditions. This typically means to send error level traps and anything more severe. This is set in Tivoli Storage Productivity Center.

You must install or enable a CIM agent for the switch to enable the following features:

- For gathering fabric performance data
- For working with a set of McDATA inactive zonesets (Note: this will be synchronized with the EFCM Server's inactive zonesets if the CIM agent is configured to run with a "proxy" connection to the EFCM Server)
- For collecting and configuring Brocade zone aliases

For information about installing or enabling a CIM agent for the switch, contact your switch vendor.

Configuring switch settings differs between switch vendors and models. For more information about configuring switches, see: http://www.ibm.com/ developerworks. In the upper right corner, search for **hislop**. Open the article "Configure switches successfully for IBM Tivoli Storage Productivity Center for Fabric." This article applies toTivoli Storage Productivity Center version 2 and 3.

## Configuring the inactive zonesets for a fabric data source

Some fabrics have multiple locations to retrieve a database for inactive zonesets. In some scenarios, and for some switch vendors, these definitions for inactive zonesets are not synchronized.

For heterogeneous fabrics composed of McDATA and Brocade switches, IBM Tivoli Storage Productivity Center allows you to choose which CIM agent to use to retrieve inactive zonesets and when configuring zoning. To set the inactive zonesets Data Source, go to Fabric Manager > Fabrics, select the fabric, and click Select Inactive Zone Sets Data Source.

## Excluding devices from Fabric agent scans

If you want to run the Fabric agent on a system that can access removable media devices such as tapes, you can remove those devices from Fabric agent attribute scans. Some removable media devices cannot handle command queueing, causing a long tape read or write command to fail. To avoid this problem, follow these steps:

- 1. Stop the Fabric agent.
- Create a file named ExcludeList in the following directory: <agent\_install\_dir>/conf
- 3. In the ExcludeList file, enter the world wide names of the devices that you want to be excluded from Fabric agent scans, each on a new line. Save the file. The file name needs to be exactly the same as the one provided above.

Here is an example of an ExcludeList file to exclude the four WWNs 1000000c920d02a, 1000000c920ccf9, 1000000c93f51ca, 10000000c926342a from receiving **scsi** commands from the Attribute scanner:

10000000c920d02a
10000000c920ccf9
10000000c93f51ca
10000000c926342a

4. Start the Fabric agent.

## Configuration guidelines for agent placement

This section provides configuration guidelines for well placed agents.

The placement of in-band agents, out-of-band agents, and CIM agents will determine the information displayed in the topology. Follow these guidelines to determine the best agent placement strategy for these agent types.

- For a topology map, if no CIM agents are present, you need to define in-band and out-of-band agents on some selected servers and switches to discover all of your topology. If CIM agents are present for McDATA or Brocade fabrics, in-band agents might still be required to collect detailed information about endpoints. If no CIM agents are present, switch zoning and LUN masking might restrict access to some devices, and some zone control features will not be available.
- For a complete topology map, including correct device icons, you need to define in-band and out-of-band agents, or in-band and CIM agents (for Brocade and McDATA), on all servers and switches, except on those supporting Remote Node Identification (RNID).
- For information on Brocade zoning, you need to configure CIM agents for the Brocade fabric. Alternatively, you can define the switches as out-of-band agents, but with this configuration, zone alias information will not be available.
- For complete device centric and host centric views, you need to place in-band agents on all servers you want to be displayed.
- Cisco needs an out-of-band discovery for VSAN information.

Before implementing in-band agents, out-of-band agents, and CIM agents, you should have a clear idea of your environment and the information you want to collect. This will help you select the agents and can minimize the overhead caused by in-band and out-of-band agents.

For information about what information the agents collect, see "Information gathered by the agents" on page 612.

For more information about the supported agent types for switch performance management and fabric zone configuration, see "Collecting data with the Fabric Manager" on page 77.

## Managing a SAN without agents

There are cases where there may be no agents on the SAN. These cases are:

- The hosts do not currently have a Fabric agent installed.
- The host operating system is not supported by the Fabric agent.
- The customer requirements do not require the deployment of a Fabric agent (topology map only).

In these cases, it is recommended that an agent be installed on the Device server itself. This allows the Device server to use advanced features like Remote Node Identification (RNID) which requires an agent.

Normally the Device server does not have a Fibre Channel host bus adapter. In this configuration, the following steps are taken:

- 1. A Fibre Channel host bus adapter is added to the manager.
- 2. An agent is installed on the Device server(the Device server is installed first).
- **3**. All storage devices are verified to ensure that they use LUN masking techniques. The LUN masking techniques prevent the Device server from accessing the disks used by the host systems.
- 4. The Fibre Channel host bus adapter is attached to the SAN to be managed. This host is added to each zone that is intended to be managed by the Device server.

## Setting timeout values for the Device server

This topic describes how to set timeout values for the Device server.

If a probe or discovery of a storage subsystem times out before the operation completes, you will receive the following error message:

HWN021650E Encountered timeout while connecting to CIMOM IP: Port. Check the CIMOM or increase timeout value.

where *IP* is the IP address, and *Port* is the port number. If you determine that the Common Information Model Object Manager (CIMOM) is not the cause of the problem, you can use the command-line interface (CLI) to increase the timeout values for the Device server.

To set timeout values for the Device server, complete the following steps:

1. Issue the **getdscfg** command to determine the current values of the timeout properties. From the command prompt, type the following command:

```
cli>tpctool getdscfg -user user -pwd password -url host:port
-property timeout_property timeout_value
```

where:

- User is an IBM Tivoli Storage Productivity Center user ID.
- Password is the password for the Tivoli Storage Productivity Center user ID.
- *Host* is the host name or IP address, and *Port* is a valid port number for the HTTP service of the Device server.
- Timeout\_property is one of the following strings:
  - http.timeout
  - CIMClientWrapper.Timeout
  - Probe.Timeout.Array
  - Probe.Timeout.InBand
  - Probe.Timeout.SVC
  - Probe.Timeout.LMM
  - Discovery.Timeout
  - CIMOMManager.TestConnectionTimeout
- *Timeout\_value* is the value for the timeout.
- 2. Issue the **setdscfg** command to increase the timeout value. Type the following command:

cli>tpctool setdscfg -user user -pwd password -url host:port -property timeout\_property timeout\_value For more information about **tpctool**, see the *Tivoli Storage Productivity Center Command-Line Interface Reference*. You also can view help from the command line by issuing the command with the **-help** option.

# Service Location Protocol (SLP) configuration recommendations

This section provides some configuration recommendations for enabling Tivoli Storage Productivity Center to discover a larger set of storage devices through SLP. These recommendations cover some of the more common SLP configuration problems. This section discusses router configuration, SLP directory agent configuration, and environment configuration.

For additional information about SLP, see the **Service Location Protocol Request for Comments** website at http://www.ietf.org/rfc/rfc2165.txt.

## **Router configuration**

Configure the routers in the network to enable general multicasting or to allow multicasting for the SLP multicast address and port, 239.255.255.253, port 427. The routers of interest are those that are associated with subnets that contain one or more storage devices that are to be discovered and managed by Tivoli Storage Productivity Center.

To configure your router hardware and software, refer to your router and configuration documentation.

## SLP directory agent configuration

This topic provides information on suggestions for configuring the SLP directory agent.

Configure the SLP directory agents (DAs) to circumvent the multicast limitations. With statically configured DAs, all service requests are unicast by the user agent. Therefore, it is possible to configure one DA for each subnet that contains storage devices that are to be discovered by Tivoli Storage Productivity Center. One DA is sufficient for each of the subnets. Each of these DAs can discover all services within its own subnet, but no other services outside its own subnet. To allow Tivoli Storage Productivity Center to discover all of the devices, it needs to be statically configured with the addresses of each of these DAs. This can be accomplished using the Tivoli Storage Productivity Center Discovery Preference panel.

You can use this panel to enter a list of DA addresses. Tivoli Storage Productivity Center sends unicast service requests to each of these statically configured DAs, and sends multicast service requests on the local subnet on which Tivoli Storage Productivity Center is installed. Configure an SLP DA by changing the configuration of the SLP service agent (SA) that is included as part of an existing CIM Agent installation. This causes the program that normally runs as an SLP SA to run as an SLP DA.

**Note:** The change from SA to DA does not affect the CIMOM service of the subject CIM Agent, which continues to function normally, sending registration and deregistration commands to the DA directly.

## **Environment configuration**

This section provides information on the configuration of your environment.

It might be advantageous to configure SLP DAs in the following environments:

- In environments where there are other non-Disk Manager SLP UAs that frequently perform discovery on the available services, an SLP DA should be configured. This ensures that the existing SAs are not overwhelmed by too many service requests.
- In environments where there are many SLP SAs, a DA helps decrease network traffic that is generated by the multitude of service replies. It also ensures that all registered services can be discovered by a given UA. The configuration of an SLP DA is particularly recommended when there are more than 60 SAs that need to respond to any given multicast service request.

## SLP registration and slptool

IBM Tivoli Storage Productivity Center uses Service Location Protocol (SLP) discovery, which requires that all of the CIMOMs that Disk Manager discovers are registered using the SLP.

In a non-multicast network environment, SLP can only discover CIMOMs that are registered in its IP subnet. For CIMOMs outside of the IP subnet, you need to use an SLP DA and register the CIMOM using **slptool**. Ensure that the **CIM\_InteropSchemaNamespace** and **Namespace** attributes are specified.

For example, enter the following command:
slptool register service:wbem:https://<myhost.com>:<port>

Where *myhost.com* is the name of the server hosting the CIMOM, and *port* is the port number of the service, for example 5989.

**Note: slptool** is installed with a CIMOM. Run the command from the machine hosting the CIMOM.

## Configuring the Data server for a Windows domain

By default, the IBM Tivoli Storage Productivity Center Data server is installed to operate under a local account created at installation time. However, if you are functioning in a Windows domain environment, and want to use domain accounts for authentication and authorization with Tivoli Storage Productivity Center, then you will need to reconfigure the service.

To configure the Data server, complete the following steps:

- Open the Windows Services panel and verify that the Windows service IBM Tivoli Storage Productivity Center - Data Server is configured to log on as a domain user in order to perform Network Management Functions.
- 2. If the Data server is not configured as indicated in step 1, perform the following steps:
  - a. In the Windows Services panel, highlight **IBM Tivoli Storage Productivity Center - Data Server**.
  - b. Right-click to bring up the service menu.
  - c. Select Properties.
  - d. Select the Log on tab.
  - e. Specify a domain account under **This account** using the <domain\_name>\<domain\_user> format.
  - f. Enter and confirm the password for the domain account.
  - g. Click **Apply** for the setting, and then click **OK**.

- h. Restart the Data server.
- **3**. Log onto the Tivoli Storage Productivity Center GUI as a Tivoli Storage Productivity Center superuser.
- 4. Click Administrative Services > Configuration > Role-to-Group mappings.
- 5. Delete any instances of previous domain group mappings.
- 6. Save the changes.
- 7. Create new Role-to-Group mappings by specifying only the domain group name.
- 8. Save the changes.
- You can now log onto the Tivoli Storage Productivity Center GUI with a domain account belonging to the domain group by using the <domain\_name>\<domain\_user> format.

## Granting local administrative privileges to a domain account

For Windows users, the user account which the Common agent runs under requires local administrative rights. Because these rights are not necessarily guaranteed for domain users in a Windows domain environment, this topic provides information on how to grant local administrative rights for domain users. Using this procedure, you do not have to manually process each machine in the domain.

To use Group Policy to grant local administrative privileges to a domain account, complete the following steps:

- 1. On the domain controller, go to Administrative Tools → Active Directory Users and Computers (you must be running with Domain Administrator privileges).
- **2**. Right-click on the Organizational Unit (OU) upon which you want to apply the Group Policy. Click **Properties**.
- **3**. The Group Policy Properties panel is displayed. Select the Group Policy tab and click **New** to create a new Group Policy.
- 4. Designate a name for the new Group Policy. Select the new Group Policy and click **Edit**.
- 5. The Group Policy Object Editor panel is displayed. Go to New Group Policy Object <your\_policy> → Computer Configuration → Windows Settings → Security Settings → Restricted Groups. Right-click on Restricted Groups. Click Add Group.
- 6. For example, name the new group "Administrators." Under "Properties", add the user "Administrator", and the domain accounts or groups upon which you want the Group Policy in effect for. For example, you can add "TPC\tapeadmin", "TPC\tapegroup", and "TPC\TestGroup". Click **OK**.
- 7. Add these user rights to the domain account:
  - Act as part of the operating system
  - Log on as a service

In the Group Policy Object Editor, go to **New Group Policy Object** <your\_policy> → Computer Configuration → Windows Settings → Security Settings → Local Policies → User Rights Assignments. In the right pane, select "Log on as a service" and double-click. Add the domain user for whom you are granting the user right for and click OK. Repeat this step for "Act as part of the operating system."

**8**. The group policy is now enforced for the Organizational Unit to include the domain accounts and groups specified under the local Administrators group on

each computer in the Organizational Unit. In addition, the domain user has been granted the necessary rights. To verify this, log into a domain computer and open the Computer Management console. Select **Groups**, double-click on the Administrators group, and verify the membership of the domain users.

## Configuring IP addressing

This section provides information about configuring IP addressing.

## Configuring IBM Tivoli Storage Productivity Center with multiple IP addresses

If the system where IBM Tivoli Storage Productivity Center is to be installed has multiple IP addresses, then a configuration value has to be set manually as a post-installation task using the **tpctool setdscfg** command. The value to be set is for the local IP address which has to be used for subscription for CIM Indications for CIM agents.

If you are using IPv6 machines, see "Planning for Internet Protocol Version 6" on page 34.

For multiple IPv6 addresses, the IPv6 address to use for CIM indication subscription by Tivoli Storage Productivity Center can be specified by setting the property System.LocalIPv6Address as described below.

With dual stack IPv4 and IPv6 Tivoli Storage Productivity Center servers, two IP addresses are needed to subscribe to IPv4 CIMOMs and IPv6 CIMOMs. The configuration property System.LocalIPv6Address is used for IPv6 CIMOMs and the property System.LocalIPAddress is used for IPv4 CIMOMs.

To change the IP address, follow these steps:

- 1. Open a command prompt window on the server machine.
- 2. Change to the following directory:

cd <TPC\_install\_dir>\cli

**3**. Enter the following command:

tpctool setdscfg -user <user\_ID> -pwd <password> -url
<host>:<port> -property System.LocalIPv6Address <value>

Where:

user\_ID

is the user ID.

### password

is the password for the user.

- **host** is either the host name or IP address of the system running Tivoli Storage Productivity Center.
- **port** is a valid port number for the HTTP service of the Device server (the default is 9550).
- **value** is the local IP address which has to be used for subscription for CIM Indications for CIM agents.
- 4. Verify that the command was successful by entering this command:

tpctool getdscfg -user <user\_ID> -pwd <password>
-url <host>:<port> -property System.LocalIPv6Address

## Changing the HOSTS file

When you install Windows on your computers, you must follow these steps to avoid addressing problems with IBM Tivoli Storage Productivity Center. The problem is caused by the address resolution protocol which returns the short name (not-fully qualified host name). This problem can be avoided by changing the entries in the corresponding host tables on the DNS server and on the local computer. The fully qualified host name must be listed before the short name.

To change the HOSTS file, follow these steps:

- In the %SystemRoot%\system32\drivers\etc\ directory, you will find the HOSTS file.
- 2. You will have to edit the **HOSTS** file. An example of a **HOSTS** file is shown below.

# Copyright (c) 1993-1995 Microsoft Corp. # # This is a sample HOSTS file used by Microsoft TCP/IP for Windows NT. # This file contains the mappings of IP addresses to host names. Each # entry should be kept on an individual line. The IP address should # be placed in the first column followed by the corresponding host name. # The IP address and the host name should be separated by at least one # space. # Additionally, comments (such as these) may be inserted on individual # lines or following the machine name denoted by a '#' symbol. # For example: # 
 102.54.94.97
 rhino.acme.com
 # source server

 38.25.63.10
 x.acme.com
 # x client host
 # 192.168.123.146 jason jason.groupa.mycompany.com

**3**. Enter the fully qualified host name as the first line to be searched in the table. (Lines preceded with a # sign are comment lines.) For example, add the line in bold highlight to the file below. The lines must be entered in the order shown.

# # 102.54.94.97 rhino.acme.com # source server # 38.25.63.10 x.acme.com # x client host **192.168.123.146 jason.groupa.mycompany.com jason** 192.168.123.146 jason jason.groupa.mycompany.com

**Note:** Host names are case-sensitive. This is a WebSphere limitation. Check your host name. For example, if your computer shows the name as JASON (upper case), then you must enter JASON in the HOSTS file.

## Configuring Java Web Start to start the IBM Tivoli Storage Productivity Center GUI

This topic describes how to configure Java Web Start to start the IBM Tivoli Storage Productivity Center GUI.

## Overview

# For example:

The following information pertains to starting Tivoli Storage Productivity Center using Java Web Start:

- The IBM WebSphere Application Server is automatically installed on the same computer as the Tivoli Storage Productivity Center Device server and Data server.
- The Java Web Start application enables a system to communicate with Tivoli Storage Productivity Center that is running on AIX, Linux, UNIX, and Windows systems. Users launch Tivoli Storage Productivity Center using an Internet Explorer or Firefox Web browser. The following list shows the supported Web browser versions by operating system:
  - AIX: Firefox 2.0
  - Linux: Firefox 2.0
  - Windows: Internet Explorer 7 or Firefox 2.0 and 3.0
- The remote system must have IBM Java Runtime Environment (JRE) 1.5 and Java Web Start installed to start the GUI using a Web browser. Java Web Start on the server automatically checks the remote system and provides links to the appropriate levels of the JRE and Java Web Start if it does not detect them.

You can start the Tivoli Storage Productivity Center GUI in one of the following ways:

- Starting the Tivoli Storage Productivity Center GUI without IBM Tivoli Integrated Portal
- Starting the Tivoli Storage Productivity Center GUI through IBM Tivoli Integrated Portal

## Note:

- Each time that you start Tivoli Storage Productivity Center GUI from the remote system, Java Web Start compares the version running on the remote system to determine if there is an updated version on the server. If the server version is more current, Java Web Start opens the more current version of the GUI.
- If you are running Java Web Start on a computer that is on the other side of a firewall from the Tivoli Storage Productivity Center server, you must enable some ports (in both directions: in and out). These ports are 9550 (port for the Device server) and 9549 (port for the Data server).

## Starting the GUI without IBM Tivoli Integrated Portal

To configure Java Web Start to launch Tivoli Storage Productivity Center from a Web browser, complete the following steps:

- 1. Start the Device server on the server where you installed Tivoli Storage Productivity Center.
- 2. From the remote system, open a Web browser window and enter the Web address of the target server. The URL is in the format http:// <device\_server\_location>:<device\_server\_port>/ITSRM/app/welcome.html.

**Note:** The default Device server port is 9550; however, this number could have been changed during installation. You should check with your system administrator to see if this port has changed.

- **3.** Tivoli Storage Productivity Center requires that IBM JRE 1.5 is installed on your remote system. If the JRE is not installed, a message displays with a link that enables you to download the JRE. The Web browser displays messages based on your system. If your language is not supported, English displays in your Web browser.
- 4. If necessary, download and install IBM JRE 1.5.

5. After the JRE has installed, Java Web Start on the server determines if Java Web Start is installed on the remote system. If Java Web Start is not installed, a message displays with a link that enables you to download Java Web Start.

After you have completed these steps, you can start the Tivoli Storage Productivity Center from a remote system using the following mechanisms:

- From an Internet Explorer or Firefox browser window, either by typing in the appropriate Web address or by clicking a saved bookmark.
- From the Java Web Start Cache Viewer.

## Note:

• For Internet Explorer 7, the browser uses Java Web Start to open the launch.jnlp file and continue with the download and launch of Tivoli Storage Productivity Center.

For Firefox, you will see a pop-up window asking what you would like to do with the launch.jnlp file. Select the **Open with** radio button. Ensure that the program being used to open the file is Java Web Start. Check the box for **Do this automatically for files like this from now on**. Click **OK**.

- For example, if you are using Firefox on AIX or Linux, follow these steps:
  - 1. Download a MIME type editor extension for Mozilla Firefox 2.0 (for example, Mime Edit 0.60) on the AIX or Linux system. To download the MIME editor, go to https://addons.mozilla.org/en-US/firefox/addon/4498.
  - 2. Start the Firefox browser.
  - 3. Click File > Open File.
  - 4. Go to the mime\_edit-0.60-fx+tb.xpi file and click **Open**. Firefox guides you through the installation of the extension and then tells you to restart Firefox.
  - 5. When you have restarted Firefox, click **Tools > Mimetypes**.
  - 6. If there is an entry for "application/x-java-jnlp-file" in the File types list, select it and click Edit. In the section "When a file of this type is encountered" select Open it with. Enter the path to javaws on your AIX or Linux system. The most common path is /usr/java5/jre/javaws/javaws. Click OK to close the dialog used for editing the entry. Click OK to close the Mimetypes interface.
  - 7. If there is no entry for "application/x-java-jnlp-file" in the File types list, click **New Type**. Enter the following values:
    - MIME Type = application/x-java-jnlp-file
    - Description = Java Web Start
    - Extension = jnlp

In the section "When a file of this type is encountered" select **Open it with**. Enter the path to javaws on your AIX or Linux system. The most common path is /usr/java5/jre/javaws/javaws. Click **OK** to close the dialog used for editing the entry. Click **OK** to close the Mimetypes interface.

## Using Internet Explorer or Firefox on Windows (with IBM Tivoli Integrated Portal)

If you are using Internet Explorer 7, Firefox 2.0, or Firefox 3.0 on Windows, follow these steps:

- 1. Install IBM 1.5 JRE.
- **2**. Start an Internet Explorer or Firefox Web browser, and type the following information in the address bar:

#### http://hostname:port

Where *hostname* defines the server that is running Tivoli Integrated Portal such as the server name or IP address and *port* defines the port number for Tivoli Integrated Portal. If the default port was accepted during the installation of Tivoli Integrated Portal, the port number is 16310. Contact your Tivoli Storage Productivity Center administrator if you need to verify the host name and port number.

**3**. On the IBM Tivoli Integrated Portal logon page, type your Tivoli Storage Productivity Center ID and password in the **User ID** and **Password** boxes and click **Log in**.

**Note:** To have administrator permissions in IBM Tivoli Integrated Portal, you must log on as a member of the Tivoli Storage Productivity Center superuser role.

- 4. In the IBM Tivoli Integrated Portal navigation tree, click Tivoli Storage Productivity Center.
- 5. On the Tivoli Storage Productivity Center portlets page, click **Start Storage Productivity Center**.
- 6. For Internet Explorer 7, the browser uses Java Web Start to open the launch.jnlp file and continue with the download and launch of Tivoli Storage Productivity Center.

For Firefox, you will see a pop-up window asking what you would like to do with the launch.jnlp file. Select **Open with**. Ensure that the program being used to open the file is Java Web Start. Check the box for **Do this automatically for files like this from now on**. Click **OK**.

7. Java Web Start should continue with the download and launch of the Tivoli Storage Productivity Center GUI.

## Using Firefox on Linux (with IBM Tivoli Integrated Portal)

If you are using Firefox 2.0 or Firefox 3.0 on Linux, follow these steps:

- 1. Install IBM 1.5 JRE.
- 2. Start the Firefox Web browser, and type the following information in the address bar:

http://hostname:port

Where *hostname* defines the server that is running Tivoli Integrated Portal such as the server name or IP address and *port* defines the port number for Tivoli Integrated Portal. If the default port was accepted during the installation of Tivoli Integrated Portal, the port number is 16310. Contact your Tivoli Storage Productivity Center administrator if you need to verify the host name and port number.

**3**. On the IBM Tivoli Integrated Portal logon page, type your Tivoli Storage Productivity Center ID and password in the **User ID** and **Password** boxes and click **Log in**.

**Note:** To have administrator permissions in IBM Tivoli Integrated Portal, you must log on as a member of the Tivoli Storage Productivity Center superuser role.

4. In the IBM Tivoli Integrated Portal navigation tree, click Tivoli Storage Productivity Center.

- 5. On the Tivoli Storage Productivity Center portlets page, click **Start Storage Productivity Center**.
- 6. For Firefox, you will see a pop-up window asking what you would like to do with the launch.jnlp file. Select **Open with**. Ensure that the program being used to open the file is Java Web Start. Check the box for **Do this automatically for files like this from now on**. Click **OK**.
- 7. Java Web Start should continue with the download and launch of the Tivoli Storage Productivity Center GUI.

## Using Firefox on AIX (with IBM Tivoli Integrated Portal)

If you are using Firefox 2.0 on AIX follow these steps:

- 1. Install IBM 1.5 JRE.
- 2. Download a MIME type editor extension for Mozilla Firefox 2.0 (for example, Mime Edit 0.60) on the AIX system. To download the MIME editor, go to https://addons.mozilla.org/en-US/firefox/addon/4498.
- 3. Start the Firefox browser.
- 4. Click **File > Open File**.
- 5. Go to the mime\_edit-0.60-fx+tb.xpi file and click **Open**. Firefox guides you through the installation of the extension and then tells you to restart Firefox.
- 6. When you have restarted Firefox, click **Tools > Mimetypes**.
- 7. If there is an entry for "application/x-java-jnlp-file" in the File types list, select it and click Edit. In the section "When a file of this type is encountered" select **Open it with**. Enter the path to javaws on your AIX or Linux system. The most common path is /usr/java5/jre/javaws/javaws. Click **OK** to close the dialog used for editing the entry. Click **OK** to close the Mimetypes interface.
- 8. If there is no entry for "application/x-java-jnlp-file" in the File types list, click **New Type**. Enter the following values:
  - MIME Type = application/x-java-jnlp-file
  - Description = Java Web Start
  - Extension = jnlp

In the section "When a file of this type is encountered" select **Open it with**. Enter the path to javaws on your AIX or Linux system. The most common path is /usr/java5/jre/javaws/javaws. Click **OK** to close the dialog used for editing the entry. Click **OK** to close the Mimetypes interface.

**9**. Start the Firefox Web browser, and type the following information in the address bar:

## http://hostname:port

Where *hostname* defines the server that is running Tivoli Integrated Portal such as the server name or IP address and *port* defines the port number for Tivoli Integrated Portal. If the default port was accepted during the installation of Tivoli Integrated Portal, the port number is 16310. Contact your Tivoli Storage Productivity Center administrator if you need to verify the host name and port number.

**10**. On the IBM Tivoli Integrated Portal logon page, type your IBM Tivoli Storage Productivity Center ID and password in the **User ID** and **Password** boxes and click **Log in**.

**Note:** To have administrator permissions in IBM Tivoli Integrated Portal, you must log on as a member of the Tivoli Storage Productivity Center superuser role.

- 11. In the IBM Tivoli Integrated Portal navigation tree, click Tivoli Storage Productivity Center.
- 12. On the Tivoli Storage Productivity Center portlets page, click **Start Storage Productivity Center**.

## **Configuring tracing**

Configure tracing for the Data server, agent, scheduler, Device server, and GUI by setting the debug level and log file characteristics. The level of information saved in a log file is determined by the tracing level. Tracing settings can only be changed by users with administrator authority.

To configure tracing for IBM Tivoli Storage Productivity Center, complete the following steps:

- 1. In the navigation tree pane, expand Administrative Services → Services → Data Server.
- 2. Right-click on one of the following components:
  - Server
  - Agent
  - Scheduler
  - Device
  - GUI

Click Configure Tracing.

**3**. In the Server Tracing Configuration window, check the **Enable Trace** check box. Specify additional tracing options:

**Level** Select the level of debugging you want to perform. Select one of the following:

- DEBUG\_MIN Provides minimal information on errors. This is the default value.
- DEBUG\_MID Provides more information on errors.
- DEBUG\_MAX Lists all debugging trace information.

### Maximum number of files

Select the maximum number of trace files that will be created. When the maximum number of files has been reached, tracing will rollover and start writing to the first file. (default is 5)

The value in this field also applies to Data Server's other services for which tracing is enabled.

## Maximum File Size (kilobytes)

Select the maximum size of each log file. When the current trace file has reached its maximum capacity, tracing will continue to the next available trace file as defined in the Maximum Number of Files field. (default is 20 MB).

## 4. Click OK.

Tracing can be turned off by de-selecting the **Enable Trace** option in the Server Tracing Configuration window.

## Configuring the DB2 JDBC driver

This topic describes how to configure the DB2 JDBC driver for the Tivoli Common Reporting component.

To configure the DB2 JDBC driver, follow these steps:

- 1. Stop the IBM Tivoli Integrated Portal.
- 2. Copy the following files:
  - db2jcc.jar
  - db2jcc\_license\_cu.jar

Copy the files from this directory:

C:\Program Files\IBM\SQLLIB\java (for Windows) <usr or opt>/IBM/SQLLIB/java (for UNIX)

To this directory:

C:\Program Files\IBM\tivoli\tip\products\tcr\ lib\birt-runtime-2\_2.1\ReportEngine\plugins\ org.eclipse.birt.repot.data.oda.jdbc\_2.2.1\_r22x\_v20070919\ dirvers

**3**. Start the IBM Tivoli Integrated Portal.

## Configuration guidelines for 500 or more agents

This topic provides information if you have 500 or more agents in IBM Tivoli Storage Productivity Center.

If you have 500 or more agents for the Data Server, follow these steps.

**Note:** Probes can overwhelm Data Server resources, because by default, they can return information all at once.

- 1. Probe the machines at least once a day (or more depending on when you want to test for alert conditions (other than directory alerts, quotas, or constraints).
- 2. If you use anything but the "ALL" groups (ALL file systems, ALL computers), you will need to manually populate the groups.
- **3**. Always run a probe before a scan. Set the following parameters in the server.config file:

#### MaxConnections=1200

The default is 500. Agents can have multiple connections to the server.

#### routerThreads=3 (max)

Incoming connections need to be routed to the correct Data Manager "service" queue and can stack up behind this thread. You can watch this by watching the connections in the "server service" and the "agent service" in the GUI. The server service runs the router and the agent service is where the connections will queue up once routed to be saved by any of three threads here to the repository.

4. Set the following parameter in the Scheduler.config file:

#### MaxSubmitthreads=8

This tells how many threads are used to tell the agents to start a job. Agent connections can queue up the scheduler service. After a job is run, the agent makes a connection to communicate with this thread to give it the job status.

## Using a master image to set up Common agent machines

If you use a master operating system image to deploy new servers in your environment, you can include the IBM Tivoli Storage Productivity Center agents on that master image, so that the Tivoli Storage Productivity Center agents will start up and register with the Tivoli Storage Productivity Center server automatically upon deployment.

It is assumed that the copied images will point to the existing Agent Manager and the Tivoli Storage Productivity Center server machine. If you intend to deploy machines with Tivoli Storage Productivity Center agents and have them point to different Tivoli Storage Productivity Center servers, see "Registering the Data agent with a different server" on page 449.

The default agent directory is:

- For Windows: C:\Program Files\IBM\TPC\ca
- For UNIX: /opt/tivoli/ep
- For AIX: /usr/tivoli/ep

Follow these instructions to prepare the master image for the Tivoli Storage Productivity Center agents:

- 1. Install the Data agent. This will also install the Common agent.
- 2. Install the Fabric agent. The Fabric agent requires a SAN connected to an HBA to be functional in production.
- In the endpoint.properties file, change the following: agent.ssl.truststore.download=true

The endpoint.properties file is in this directory: <agent install dir>/config/

4. Verify that the agent is able to register with the Agent Manager. Check the msgAgent.log file for these messages:

BTC1025I REG: Agent is now attempting to register and obtain security credentials from Agent Registration Service amserver.yourcompany.com at port 9511. BTC1022I REG: Registration succeeded after 1 attempts.

The msgAgent.log file is in this directory:
<agent\_install\_dir>/logs/

- 5. Stop the Common agent.
  - For Windows, click Start > Settings > Control Panel > Administrative Tools > Services. Stop the following service:

IBM Tivoli Common Agent <directory>

<directory> is where the Common agent is installed. The default is: <TPC\_install\_dir>\ca.

- For UNIX: cd /opt/Tivoli/ep ./endpoint.sh stop
- 6. Set the GUID on the Common agent machine to all hexadecimal zeros. This causes the agent to register with the Agent Manager and set a new GUID.
  - For Windows:

For UNIX:

- 7. Create an empty "PROBE\_ME" file in the Data agent directory. (Case is important here with no file extension.)
  - For Windows:

C:\Program Files\IBM\TPC\ca\subagents\TPC\Data

```
• For UNIX:
```

/opt/tivoli/ep/subagents/TPC/Data

- 8. Delete the contents of the <agent\_install\_dir>/cert directory. This causes the agent to download new certificates.
- 9. Delete the contents of the <agent\_install\_dir>/logs directory. This clears existing messages so you will be able to view new messages.
- **10**. If any other software is installed after this point, you will need to verify that the GUID still has all hexadecimal zeros.
- **11**. Make the master image copies from this Tivoli Storage Productivity Center agent machine.
- 12. When a new machine is preloaded with this image and started, it should:
  - Register with the Agent Manager
  - Create a unique GUID
  - Register both the Data agent and Fabric agent with Tivoli Storage Productivity Center.

Check that the Data agent and Fabric agent show up in **Administrative Services** → **Agents**. You will need to refresh the views.

You should also have a data probe job set up to use the Default Computer Group. This will automatically include any new Data agents that get added. You should also have a fabric probe job that uses the Default Fabric Group to automatically probe any new fabrics.

# Configuring IBM Tivoli Storage Productivity Center for batch reports on UNIX or Linux

This section describes how to configure IBM Tivoli Storage Productivity Center for creating batch reports on UNIX or Linux.

If you want to run batch reports on a Linux or UNIX agent machine, follow these steps:

- 1. Make sure that the agent machine can connect to an X server. The X server must be installed and running.
- 2. Install the agent.
- 3. On the Linux or UNIX agent on which you want to generate PDF or HTML charts, you need to edit <TPC\_install\_directory>/ca/config/ nonstop.properties. Add the following parameter to the nonstop.properties file:

-Djava.awt.headless=true

After editing the file, the parameter list should look like this:

parameter="-cp :lib/smf.jar:lib/SMFCoreMsg\_en.jar:lib/ep\_system.jar

- -Dcom.tivoli.agent.nonstop.launcher=true
- -Dcom.ibm.osg.smf.bundledir=installedBundles
- -Djlog.noLogCmd=true
- -Djava.awt.headless=true com.tivoli.agent.system.SMFLauncher"
- 4. Save the file. Restart the machine to make the changes effective.

## Configuring LUN provisioning for Sun Solaris

IBM Tivoli Storage Productivity Center for Data provides a file system extension feature that can be used to automatically increase file system capacity for managed hosts when utilization reaches a specified level. This function allows for the automatic provisioning of IBM Enterprise Storage Server(Tivoli Storage Enterprise Storage Server, DS6000, DS8000) LUNs when there is not enough space available in a volume group to extend a file system. This section provides information on LUN provisioning for Sun Solaris.

LUNs can be provisioned for file system hosts running Sun Solaris, but the hosts must be configured to avoid a reboot after provisioning. Before you install the Data agent, you must do the following:

- 1. Assign Tivoli Storage Enterprise Storage Server, DS6000, or DS8000 LUNs to Sun Solaris Host Bus Adapters (HBAs).
- 2. Modify the HBA configuration file to include persistent name binding.
- **3.** Modify the SCSI Disk configuration file to allow the maximum number of LUNs.
- 4. If you are using multipathing, ensure that Tivoli Storage Enterprise Storage Server, DS6000, or DS8000 multipaths are detected by the Veritas Dynamic Multipathing (VxDMP) utility.

This section provides basic instructions for performing these configuration steps. For detailed information, see the HBA and VxDMP documentation.

# Assigning Tivoli Storage Enterprise Storage Server, DS6000, or DS8000 LUNs to Sun Solaris HBAs

This section provides information on assigning Tivoli Storage Enterprise Storage Server, DS6000, or DS8000 LUNs to Sun Solaris HBAs.

You must assign at least one Tivoli Storage Enterprise Storage Server, DS6000, or DS8000 LUN to each HBA on the Sun Solaris host.

If you are using multipathing, there are different ways to configure either the host and Tivoli Storage Enterprise Storage Server, DS6000, or DS8000. For example:

- For an Tivoli Storage Enterprise Storage Server, DS6000, or DS8000 without internal multipath configuration, assign the same LUNs to the World Wide Port Node (WWPN) of each HBA.
- For an Tivoli Storage Enterprise Storage Server, DS6000, or DS8000 with internal multipath configuration, assign the LUNs to the WWPN of one HBA or assign the same LUNs to the WWPNs of two or more HBAs.
## Modifying the HBA configuration file

The HBA configuration file must be modified to include Persistent Name Binding on HBAs and targets so that both the controller and target numbers will remain the same across system reboots. This section provides information on what to modify in the configuration file.

The HBA configuration file (for example, qla2200.conf) must be modified to include Persistent Name Binding on HBAs and targets so that both the controller and target numbers will remain the same across system reboots. You must reboot the system with the new configuration for the changes to take effect.

QLogic QLA2200 and QLA2300 HBAs have been tested for use with IBM Tivoli Storage Productivity Center. You can use the QLogic SANblade Control FX (**scfx**) application to modify the configuration file for these HBAs. The **scfx** application is included as part of the device driver installation package. The **scfx** application is installed in the /opt/QLogic\_Corporation/SANblade\_Control\_FX directory.

## Setting Persistent Name Binding for QLA2200 and QLA2300 HBAs using scfx

This section describes how to set Persistent Name Binding in the HBAs using **scfx** for LUN provisioning under Sun Solaris.

Follow these steps:

- Install the QLogic HBA Driver, Common API Library, and QLogic SANblade Control FX (scfx) application if you have not already done so. For installation instructions, see the SANblade 2200 Series User's Guide or SANblade 2300 Series User's Guide. After these packages are installed successfully, restart and reconfigure the system using the reboot -- -rv command.
- 2. After the system is rebooted, use **scfx** to configure Persistent Bind on HBAs and Targets in the /kernel/drv/qla2xxx.conf file.
  - a. Start the scfx application. For example:

# /opt/QLogic\_Corporation/SANblade\_Control\_FX/scfx

The main window of the **scfx** application consists of three sections:

## Menu Bar

The Menu Bar provides three options: File, Tools, and Help.

## HBA Tree

The HBA Tree displays the host with its connected adapters (HBAs), devices and LUNs. The HBAs are displayed with a model name and instance number. For example, Adapter 2200 (Instance #0). If a device is connected to an HBA, it has a plus sign (+) to the left of the HBA, which can be expanded to view the list of attached devices. The devices are listed with their World Wide Port Names (WWPN).

Click the plus sign next to a device to expand the tree to show all the LUNs in that device. For a RAID device, such as an Tivoli Storage Enterprise Storage Server, DS6000, or DS8000, there are multiple LUNs per device.

**Note:** Expand all the devices to search the Tivoli Storage Enterprise Storage Server, DS6000, or DS8000 LUNs assigned to the system and

note the WWPN of the target device. This information is needed to identify the SCSI Target ID assigned or specified for the Persistent Bind Targets Setting.

## **Tabbed Pages**

The contents of the Tabbed Pages will change depending on what is currently selected in the HBA Tree.

b. Select an HBA.

Select an adapter in the HBA Tree. The Tabbed Pages will show the **HBA Information**, **HBA Options**, **Target Settings**, **Boot Device**, **Diagnostics**, and **Utilities** tabs.

c. Select the Persistent Bind HBA Setting.

Click the **HBA Options** tab. In the **Select Parameter Section** drop down box, select **Advanced Host Parameters**. Select the check box for **Persistent Bind HBA**. Click **Save**.

d. Select the Persistent Bind Target Setting.

Click the **Target Settings** tab. Select the check box for each target in the **Bind** column. If the check boxes are already checked and grayed out, proceed to the next step. In the **Target ID** column, you can either accept the pre-selected SCSI Target ID or change to a different value. Each SCSI target ID must be unique and range from 0 to 255.

**Note:** Write down the selected Target ID for each Tivoli Storage Enterprise Storage Server subsystem device. Click **Save**.

- e. Repeat Steps b through d for the next HBA.
- f. Exit the **scfx** application.

From the **Menu Bar**, select **File** | **Exit**. A Reboot Reminder dialog will appear. Click **OK** to exit.

3. Restart and reconfigure the system using the reboot -- -rv command.

## Modifying the SCSI disk configuration file

You must configure the SCSI disk configuration file for the maximum number of LUNs per target for LUN provisioning for Sun Solaris.

You must configure the SCSI disk (sd.conf) configuration file for the maximum number of LUNs (256) per target. The system must then be rebooted with the new configuration for the changes to take effect. Follow these steps:

- 1. Identify the SCSI Target ID assigned to the Tivoli Storage Enterprise Storage Server.
- 2. Edit the /kernel/drv/sd.conf file to include all the possible target and LUN mappings for the RAID device. For example, assume the SCSI Target ID assigned for an Tivoli Storage Enterprise Storage Server is 2. You will want to allow up to 256 LUNs (0 255) for this target as follows:

```
name="sd" class="scsi" target=0 lun=0;
name="sd" class="scsi" target=1 lun=0;
name="sd" class="scsi" target=2 lun=0;
name="sd" class="scsi" target=2 lun=1;
name="sd" class="scsi" target=2 lun=2;
:
:
name="sd" class="scsi" target=2 lun=253;
name="sd" class="scsi" target=2 lun=254;
name="sd" class="scsi" target=2 lun=255;
```

```
name="sd" class="scsi" target=3 lun=0;
name="sd" class="scsi" target=4 lun=0;
:
name="sd" class="scsi" target=253 lun=0;
name="sd" class="scsi" target=254 lun=0;
name="sd" class="scsi" target=255 lun=0;
```

In this example, the system can detect up to 256 targets with 1 LUN (for example, multiple RAID devices with a total of 256 LUNs) and up to 256 LUNs for target 2 (for example, a RAID device with a total of 256 LUNs).

3. Restart and reconfigure the system using the **reboot** -- -**rv** command.

## Checking for Tivoli Storage Enterprise Storage Server, DS6000, or DS8000 multipaths in VxDMP

If you are using IBM Tivoli Storage Enterprise Storage Server, DS6000, or DS8000 LUNs with multipaths, you must ensure that all the paths are detected by Veritas Dynamic MultiPathing (VxDMP) utility. This section provides information on how to check for multipathing in the VxDMP utility.

The VxDMP utility is an administrative interface to the Veritas Volume Manager (VxVM) Dynamic Multipathing (DMP) facility. It lists the paths under a DMP device, gets the DMP device corresponding to a path, lists all the disk controllers on the system, lists all the paths through a host disk controller, lists all the DMP nodes through a disk array, and enables or disables a host disk controller on the system. For more information, and detailed instructions, see the VxDMP documentation.

To list all disk controllers on the system, enter the following: # vxdmpadm listctlr all

The following sample output shows that controllers c3 and c4 are connected to the IBM Tivoli Storage Enterprise Storage Server with an Enclosure Type of IBM\_SHARK and an Enclosure Name of IBM\_SHARK0.

CTLR-NAME	ENCLR-TYPE	STATE	ENCLR-NAME
c1	Disk	ENABLED	Disk
c3	IBM_SHARK	ENABLED	IBM_SHARK0
c4	IBM_SHARK	ENABLED	IBM_SHARK0

To list all subpaths for controller c3, enter the following command: # vxdmpadm getsubpaths ctlr=c3

The following sample output shows that the **dmpnodename** is the same as the device name for each Tivoli Storage Enterprise Storage Server LUN:

NAME	STATE	PATH-TYPE	DMPNODENAME	ENCLR-TYPE	ENCLR-NAME
======================================	ENABLED	-	c3t4d0s2	IBM_SHARK	IBM_SHARK0
c3t4d1s2	ENABLED	-	c3t4d1s2	IBM_SHARK	IBM_SHARK0

To list all subpaths for controller c4, enter the following command:

# vxdmpadm getsubpaths ctlr=c4

The following sample output shows that the **dmpnodename** for each Tivoli Storage Enterprise Storage Server LUN is from controller c3. This means that VxDMP will

refer to the Tivoli Storage Enterprise Storage Server, DS6000 or DS8000 LUNs as devices from controller c3 and mask devices on controller c4 from VxVM:

NAME	STATE	PATH-TYPE	DMPNODENAME	ENCLR-TYPE	ENCLR-NAME
================					=======
c4t4d0s2 c4t4d1s2	ENABLED ENABLED	-	c3t4d0s2 c3t4d1s2	IBM_SHARK IBM_SHARK	IBM_SHARK0 IBM_SHARK0

## How to import a Storage Resource agent's authentication information

The Storage Resource agent is installed as a non-daemon or daemon process. IBM Tivoli Storage Productivity Center stores the authentication information to connect to the host on which the Storage Resource agent has installed for the non-daemon agent. This authentication information can be changed depending on the environment.

To change a Storage Resource agent's authentication information (for non-daemon service), follow these steps:

- 1. Export the Storage Resource agent's authentication information. See "Exporting a Storage Resource agent list" on page 448.
- 2. The data file exported contains information such as the host name, user ID, password, certificate location, and passphrase for every agent selected. The information is separated by the pipe character (1). For example:

<agent\_host>|<user>|<password>|<certificate>|<passphrase>

You can update the password or passphrase in encrypted format or plain text format. If you want to update the password or passphrase in encrypted format, then you can use the **tpctool**. For example go to this directory and run the **tpctool**:

cd <TPC\_install\_directory>/cli
tpctool encrypt <string\_to\_be\_encrypted>

This generates an encrypted string. Place this string in the data file to be imported and add @ENC@ to the end of the encrypted string. For example:

<agent\_host>|usera|encrypted\_password@ENC@|certificate| encrypted\_passphrase@ENC@

encrypted\_password is the encrypted string for the password and encrypted\_passphrase is the encrypted string for the passphrase.

3. Import the data file. See "Updating a Storage Resource agent list" on page 448.

## Configuring Tivoli Storage Productivity Center for DS8000 LDAP support

You must configure Tivoli Storage Productivity Center to use LDAP for single sign-on support for the DS8000 R4.2.

## **Overview**

Configuring Tivoli Storage Productivity Center and DS8000 for single sign-on involves these general steps:

## For Tivoli Storage Productivity Center

- Extract the certificate. This certificate is used for securing communication between the Authentication Client on the HMC and the Authentication Service (server component) on Tivoli Storage Productivity Center.
- 2. Create a trust store which includes the certificate from step 1.
- 3. You will need to know the URL for the Authentication Service.

## For DS8000

- 1. Create a Storage Authentication Service (SAS) policy with information collected from Tivoli Storage Productivity Center and the LDAP server.
- **2**. Test the Storage Authentication Service policy using a valid LDAP user mapped to a DS8000 user role in the policy.
- **3**. Activate the Storage Authentication Service policy using a valid LDAP user mapped to the DS8000 administrative user role in the policy.

## Procedure for configuring Tivoli Storage Productivity Center

This procedure assumes that Tivoli Storage Productivity Center is set up with the LDAP repository. Follow these steps:

1. You will need to know the URL for the Authentication Service.

**Note:** An example of the Authentication Service URL is: https://<TIP\_server\_host>:16311/TokenService/services/Trust

Here is an example:

https://tpcserver1.storage.mycompany.com:16311/TokenService/services/Trust

The port for the Authentication Service (16311) is one plus the default Tivoli Integrated Portal port (16310). If you change the default port, for example, 17522, then the port number to use for the Authentication Service is one plus the Tivoli Integrated Portal port. In this example, the port number would be:

https://tpcserver1.storage.mycompany.com:17523/TokenService/services/Trust

- 2. Create the trust store.
  - a. Open the IBM Tivoli Integrated Portal console.
  - b. Go to the Personl Certificates page for the Default Keystore. Click Security
     > SSL certificate and key management > Key stores and certificates > NodeDefaultKeyStore > Personal Certificates. On this page, select the default certificate and click Extract. On the resulting page, enter the following information:

## Certificate file name

Enter a file name for the extracted certificate. This file will automatically get created in <TIP\_install\_directory>/profiles/ TIPProfile/etc/. For Windows, the default directory is C:\<TIP\_install\_directory>\profiles\TIPProfile\etc\. Click **OK**.

- c. Create the trust store file and import the certificate into the trust store file.
  - 1) Launch the ikeyMan tool.

For example on Windows:

c:\Program Files\IBM\tivoli\tip\bin\ikeyman.bat

2) Click **Key Database File > New**. On the New panel, enter the following information and click **OK**:

## Key database type

Enter or leave the default JKS.

## File Name

Enter a file name. For example, enter tpc\_ess.jks.

**Note:** The default location is:

c:\Program Files\IBM\tivoli\tip\bin\

Location

Enter a location. For example, enter c:\tpc\. Click **OK**.

- **3)** The next panel prompts you to specify a password for this trust store. Specify a password that you can remember. Click **OK**.
- On the next panel, click Add. This opens the Add CA certificate from a file panel. Click Browse and select the certificate file you created in step 1b. Click OK.
- 5) You will see a prompt to specify a label. Provide any label. An example of a label is: ESS\_Cert. Click **OK**.
- 6) ESS\_Cert will now be one of the certificates listed.
- 7) Exit the **ikeyman** tool and locate the trust store file (for this example, tpc\_ess.jks). You will need this trust store file and the password for it while configuring the LDAP-based policy on DS8000.
- **3.** Find the user ID and password that is used in LDAP to use for the DS8000 Storage Authentication Service policy configuration page.

This is the user ID used for authenticating with the Authentication Service. It can be any user ID in LDAP, or a user ID that is also used by Tivoli Storage Productivity Center. This user ID is used as the "Application Client User ID" for a Storage Authentication Service policy on the DS8000.

4. Find the name of a group in LDAP with which you can login to Tivoli Storage Productivity Center and the DS8000. You would use this LDAP group on the DS8000 also, for mapping to DS8000 roles.

You can go to the Tivoli Storage Productivity Center **Role-to-Group Mapping** node to find out which LDAP group is mapped to the role in Tivoli Storage Productivity Center.

To find the LDAP group name, open the Tivoli Storage Productivity Center GUI and click **Tivoli Storage Productivity Center > Configuration > Role-to-Group Mapping**.

The information gathered in steps 1, 2, 3, and 4 is used on the DS8000 Storage Authentication Service policy creation page.

5. Configure DS8000 R 4.2.

## Configuring DS8000 for LDAP authentication

Follow these steps:

- 1. Open the DS8000 GUI using the administrative user ID and password. Enter the User Name and Password. Click **OK**.
- On the DS8000 Storage Manager Welcome page, click Real-time manager > Monitor System > User Administration.
- 3. On the User and Authentication Policy Administration Summary page, select a Complex Name. Under the Select action menu, select **Create Storage Authentication Service Policy**.
- 4. The Authentication Service Configuration page is displayed. Enter the following information:
  - Policy Name
  - Authentication Service URL (primary)

- Authentication Service Client User ID
- Authentication Service Client Password
- Confirm Authentication Service Client Password

Click Next.

**Note:** An example of the authentication URL is: https://<TIP\_server\_host>:16311/TokenService/services/Trust

Here is an example:

https://tpcserver1.storage.mycompany.com:16311/TokenService/services/Trust

The port for the Authentication Service (16311) is one plus the default Tivoli Integrated Portal port (16310). If you change the default port, for example, 17522, then the port number to use for the Authentication Service is one plus the Tivoli Integrated Portal port. In this example, the port number would be: https://tpcserver1.storage.mycompany.com:17523/TokenService/services/Trust

- **5**. The Truststore file Information page is displayed. Enter the following information:
  - Truststore File Location
  - Truststore File Password
  - Confirm Truststore File Password

Click Next.

- **6**. The Map External Users and User Groups to DS8000 User Roles page is displayed. Enter the following information:
  - External Entity Name
  - External Entity Type
  - DS8000 User Role

Click **Add**. The entry is entered in the table at the bottom of this page. Select the entry you created and click **Next**.

- 7. The Verification page is displayed. Verify the information and click Next.
- 8. The Summary page is displayed. Click **Activate the Policy** if you want to activate the policy immediately. If you want to test the policy before activating it, do not select **Activate the Policy** and just click **Finish** to create the policy. This scenario assumes you want to test the policy before activating it. You will see a message dialog indicating whether the policy was successfully created or not. If the policy was successfully created, close the message dialog.
- **9**. The Manage Authorization Policy page is displayed. Select a policy. Under the Select action menu, click **Test Authentication Policy**.
- **10**. The Test Storage Authentication Service Policy page is displayed. Enter the following information:
  - External User Name
  - External User Password

Provide an LDAP user ID and password for External User Name and External User Password. The user ID must already be mapped to a valid DS8000 user role in the Storage Authentication Service policy. This user ID does not have to be in the Administrator group. Click **OK**.

11. The Manage Authentication Policy page is displayed. Select the policy you want. Under the Select action menu, click **Activate Authentication Policy**.

- **12.** The Activate Storage Authentication Service Policy page is displayed. Enter the following information:
  - External User Name
  - External User Password

Provide an LDAP user ID and password for External User Name and External User Password. The user ID must already be mapped to a valid DS8000 user role in the Storage Authentication Service policy. This user ID must be in the Administrator group. Click **OK**. The policy will now be activated. Close the page.

## Configuring multiple Tivoli Storage Productivity Center servers with a single DS8000 R4.2

You can configure multiple Tivoli Storage Productivity Center servers to use LDAP for single sign-on support for the DS8000 R4.2.

## Procedure for configuring multiple Tivoli Storage Productivity Center servers

Follow these steps:

- Configure one server as described in "Configuring Tivoli Storage Productivity Center for DS8000 LDAP support" on page 336. We will call this server TPC\_server1.
- 2. Install a second Tivoli Storage Productivity Center server with the same LDAP information as the first server. We will call this second server TPC\_server2.
- Open a command prompt window. Go to the following directory: <TIP installation directory>/bin
- 4. Run the **wsadmin** command to export LTPA keys from TPC\_server1 into a file on TPC\_server2.

```
wsadmin -user <TIP_admin_ID> -password <TIP_admin_password> -lang jython
-port <TIP_SOAP_port> -host <TPC_server1_hostname or IP_address>
-f "<TPC_install_dir on TPC_server2>/tip/scripts/exportLTPAKeys.py"
"<LTPA_keys_file_name>" <1tpa_Keys_Password>
```

An example is:

```
c:\Program Files\IBM\Tivoli\TIP\bin>wsadmin -user tpcsuperuser
-password tpcsuperuser -lang jython
-port 16313 -host 9.56.98.41
-f "c:/program files/ibm/tpc/tip/scripts/exportLTPAKeys.py"
"c:/share/ltpaKeys_serv1" ltpa123
```

This creates a file named ltpaKeys\_serv1 containing the LTPA keys of TPC\_server1. The LTPA keys will be imported into TPC\_server2.

Note: Use forward slashes.

5. In the same command window, run the following command to import the LTPA keys into IBM Tivoli Integrated Portal and then into the Device server.

wsadmin -user <TIP\_admin\_ID> -password <TIP\_admin\_password> -lang jython -f "<TPC\_install\_dir on TPC\_server2>/tip/scripts/importLTPAKeys.py" "<LTPA\_keys\_file\_name>" <1tpa\_Keys\_Password>

An example is:

c:\Program Files\IBM\Tivoli\TIP\bin>wsadmin -user tpcsuperuser -password tpcsuperuser -lang jython -f "c:/program files/ibm/tpc/tip/scripts/importLTPAKeys.py" "c:/share/ltpaKeys\_serv1" ltpa123

Note: Use forward slashes.

6. Change to the Device server WebSphere bin folder and run the same command there.

c:\Program Files\IBM\Tivoli\TIP\bin>wsadmin -user tpcsuperuser -password tpcsuperuser -lang jython -f "c:/program files/ibm/tpc/tip/scripts/importLTPAKeys.py" "c:/share/ltpaKeys\_serv1" ltpa123

Note: Use forward slashes.

7. The LTPA keys in TPC\_server1 and TPC\_server2 are now synchronized. You will be able to perform a successful single sign-on launch from TPC\_server2 to the DS8000 R4.2. The DS8000 uses the same policy that was set up when you set up TPC\_server1.

The same steps can be used to launch the same DS8000 from any number of IBM Tivoli Storage Productivity Center servers.

**Note:** This is not a high-availability setup because the policy in DS8000 is still pointing to only one Embedded Security Services, which is that of TPC\_server1.

## Disabling Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication

If you have a system with 4-8 GB of RAM, you cannot run Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication at the same time. You must disable Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication after installation.

If you want to run only Tivoli Storage Productivity Center, then you can disable Tivoli Storage Productivity Center for Replication. To disable Tivoli Storage Productivity Center for Replication, follow these steps:

#### **On Windows**

To stop the Tivoli Storage Productivity Center for Replication server, go to **Start > Settings > Control Panel > Administrative Tools > Services**. Stop the following service:

IBM WebSphere Application Server V6.1 - CSM

If you want to set your system so that Tivoli Storage Productivity Center for Replication does not start up on system reboot, you must disable this service.

#### On Linux and AIX

To stop the Tivoli Storage Productivity Center for Replication server, run this command from a command prompt window:

/opt/IBM/replication/eWAS/profiles/CSM/bin/stopServer.sh server1
-username <username> -password <password>

Where <username> is the user ID and <password> is the password for this user ID.

If you want to set your system so that Tivoli Storage Productivity Center for Replication does not start up on system reboot, you must go into /etc/inittab and remove the line that starts up Tivoli Storage Productivity Center for Replication.

If you want to disable Tivoli Storage Productivity Center, follow these steps:

## **On Windows**

Go to **Start > Settings > Control Panel > Administrative Tools > Services** and stop the following services:

- IBM WebSphere Application Server V6.1 DeviceServer
- IBM Tivoli Storage Productivity Center Data Server
- IBM Tivoli Common Agent <directory>
  - (<directory> is where the common agent is installed. The default is <TPC\_install\_directory>\ca)
- IBM Tivoli Storage Resource Agent <directory>
   (<directory> is where the Storage Resource Agent is installed. The
   default is <TPC\_install\_directory>\agent)
- Tivoli Integrated Portal TIPProfile Port <xxxxx>
- (<xxxxx> indicates the port specified during installation. The default port is 16310.)
- IBM ADE Service (Tivoli Integrated Portal registry)

#### Note:

- Stop Tivoli Integrated Portal and IBM ADE Service only if no other applications are using these services.
- If you want to set your system so that Tivoli Storage Productivity Center does not start up on system reboot, you must disable these services.

#### **On Linux**

To stop the Tivoli Storage Productivity Center services, run these commands in a command prompt window:

Data server: /<usr or opt>/IBM/TPC/data/server/tpcdsrv1 stop Device server: /<usr or opt>/IBM/TPC/device/bin/linux/stopTPCF.sh Common agent: /<usr or opt>/IBM/TPC/ca/endpoint.sh stop Storage Resource agent: /<usr or opt>/IBM/TPC/agent/bin/agent.sh stop

#### On AIX

To stop the Tivoli Storage Productivity Center services, run these commands in a command prompt window:

Data server: stopsrc -s TSRMsrv1 Device server: /<usr or opt>/IBM/TPC/device/bin/aix/stopTPCF.sh Common agent: /<usr or opt>/IBM/TPC/ca/endpoint.sh stop Storage Resource agent: /<usr or opt>/IBM/TPC/agent/bin/agent.sh stop

#### Stop Tivoli Integrated Portal on AIX and Linux

To stop Tivoli Integrated Portal, run this command in a command prompt window:

<install\_directory>\tip\profiles\TIPProfile\bin\stopServer server1
-username <tipadmin>
-password <password>

Where <tipadmin> is the administrator user ID and <password> is the administrator password. Wait for the server to complete the operation.

To stop the IBM ADE Service, run this command in a command prompt window:

**Note:** Stop Tivoli Integrated Portal and IBM ADE Service only if no other applications are using these services.

## Chapter 4. Upgrading and migrating the IBM Tivoli Storage Productivity Center family

You can upgrade previous TotalStorage Productivity Center 3.1.3 or later releases to Tivoli Storage Productivity Center version 4.1. You can migrate previous IBM TotalStorage Productivity Center for Replication version 3.x to Tivoli Storage Productivity Center version 4.1. This section provides information about upgrading and migrating.

## **Overview**

When you upgrade Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication, if a component fails to upgrade, then just the component will not be upgraded.

If Tivoli Storage Productivity Center exists but Tivoli Storage Productivity Center for Replication does not, then this upgrade will be a fresh installation of Tivoli Storage Productivity Center for Replication and an upgrade of Tivoli Storage Productivity Center. If a failure occurs, an error message will be displayed but there will be no rollback.

If Tivoli Storage Productivity Center for Replication exists and Tivoli Storage Productivity Center does not, then this upgrade will be a fresh installation of Tivoli Storage Productivity Center and an upgrade of Tivoli Storage Productivity Center for Replication. If there is a failure in the Tivoli Storage Productivity Center installation, a rollback will occur of Tivoli Storage Productivity Center (Tivoli Storage Productivity Center for Replication will still remain).

Tivoli Storage Productivity Center for Replication is no longer a stand-alone application. Tivoli Storage Productivity Center Version 4.1 now installs Tivoli Integrated Portal and Tivoli Storage Productivity Center for Replication Version 4.1.

## Upgrading and migrating Tivoli Storage Productivity Center

All PTFs and patches use the upgrade procedure to install Tivoli Storage Productivity Center and do not require you to run the migration tool. You must have a valid Tivoli Storage Productivity Center license to use the upgrade procedure. For information about PTFs and patches, go to http://www.ibm.com/ systems/support/storage/software/tpc/. Click **IBM Tivoli Storage Productivity Center for Data.** Click **Download**. Click **Downloadable files**.

If you are upgrading from one license to a higher-level license, for example, you have IBM Tivoli Storage Productivity Center Basic Edition installed and want to upgrade to IBM Tivoli Storage Productivity Center Standard Edition, you must first install the IBM Tivoli Storage Productivity Center Standard Edition license, then you can upgrade the product.

## Note:

IPv6

You can upgrade an existing version of Tivoli Storage Productivity Center on an IPv4-only computer for use on a computer that is configured for both IPv4 and IPv6 (dual stack). You cannot upgrade Tivoli Storage Productivity Center on an IPv4-only computer for use on a computer that is configured for IPv6 only. If you want to use Tivoli Storage Productivity Center on an IPv6-only computer, you must perform a new install of the product on that computer.

## Agent Manager and agents

Agent Manager version 1.3.2 is available for use with Tivoli Storage Productivity Center 4.1. If you have Agent Manager 1.2, it is optional to upgrade to V1.3.2. Note that the common agents remain at release 1.2 and is compatible with Agent Manager 1.3.2. If this is a new installation of Tivoli Storage Productivity Center, then you can optionally install Agent Manager version 1.3.2 as part of the new Tivoli Storage Productivity Center environment.

If you install an agent locally through the Tivoli Storage Productivity Center installation program, and a Common agent already exists on the system, the Common agent will be upgraded from version 1.2.2 to version 1.2.3.

**Note:** If you have Agent Manager 1.2.3 and it is running well, do not upgrade Agent Manager.

## Upgrading database schema

If you are upgrading the database schema from TotalStorage Productivity Center 3.3.x to Tivoli Storage Productivity Center 4.1 on Windows Server 2003, there is an issue with the maximum size of environment variables like the PATH variable. The maximum size of the PATH variable is 2048 . However, in some cases, the PATH variable is truncated to 1024 characters. You need to install a hot fix from Microsoft. For information about the hot fix, go to http://support.microsoft.com/kb/906469.

## Upgrading the Tivoli Storage Productivity Center license

For information about upgrading the Tivoli Storage Productivity Center installation license, see "Adding an installation license" on page 240.

## **Database migration tool**

After you perform the upgrade operation, you must migrate the Tivoli Storage Productivity Center database using the database migration tool (**partitiontables.bat** or **partitiontables.sh**). The Tivoli Storage Productivity Center version 4.1 database has been changed to improve performance of some queries by either partitioning some databases or including multidimensional clustering. These changes are automatically included when you install Tivoli Storage Productivity Center (but the Tivoli Storage Productivity Center version 3.x database is not migrated at this time). Because the database migration tool can take a long time to run (depending on the size of the database to be migrated), you can run the migration tool at a time that is convenient for you. You only have to run the database migration tool one time. You must run the database migration tool before you apply any patches or PTFs for Tivoli Storage Productivity Center.

When you run the database migration tool, you can check the progress of the database migration in the migrateTable.log file in the <TPC\_install\_directory>\ data\server\tools directory. You will see warning messages if the migration cannot be performed on the database or if the migration has been previously completed. The database migration tool prints out messages indicating which table is currently being migrated and which subsystem ID is currently being migrated.

The database migration tool can be run more than once if an error occurred during execution. Tables that were migrated during previous attempts will not be migrated in subsequent runs.

## InstallShield limitations

These are some limitations you might encounter when installing Tivoli Storage Productivity Center:

- When running the Tivoli Storage Productivity Center installation program on Solaris systems, some of the graphical elements in the installation panels might not display correctly. For example, in the Select the type of installation you want to run panel, the TPC Installation Location button might appear truncated. This is due to an InstallShield limitation on Solaris systems.
- When using the Tivoli Storage Productivity Center installation program to install IBM Tivoli Integrated Portal on AIX systems, the progress bar incorrectly indicates that IBM Tivoli Integrated Portal installation is 100% complete even though it is not yet complete. You must continue to wait until installation is complete. This is due to an InstallShield limitation on AIX systems that prevents the progress bar from correctly reflecting the installation progress.
- When you install Tivoli Storage Productivity Center on AIX, the progress bar can incorrectly display 100% for any component that is installed even though the installation is not complete. This does not affect the installation.
- When you are upgrading the system, you might see several windows prompting you with the text **Replace Existing File**. Reply **Yes to All** to these prompts.

## Migrating TotalStorage Productivity Center 3.x to Tivoli Storage Productivity Center 4.1

If you have TotalStorage Productivity Center 3.x installed and want to migrate to Tivoli Storage Productivity Center 4.1, follow these general steps.

Follow these general steps:

## If you have DB2 version 8.1 installed

Follow these steps:

- 1. Migrate DB2 8.1 to DB2 version 9.5. See "Migrating the database repository" on page 349.
- 2. Upgrade TotalStorage Productivity Center 3.x to Tivoli Storage Productivity Center 4.1. See "Upgrading IBM Tivoli Storage Productivity Center (excluding agents)" on page 363.

## If you have DB2 version 9.1 installed

Follow these steps:

- 1. If you have DB2 version 9.1 with fix pack 2 installed, apply fix pack 5.
- 2. Upgrade TotalStorage Productivity Center 3.x to Tivoli Storage Productivity Center 4.1. See "Upgrading IBM Tivoli Storage Productivity Center (excluding agents)" on page 363.

## If you have DB2 version 9.1 with fix pack 5 installed

Follow these steps:

 If you want to stay with DB2 version 9.1 with fix pack 5, then you can upgrade TotalStorage Productivity Center 3.x to Tivoli Storage Productivity Center 4.1. See "Upgrading IBM Tivoli Storage Productivity Center (excluding agents)" on page 363. 2. If you want to upgrade to DB2 version 9.5, then upgrade to DB2 version 9.5, then upgrade TotalStorage Productivity Center 3.x to Tivoli Storage Productivity Center 4.1. See "Upgrading IBM Tivoli Storage Productivity Center (excluding agents)" on page 363.

## If you have DB2 version 9.5 with fix pack 3a installed

Follow these steps:

- 1. If you have DB2 version 9.5 with fix pack 3a installed, you do not need to upgrade DB2.
- 2. Upgrade TotalStorage Productivity Center 3.x to Tivoli Storage Productivity Center 4.1. See "Upgrading IBM Tivoli Storage Productivity Center (excluding agents)" on page 363.

# Migrating IBM Tivoli Storage Productivity Center for Replication from V3.*x* to V4.1

This topic describes the migration from IBM Tivoli Storage Productivity Center for Replication version 3.x to version 4.1.

IBM Tivoli Storage Productivity Center for Replication is no longer a stand-alone application. IBM Tivoli Storage Productivity Center Standard Edition Version 4.1 now installs Tivoli Integrated Portal and IBM Tivoli Storage Productivity Center for Replication Version 4.1. Before you can migrate, verify that you have the minimum prerequisites required for IBM Tivoli Storage Productivity Center and IBM Tivoli Integrated Portal. For more information about hardware and software requirements, see "Hardware requirements for the IBM Tivoli Storage Productivity Center family" on page 2 and "Software requirements" on page 4.

You do not need to uninstall the previous version of IBM Tivoli Storage Productivity Center for Replication to migrate from one version to the next. Version 4.1 can be installed on an existing version 3.x installation if you have met the hardware and software requirements needed to support IBM Tivoli Storage Productivity Center and IBM Tivoli Integrated Portal.

The following information relates to your migration:

## Installing DB2 FixPacks ( if you installed DB2 with IBM Tivoli Storage Productivity Center for Replication 3.4.x )

To upgrade to a new DB2 FixPack, follow these steps:

- 1. Turn off the heartbeat function, as described in "Managing and Monitoring" chapter in the *User's Guide*.
- 2. Stop the IBM WebSphere Application Server CMS process.
- **3**. Install the DB2 FixPack.
- 4. Verify DB2 is running.
- 5. Start the WebSphere Applications Server.
- 6. Turn on the heartbeat function.

## Changing databases after a migration

If you are using the DB2 or Derby database and you want to switch from DB2 to Derby or Derby to DB2, contact the IBM Support Center for assistance.

## Using an existing database

If you are using an existing DB2 database from a 3.x release, IBM Tivoli Storage Productivity Center for Replication will continue to use the DB2 database. The 4.1 installation program will detect that DB2 is being used and continue using the same DB2 configuration. There is no migration necessary. However, in this situation, the 4.1 installation program does not allow new DB2 configurations.

If you are using an existing Derby database from a 3.x release, you do not need to do any database migration. The installation program will use the same database and update any database schema changes automatically.

#### Using the standby and active servers to migrate the database

If you want IBM Tivoli Storage Productivity Center for Replication to migrate the database automatically using the standby and active servers, follow these general steps:

- 1. The active server will be on Machine A. Schedule some time so that the database can be migrated.
- **2**. Create a new standby server on Machine B. Install IBM Tivoli Storage Productivity Center for Replication version 3.4 on Machine B (the active and standby servers need to be at the same release level).
- **3.** On Machine A, define the standby server (Machine B). This will automatically replicate the database on Machine B. Wait for the replication to complete. You can tell when the active and standby servers are synchronized by looking at the "Management Servers" page. There is a status on that page that indicates "consistent synchronized" when the database have been synchronized.
- 4. Install IBM Tivoli Storage Productivity Center for Replication 4.1 on Machine B.
- 5. On Machine A, undefine the standby server (Machine B).

After you have completed the necessary migration tasks, use the IBM Tivoli Storage Productivity Center installation wizard to complete a typical or custom installation of IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication. For information about installing, see Chapter 2, "Installing the IBM Tivoli Storage Productivity Center family," on page 119.

## Upgrading to DB2 9.5

If you are upgrading DB2 9.1 to DB2 9.5, use the DB2 Information Center for information about upgrading.

For information about upgrading to DB2 9.5, go to this Web Site: http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp. Search for **Migration for DB2 servers**.

## Migrating the database repository

Use this information to learn about the general migration steps required to migrate the database repository from DB2 8.1 with any fix pack to DB2 9.5.

You would perform this procedure only after you have migrated from DB2 8.1 with any fix pack to DB2 9.5 and have upgraded or installed IBM Tivoli Storage Productivity Center 4.1 or Agent Manager or both.

The default database name for IBM Tivoli Storage Productivity Center is **TPCDB**. The default database name for Agent Manager is **IBMCDB**. The same procedure is used for both IBM Tivoli Storage Productivity Center and Agent Manager. To migrate the DB2 database, these are the general steps to follow:

- 1. Stop the IBM Tivoli Storage Productivity Center services and Agent Manager (if you have Agent Manager installed).
- 2. Pre-check the database for migration.
- **3**. Back up the DB2 8.1 database.
- 4. Migrate the DB2 instance.
- 5. Migrate the database.
- 6. Verify the migration.
- 7. Start the IBM Tivoli Storage Productivity Center services and Agent Manager (if you have Agent Manager installed).

Note: In this topic, DB2 8.1 is synonymous with DB2 8.2.

## Migrating the database repository for Windows

This topic provides general migration steps to migrate the database repository from DB2 8.1 with any fix pack to DB2 9.5 on Windows.

**Note:** This procedure also applies to the Agent Manager if you have the Agent Manager installed.

This scenario assumes you have Agent Manager installed on the same machine. If you do not have Agent Manager installed, skip the instructions for Agent Manager.

These are the general steps for migrating the database repository:

- 1. Upgrade DB2 to 9.5. See the steps below.
- 2. Upgrade IBM Tivoli Storage Productivity Center to 4.1. See "Upgrading and migrating the IBM Tivoli Storage Productivity Center family" on page 111.

To migrate the DB2 database on Windows, follow these steps:

- 1. Stop the IBM Tivoli Storage Productivity Center services.
- 2. Verify that your databases are ready for migration.
  - a. Log onto the DB2 server as the DB2 instance owner that you want to migrate.
  - b. Stop the instance by running the db2stop command: db2stop force
  - c. From the DB2 command prompt window, go to the following directory:

#### For UNIX or Linux

Change to the \$DB2DIR/bin directory where DB2DIR is the location that you specified during the DB2 Version 9.5 installation.

#### For Windows

Insert the DB2 Version 9.5 product CD into the CD-ROM drive and change to the \db2\Windows\utilities directory.

d. Run the **db2ckmig** command to verify that the databases that are owned by the current instance are ready to be migrated and to generate a log file. Here is the syntax of the command:

db2ckmig <database> -1 db2ckmig.log -u <admin\_user> -p <password>

Here is an example of the command:

db2ckmig TPCDB -1 db2ckmig.log -u db2admin -p password

If the **db2ckmig** command is successful, the databases can be migrated. The db2ckmig.log file is created in the current directory and includes information about errors and warnings.

Each time you run this command, it overwrites the existing log file. You can rename the log file to avoid losing error information. You must correct these errors before you migrate the database.

When the **db2migr** command runs the **db2ckmig** command, the log file specified is the migration.log file in the instance home directory for Linux and UNIX or in the current directory for Windows.

Ensure that the log file for the **db2ckmig** command the following text: Version of DB2CKMIG being run: VERSION 9.5.

This text confirms that you are running the correct level of the **db2ckmig** command.

- e. Start the instance by running the **db2start** command.
- **3**. Revoke the EXECUTE privilege on migrated routines from PUBLIC. To revoke the EXECUTE privilege on migrated routines from PUBLIC, follow these steps:
  - a. Run the **db2undgp** command. In the following example, the option **-o** creates a file that contains all the REVOKE statements needed to remove the EXECUTE privilege from PUBLIC:

db2undgp -d <database> -o revoke.db2

You can review or edit this file to remove any specific statements when you want to keep the EXECUTE privilege granted to PUBLIC for any routine.

 b. Grant the EXECUTE privilege to specific users on all your routines. The following example shows how to grant this privilege on all functions under a specific schema: CONNECT TO TPCDB

db2 GRANT EXECUTE ON FUNCTION <schema nsme>.\* to USERID

- **c**. Run all your routines as a user granted with the EXECUTE privilege to ensure that the routines run successfully.
- 4. Back up your databases before migration.

To perform an offline full backup for each of your local databases, follow these steps:

a. Disconnect all applications and users from the database. To get a list of all database connections for the current instance, run the **list applications** command:

db2 list applications

If all the applications are disconnected, you will see this message:

 ${\rm SQL1611W}$  No data was returned by the Database System Monitor.  ${\rm SQLSTATE}{=}00000$ 

b. To disconnect all applications and users, use the **force application** command:

db2 force application all

c. Back up your database using the **backup database** command.

This is the syntax for the command:

db2 BACKUP DATABASE <database> USER <user\_ID> USING <password> TO <backup\_directory> This is an example of the command: db2 BACKUP DATABASE TPCDB USER db2admin USING password TO C:\DB2BK

In partitioned database environments, back up all the database partitions. If you performed a full offline database backup recently and you cannot perform another one before migration, you can perform an incremental offline database backup instead. For information about how to perform an incremental offline database backup, see step 5.

d. This is an optional step. You can test the integrity of the backup image to ensure that the image can be restored using the **db2ckbkp** command. Here is the syntax of the command:

db2ckbkp <database>

Here is an example of the command: cd <backup\_directory> db2ckbkp SAMPLE.0.arada.NODE0000.CATN0000.20051014114322.001

You will see this output: [1] Buffers processed: ####### Image Verification Complete - successful.

- 5. Migrate the DB2 server. To migrate the DB2 server from DB2 Version 9.1 or DB2 UDB Version 8 to DB2 Version 9.5, follow these steps:
  - a. Log onto the DB2 server as a user with Local Administrator authority.
  - b. Install DB2 Version 9.5 by running the setup.exe command to launch the DB2 Setup wizard. You have three choices:

## Work with Existing option

This option appears on the Install a Product panel. In the Work with Existing panel, select the DB2 copy name with the migrate action. All your instances running on the selected DB2 copy and your DAS are automatically migrated to the DB2 Version 9.5 copy. The selected DB2 copy and add-on products are uninstalled.

You will get a warning message that recommends that you run the **db2ckmig** command if you have local databases. If you completed the pre-migration tasks, ignore this warning message and continue with the migration. Otherwise, verify that your databases are ready for DB2 migration before continuing with the installation.

## Install New option

This option appears on the Install a Product panel. This option creates a new copy of DB2 Version 9.5, and you must migrate your instances after installation.

## Work with Existing option, create response file

This option appears on the Install a Product panel. In the Work with Existing panel, select the DB2 copy name with the migrate action. In the Select the installation panel, response file creation, or both window, select **Save my installation setting in a response file** option to create a response file for a response file installation. The response file has the required MIGRATE\_PRIOR\_VERSIONS keywod, the DB2 copy name, and the installation path.

The response file installation will be the same as the first choice, all your instances running on the selected DB2 copy and your DAS are automatically migrated to the DB2 Version 9.5 copy.

- **c.** If you want your applications to access the DB2 Version 9.5 copy through the default interface or if you migrated your existing DB2 UDB Version 8 copy, set the DB2 Version 9.5 copy as the DB2 default copy. You must define a default copy if you migrated from DB2 UDB Version 8 because there is no default copy defined in your DB2 server.
- d. This is an optional step. When you select to install a new copy, migrate the DAS if you want to keep your existing DAS configuration and use new functions available with DB2 Version 9.5. If your DAS is running on DB2 UDB Version 8, you need to migrate it to use the Control Center to administer your DB2 Version 9.5 and Version 9.1 instances.
- 6. Migrate your databases. To migrate a DB2 database, follow these steps:
  - a. Log onto the DB2 server as the instance owner or a user with SYSADM authority.
  - b. This is an optional step. Rename or delete the db2diag.log file so that a new file is created. Also, remove or move any existing dump files, trap files, and alert log files from the directory indicated by the **diagpath** parameter. Move these files to another directory. By doing this, the files only contain information about the migration process and helps you isolate and understand any problems that might occur during database migration.
  - **c.** Migrate the database using the **migrate database** command. Here is the syntax for the command:

db2 MIGRATE DATABASE <database\_alias> USER <user\_ID> USING <password>

Where <database\_alias> is the name or the alias of the database you want to migrate. <user\_ID> is the user ID with SYSADM authority. Here is an example of the command:

db2 MIGRATE DATABASE TPCDB USER db2admin USING password

d. If the database migration fails and returns the error message SQL1704N with a reason code that describes the cause of the failure, find this SQL error code and determine the list of the possible solutions for each reason code. One of the most common causes of migration failure is that the log file space is not large enough, in which case the following error is returned:

SQL1704N Database migration failed. Reason code "3".

You must increase the log file size and run the **migrate database** command again. Once the database migration is complete, reset the value of logfilsiz, logprimary, and logsecond database configuration parameters. There are additional error codes that are returned by the **migrate database** command for specific cases that are not supported by the database migration. These cases are described in the migration restrictions for DB2.

e. If the database migration returns the warning message SQL1243W, you need to drop or rename the SYSTOOLS.DB2LOOK\_INFO table. Otherwise, the ALTER TABLE and COPY SCHEMA statements will fail to run. Check if the SYSTOOLS.DB2LOOK\_INFO table exists by running the following command:

If you created this table, simply rename it by running the RENAME statement:

db2 RENAME SYSTOOLS.DB2LOOK\_INFO TO <new\_table\_name>

If you did not create this table, simply remove it by running the DROP command:

db2 DROP TABLE SYSTOOLS.DB2LOOK\_INFO

7. Verify that your database migration is successful. Connect to the migrated databases and run a small query. Here is an example of the **db2 connect** command:

db2 connect to  $\ensuremath{\mathsf{TPCDB}}$ 

**8**. After you have migrated a database from DB2 8.1 to DB2 9.5, there are several parameters that need to be set manually.

## Self-tuning memory

The self-tuning memory can be enabled for migrated databases by setting the **self\_tuning\_mem** configuration parameter to ON and setting these parameters:

#### self\_tuning\_mem

Run the following command in Windows and Linux for IBM Tivoli Storage Productivity Center:

DB2 UPDATE DB CFG FOR TPCDB USING SELF\_TUNING\_MEM ON

For Agent Manager, run this command:

DB2 UPDATE DB CFG FOR IBMCDB USING SELF\_TUNING\_MEM ON

#### pckcachesz

Run the following command in Windows and Linux for IBM Tivoli Storage Productivity Center:

DB2 UPDATE DB CFG FOR TPCDB USING PCKCACHESZ AUTOMATIC

For Agent Manager, run this command:

DB2 UPDATE DB CFG FOR IBMCDB USING PCKCACHESZ AUTOMATIC

#### database\_memory

Run the following command for IBM Tivoli Storage Productivity Center:

For Windows

DB2 UPDATE DB CFG FOR TPCDB USING DATABASE\_MEMORY AUTOMATIC

Run the following command for Agent Manager:

For Windows

DB2 UPDATE DB CFG FOR IBMCDB USING DATABASE\_MEMORY AUTOMATIC

## avg\_appls

This parameter is used by the query optimizer to estimate how much buffer pool will be available at run-time for the access plan chosen. Run this command for Windows and Linux for IBM Tivoli Storage Productivity Center:

DB2 UPDATE DB CFG FOR TPCDB USING AVG\_APPLS AUTOMATIC

Run this command for Agent Manager:

DB2 UPDATE DB CFG FOR IBMCDB USING AVG\_APPLS AUTOMATIC

- 9. Restart the IBM Tivoli Storage Productivity Center services.
- **10.** Upgrade IBM Tivoli Storage Productivity Center to 4.1. See "Upgrading and migrating the IBM Tivoli Storage Productivity Center family" on page 111.

## Migrating the database repository for AIX

This topic provides general migration steps to migrate the database repository from DB2 8.1 with any fix pack to DB2 9.5 on AIX.

When installing or upgrading IBM Tivoli Storage Productivity Center or DB2 on AIX, you will need a Telnet/SSH session and a graphical display.

These are the general steps for migrating the database repository:

- 1. Upgrade DB2 to 9.5. See the steps below.
- 2. Upgrade IBM Tivoli Storage Productivity Center to 4.1. See "Upgrading and migrating the IBM Tivoli Storage Productivity Center family" on page 111.

To migrate the DB2 database on AIX, follow these steps:

- 1. Verify that IBM Tivoli Storage Productivity Center is up and running:
  - a. Open the IBM Tivoli Storage Productivity Center GUI.
  - b. Check to see if the following IBM Tivoli Storage Productivity Center services are running:
     Administrative Services > Services > Data Server Administrative Services > Services > Device Server
- 2. Stop the following IBM Tivoli Storage Productivity Center services:
  - a. Close the IBM Tivoli Storage Productivity Center GUI.
  - b. Stop the IBM Tivoli Storage Productivity Center Data server and Device server by running these commands:

Data Server: stopsrc -s TSRMsrv1

Device Server: /opt/IBM/TPC/device/bin/aix/stopTPCF.sh

- c. Stop the Data agent and Fabric agent by stopping the common agent: /opt/IBM/TPC/ca/subagents/TPC/Data/tpcdagt2 stop
- **3**. Make sure there are no DB2 connections to the instance used for the IBM Tivoli Storage Productivity Center database:
  - a. Log in with the instance owner ID. (You can also login using the telnet/putty session.) The command is:

su - <db2\_8.1\_instance\_owner>

For example:

su - db2inst1

- b. Stop all DB2 connections by running this command: db2 force applications all
- c. List the DB2 applications by running this command: db2 list applications

This is the output expected: SQL1611W No data was returned by Database System Monitor. SQLSTATE=00000

4. Make a database backup by running the following command and then exit:

db2 backup db <database\_name> exit

For example:

db2 backup db TPCDB exit

5. Install DB2 9.5 on your system.

Note:

- Open and use a new graphical display that is not loaded with the parameters for DB2 8.1. Otherwise, you will get an error for the DB2 9.5 installation.
- You do **NOT** need to create an instance while installing DB2 9.5. You should migrate the instance used in DB2 8.1 to DB2 9.5 after installation of DB2 9.5.
- 6. Migrate the DB2 8.1 instance to DB2 9.5 instance:
  - a. Go to the display loaded with the DB2 8.1 parameters.
  - b. Verify that the instance can be migrated from DB2 8.1 to DB2 9.5:
    - 1) Switch to the instance owner ID:

su - <db2\_8.1\_instance\_owner>

For example: su - db2inst1

 List the instances on DB2 8.1: db2ilist -a

For example, the output should be displayed as follows for the IBM Tivoli Storage Productivity Center database:

db2inst1 32/opt/IBM/db2/V8.1

- Stop the DB2 instance: db2stop
- Exit from the login session: exit
- c. Migrate the database from DB2 8.1 to DB2 9.5:
  - 1) Open a new telnet/putty/SSH session with the root ID.
  - 2) Change the directory to the DB2 9.5 installation location and instance. For example:

cd /opt/ibm/db2/V9.5/instance

- 3) Migrate the DB2 instance:
  - ./db2imigr -d -u <db2\_fence\_id> <db2\_8.1\_instance\_name>

For example: ./db2imigr -d -u db2fenc1 db2inst1

This command should return "exit 0."

 Switch to the instance owner ID: su <db2 8.1 instance owner>

For example: su - db2inst1

5) Check the DB2 level: db2level

The output should display the version information for DB2 v9.5.0.2.

6) Migrate the IBM Tivoli Storage Productivity Center database:

db2start db2 migrate database <TPC\_database>

For example: db2start db2 migrate database TPCDB

- Exit from the login session.
   exit
- 7. Configure DB2 V9.5:
  - a. Switch to the instance owner ID:

su - <db2\_9.5\_instance\_owner>

For example:

su - db2inst1

b. Set the self-tuning memory option:

db2update db cfg for <TPC\_database> using self\_tuning\_mem on

For example:

db2 update db cfg for TPCDB using self\_tuning\_mem on

c. Set the package cache size option: db2update db cfg for <TPC\_database> using pckcachesz automatic

For example:

db2 update db cfg for TPCDB using pckcachesz automatic

d. Set the database memory option:

db2update db cfg for <TPC\_database> using database\_memory computed

For example:

db2 update db cfg for TPCDB using database\_memory computed

e. Exit from the login session:

exit

- 8. Start the IBM Tivoli Storage Productivity Center services.
- **9**. Upgrade IBM Tivoli Storage Productivity Center to 4.1. See "Upgrading and migrating the IBM Tivoli Storage Productivity Center family" on page 111.

## Migrating the database repository for Linux

This topic provides general migration steps to migrate the database repository from DB2 8.1 with any fix pack to DB2 9.5 on Linux.

When installing or upgrading IBM Tivoli Storage Productivity Center or DB2 on Linux, you will need a Telnet/SSH session and a graphical display interface.

These are the general steps for migrating the database repository:

- 1. Upgrade DB2 to 9.5. See the steps below.
- 2. Upgrade IBM Tivoli Storage Productivity Center to 4.1. See "Upgrading and migrating the IBM Tivoli Storage Productivity Center family" on page 111.

To migrate the DB2 database on Linux, follow these steps:

- 1. Verify that IBM Tivoli Storage Productivity Center is up and running:
  - a. Open the IBM Tivoli Storage Productivity Center GUI.

- b. Check to see if the following IBM Tivoli Storage Productivity Center services are running:
   Administrative Services > Services > Data Server Administrative Services > Services > Device Server
- 2. Stop the following IBM Tivoli Storage Productivity Center services:
  - a. Close the IBM Tivoli Storage Productivity Center GUI.
  - b. Stop the IBM Tivoli Storage Productivity Center Data server and Device server:

```
Data Server:
/opt/IBM/TPC/data/server/tpcdsrv1 stop
```

```
Device Server:
/opt/IBM/TPC/device/bin/linux/stopTPCF.sh
```

- c. Stop the Data agent and Fabric agent by stopping the common agent: /opt/IBM/TPC/ca/subagents/TPC/Data/tpcdagt2 stop
- **3**. Make sure there are no DB2 connections to the instance used for the IBM Tivoli Storage Productivity Center database:
  - a. Log in with the instance owner ID. (You can also login using the telnet/putty session.) The command is:

su - <db2\_8.1\_instance\_owner>

For example:

su - db2inst1

- b. Stop all DB2 connections by running this command: db2 force applications all
- c. List the DB2 applications by running this command:
   db2 list applications

This is the expected output:

 $\mathsf{SQL1611W}$  No data was returned by <code>Database System Monitor.SQLSTATE=00000</code>

 Make a database backup by running the following command and then exit: db2 backup db <database\_name> exit

For example: db2 backup db TPCDB exit

5. Install DB2 9.5 on your system.

**Note:** You do **NOT** need to create an instance while installing DB2 9.5. You should migrate the instance used in DB2 8.1 to DB2 9.5 after installation of DB2 9.5.

- 6. Migrate the DB2 8.1 instance to DB2 9.5 instance:
  - a. Verify that the instance can be migrated from DB2 8.1 to DB2 9.5:
    - 1) Switch to the instance owner ID:

su - <db2\_8.1\_instance\_owner>

For example: su - db2inst1

2) List the instances on DB2 8.1: db2ilist -a For example, the output should be displayed as follows for the IBM Tivoli Storage Productivity Center database: db2inst1 32/opt/IBM/db2/V8.1

- 3) Stop the DB2 instance: db2stop
- Exit from the login session: exit
- b. Migrate the database from DB2 8.1 to DB2 9.5:
  - 1) Open a new telnet/putty/ssh session with the root ID.
  - 2) Change the directory to the DB2 9.5 installation location and instance. For example:

cd /opt/ibm/db2/V9.5/instance

**3)** Migrate the DB2 instance:

./db2imigr -d -u <db2\_fence\_id> <db2\_8.1\_instance\_name>

For example: ./db2imigr -d -u db2fenc1 db2inst1

This command should return "exit 0."

4) Switch to the instance owner ID: su - <db2\_8.1\_instance\_owner>

For example: su - db2inst1

5) Check the DB2 level: db21eve1

The output should display the version information for DB2 v9.5.0.2.

6) Migrate the IBM Tivoli Storage Productivity Center database: db2start db2 migrate database <TPC database>

For example: db2start db2 migrate database TPCDB

- Exit from the login session. exit
- 7. Configure DB2 V9.5:
  - a. Switch to the instance owner ID:

su - <db2\_9.5\_instance\_owner>

For example:

su - db2inst1

b. Set the self-tuning memory option:
 db2update db cfg for <TPC database> using self tuning mem on

For example:

db2 update db cfg for TPCDB using self\_tuning\_mem on

c. Set the package cache size option: db2update db cfg for <TPC\_database> using pckcachesz automatic For example:

db2 update db cfg for TPCDB using pckcachesz automatic

d. Set the database memory option:
 db2update db cfg for <TPC database> using database memory computed

For example:

db2 update db cfg for TPCDB using database\_memory computed

**e**. Exit from the login session:

exit

- 8. Start the IBM Tivoli Storage Productivity Center services.
- 9. Upgrade IBM Tivoli Storage Productivity Center to 4.1. See "Upgrading and migrating the IBM Tivoli Storage Productivity Center family" on page 111.

## Upgrading Agent Manager

This topic provides information on how to upgrade Agent Manager.

Agent Manager supports DB2 9.1 and DB2 9.5.

If you are upgrading Agent Manager and have also upgraded DB2 8.1 to DB2 9.5, you must also migrate the DB2 database after upgrading the Agent Manager. For information about migrating the database, see "Migrating the database repository" on page 349.

To upgrade the Agent Manager, complete the following steps:

- 1. Make a backup copy of your certificates before upgrading. For information about backing up your certificates, see "Backing up the original certificates on the Agent Manager server" on page 420.
- 2. Untar or unzip the electronic Agent Manager image or insert the Agent Manager CD into the CD-ROM drive.
- **3**. Log onto the computer with a user ID that has the appropriate authority:
  - For Windows, you must have administrative authority.
  - For UNIX or Linux, you must have root authority.
- 4. For UNIX or Linux platforms, you need to set the environment variables for the database instance (source db2profile). For example, if your DB2 instance is db2inst1, source the db2profile:
  - . /home/db2inst1/sqllib/db2profile

where *home* is the home directory of the instance owner.

- 5. From a command window, go to the directory for the platform (Windows, AIX, or Linux) where the Agent Manager source directory or CD is located.
- 6. Navigate to the EmbeddedInstaller directory. Invoke the Agent Manager installation program:
  - For Windows, double-click on setupwin32.exe in Windows Explorer.
  - For AIX, invoke **setupAix.bin**.
  - For Linux, invoke setupLinux.bin.
- 7. The Agent Manager installation program opens and discovers an existing instance of Agent Manager installed. You will see this panel with the message:

Version 1.2.3.6 of the agent manager is currently installed on this computer. Click next to upgrade this configuration to version 1.3.2.x build xxxxxxxxx. If you do not want to upgrade, click Cancel to stop the installation.

To continue, click Next.

- 8. The Database User Information panel is displayed. Accept the information or enter the correct information. Click **Next**.
- **9**. A series of installing panels for embedded WebSphere are displayed indicating the progress of the installation. Wait for the upgrade to complete.
- 10. The summary information panel is displayed indicating where Agent Manager will be installed with the size information. Review the information and click **Next**.
- **11.** A series of installing panels for Agent Manager are displayed indicating the progress of the installation. Wait for the installation to complete.
- 12. The Stop and Restart the AgentManager Application Server panel is displayed. You have these options:
  - Yes, stop and then start AgentManager now
  - No, I will stop and then start AgentManager later

Make a selection and then click Next.

- **13.** You will see a series of installing panels displayed indicating the progress of the installation. Wait for the installation to complete.
- 14. A Summary of Installation and Configuration Results panel is displayed. This panel indicates if the Agent Manager has successfully validated and installed all of its components. Review the information and click **Next**.
- **15**. The summary information panel is displayed. For a successful upgrade, you will see this displayed:

The agent manager upgrade completed successfully. Click Finish to exit the installation. The installation is complete and the agent manager application server has been started.

Click Finish.

16. You can use the **GetAMInfo** command to verify the Agent Manager version. To run the **GetAMInfo** command, go to the following directory:

<agent\_manager\_dir>/bin (for AIX and Linux) <agent\_manager\_dir>\bin (for Windows)

Run the following command:

GetAMInfo.sh (for AIX and Linux) GetAMInfo.bat (for Windows)

Here is an example of the output from the **GetAMInfo** command:

C:\Program Files\IBM\AgentManager\bin>getaminfo CTGEM2124I Agent Manager: version 1.3.2.4 build 200610260359

## Preparing for an upgrade

When you upgrade IBM Tivoli Storage Productivity Center, you will be upgrading all components (if all components are installed). This topic describes the preparation steps required before you do an upgrade installation. If you have your database on a separate machine from the server, you must also upgrade the remote database.

Before you upgrade Tivoli Storage Productivity Center, complete the following steps:

- 1. Exit all instances of the Tivoli Storage Productivity Center GUI.
- 2. Make sure you have exclusive access to the server you are installing version 4 on. If you are accessing the server remotely, make sure there are no other remote connections to the server. Multiple remote connections, such as Windows Remote Desktop Connections, will cause the upgrade to fail and may render the server unrecoverable. To log off other remote users on Windows, follow these steps:
  - a. Go to Start → Settings → Control Panel → Administrative Tools → Terminal Services Manager.
  - b. On the Users tab, right-click the users that should not be logged in to the server and select **Logoff** from the pop-up menu.
  - c. Close the Terminal Services Manager window.
- 3. Stop all three Tivoli Storage Productivity Center services. Also make sure that you stop any long running scan jobs. To stop the services on Windows, go to **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Services**. Stop the following services:
  - IBM WebSphere Application Server V6 Device server
  - IBM TotalStorage Productivity Center Data Server
  - IBM Tivoli Common agent <directory> where <directory> is where the Common agent is installed. The default is <TPC\_install\_dir>/ca.

For information about stopping the services, see "Stopping the IBM Tivoli Storage Productivity Center services" on page 464.

- 4. Back up your current IBM TotalStorage Productivity Center 3.3.x server and database. This is important in case of an upgrade failure.
  - a. Back up your IBM TotalStorage Productivity Center database using the DB2 backup and recovery process.
  - b. Back up your <TPC\_install\_dir>. For example, back up these directories: C:\Program Files\IBM\TPC (for Windows) /<usr or opt>/IBM/TPC (for UNIX or Linux)
  - c. Back up your Common agent installation directory (<common\_agent\_install\_dir>). if it is not a subdirectory under your IBM TotalStorage Productivity Center directory. For example, if you used the default directory structure when you installed version 3.3.x, your

<common\_agent\_install\_dir> would be C:\Program Files\IBM\TPC\ca and you would not need to back it up separately. It would have been backed up in the previous step.

d. Back up the registries.

## InstallShield registries

Back up the following registries:

/<usr or opt>/lib/objrepos/InstallShield/ Universal/IBM-TPC (for AIX) /root/InstallShield/Universal/IBM-TPC (for UNIX or Linux) C:\Program Files\Common Files\InstallShield\ Universal (for Windows)

## SRM legacy registry

Back up the following registries:

subsystem TSRMsrv# where # can be any number (for AIX) (1 or any number higher than 1) /etc/Tivoli (for UNIX or Linux)

#### Windows registry

Back up the Windows registry.

#### CA registry

Back up the following registries:

/<usr or opt>/tivoli/ep.reg

(for UNIX or Linux)

- C:\Program Files\tivoli\ep.reg
- (for Windows)
- 5. Restart all three services. To start the services on Windows, Start → Settings → Control Panel → Administrative Tools → Services. Start the following services:
  - IBM WebSphere Application Server V6 Device server
  - IBM TotalStorage Productivity Center Data Server
  - IBM Tivoli Common agent <directory> where <directory> is where the Common agent is installed. The default is <TPC\_install\_dir>/ca.

For information about starting the services, see "Starting the IBM Tivoli Storage Productivity Center services" on page 465.

## Upgrading IBM Tivoli Storage Productivity Center (excluding agents)

This topic describes how to upgrade all the IBM Tivoli Storage Productivity Center components except for the agents.

To upgrade Tivoli Storage Productivity Center, use the same installation program as installing the product. Depending on what components you have already installed on your system, there will be some differences in the panels you see. If you are upgrading the agents on a different server, see "Upgrading the IBM Tivoli Storage Productivity Center agents" on page 369.

Tivoli Storage Productivity Center for Replication is no longer a stand-alone application. Tivoli Storage Productivity Center Version 4.1 now installs Tivoli Integrated Portal and Tivoli Storage Productivity Center for Replication Version 4.1.

If you are upgrading the IBM Tivoli Storage Productivity Center agents in silent mode, use the setup\_agents.iss (for agents) file. See "Installing IBM Tivoli Storage Productivity Center in silent mode" on page 262.

Note the following:

- There are two installation images:
  - **disk1** Contains all the Tivoli Storage Productivity Center components. Also includes the files to perform remote Data agent installations.

The **disk1** image is in two parts. Both parts must be downloaded to the same directory.

For Storage Resource agents, the image is located in the following location:

<DVD>/data/sra/<operating\_system\_name>

The operating systems supported are listed in the following table.

Operating systemOperating system nameAIXaix\_powerLinux x86linux\_ix86Linux Powerlinux\_powerLinux s390linux\_s390Windowswindows

Table 31. Operating system for Storage Resource agents

**disk2** Contains the files to perform local agent installations. This image also contains the installation script for the Virtual I/O server. Download the file for the platform you want the agent to reside on.

For information about the Storage Resource agents, see the **disk1** image. The **disk2** location and operating system file name is the same as the **disk1** image.

• You can upgrade TotalStorage Productivity Center 3.3.x to Tivoli Storage Productivity Center version 4.1 in an IPv4 environment to an environment that supports both IPv6 and IPv4. You cannot upgrade the product from an IPv4–only environment directly to an IPv6–only environment. For more information, see "Planning for Internet Protocol Version 6" on page 34.

If you have installed all the TotalStorage Productivity Center components on your system and are upgrading to Tivoli Storage Productivity Center 4.1, complete the following steps:

- 1. Start the Tivoli Storage Productivity Center installation program.
- 2. The Select a language panel is displayed. Select a language and click OK.
- **3**. The Software License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select I accept the terms of the license agreement. Click **Next**.

**Note:** 8 GB of RAM is required. If you have 4-8 GB of RAM, you can still install Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication. However, you will get a warning message. You should run only Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication because of system load. For information about how to disable Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication after installation, see "Disabling Tivoli Storage Productivity Center or Tivoli Storage Productivity Center or Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication after installation, see "Disabling Tivoli Storage Productivity Center or Tivoli Storage Productivity Center for Replication" on page 341.

- 4. The Select the type of installation you want to run panel is displayed. Select Typical installation. Select Servers, Agents (if you have agents installed), Clients, and Register with the agent manager (if you are have the Agent Manager installed). Click Next.
- 5. The User ID and password, and server and agent information panel is displayed. Enter the User ID and password. Click **Next**.
- **6**. The Tivoli Integrated Portal panel is displayed. Enter this information and click **Next**.

## Specify the location to install TIP

Accept the default or enter a location to install Tivoli Integrated Portal.

- **Port** Enter the port number for Tivoli Integrated Portal or accept the default (16310). Tivoli Integrated Portal uses 10 port numbers. For example, if the default port 16310 is accepted, Tivoli Integrated Portal uses the following ports: 16310, 16311, 16312, 16313, 16315, 16316, 16318, 16320, 16322, and 16323. If you enter a port number other than the default number, ensure that you have the following ports available for Tivoli Integrated Portal:
  - base port
  - base port +1
  - base port +2
  - base port +3
  - *base port* +5
  - *base port* +6
  - base port +8
  - *base port* +10
  - *base port* +12
  - *base port* +13

where *base port* is the port value entered in the **Port** field.

## Reuse an existing install TIP install

If you select this option, you will see a list of existing IBM Tivoli Integrated Portal installations. Select a IBM Tivoli Integrated Portal installation.

## **TIP Administrator ID**

Enter theIBM Tivoli Integrated Portal administrator ID.

## Password

Enter the password for the IBM Tivoli Integrated Portal administrator ID.

7. The authentication panel is displayed. Enter this information and click Next.

## **OS** Authentication

This uses the operating system for user authentication. If you select this option, go to step 12.

## LDAP/Active Directory

If you select LDAP or Microsoft Active Directory for authentication, you must have an LDAP or Active Directory already installed.

If you select this option, you will also see other panels for LDAP authentication. Click **Next**.

**8**. The Lightweight Directory Access Protocol (LDAP server information) panel is displayed. Enter this information and click **Next**.

#### LDAP Server Hostname

The fully-qualified host and domain name of the machine where your LDAP-based directory is running.

#### LDAP Port Number

The port number on your LDAP server where the LDAP process is listening for communications.

#### Bind Distinguished Name

The distinguished name used to bind to the LDAP-based directory when performing a user or group search. This name is optional because some LDAP-based directories allow anonymous binds and others require you to bind with a specific name and password.

**Note:** Depending on how the LDAP server is set up, the Bind DN and password might or might not be optional. If the LDAP server allows for anonymous binds, then the Bind DN and password are optional.

If you want the ability to create or modify LDAP users and groups from the IBM Tivoli Integrated Portal administrative panel, then the Bind DN and password are required.

#### **Bind Password**

The password associated with the Bind Distinguished Name.

**9**. The Lightweight Directory Access Protocol (LDAP user and group information) panel is displayed. Enter this information and click **Next**.

#### **Relative Distinguished Name for usernames**

Tells IBM Tivoli Storage Productivity Center where to start a search in the directory when performing user authentication.

#### Attribute to use for usernames

Tells IBM Tivoli Storage Productivity Center which attribute in a user's directory entry contains the user's name for authentication.

## **Relative Distinguished Name for groups**

Tells IBM Tivoli Storage Productivity Center where in the directory to start a search when performing a group search for authorization.

## Attribute to use for groups

Tells IBM Tivoli Storage Productivity Center which attribute in a group's directory entry contains the group's name for authorization.

**10.** The Lightweight Directory Access Protocol (LDAP TPC Administrator user and group) panel is displayed. Enter this information and click **Next**.

## LDAP TPC Administrator username

The user ID that IBM Tivoli Storage Productivity Center will configure as the IBM Tivoli Storage Productivity Center superuser during installation. This user name should already exist in the directory before you start the IBM Tivoli Storage Productivity Center installation and should be a member of your designated LDAP IBM Tivoli Storage Productivity Center Administrator group in the directory.

**Note:** If you install IBM Tivoli Storage Productivity Center on a Windows system and have IBM Tivoli Storage Productivity Center authenticate users against an LDAP-based repository, then the LDAP TPC Administrator username must **not** contain a space or blank character in it. See the WebSphere Application Server APAR PK77578.

Ensure that you use the correct case when entering the values for the LDAP TPC Administrator username and LDAP TPC Administrator group. If you use the incorrect case when entering these values, then you will not be able to login to Tivoli Storage Productivity Center for Replication with the user name you expected to use.

#### LDAP TPC Administrator password

Password for the administrator.

## LDAP TPC Administrator group

The group that Tivoli Storage Productivity Center will map to the

Tivoli Storage Productivity Center superuser role during installation. This group should already exist in the directory before you start the Tivoli Storage Productivity Center installation and should have the designated LDAP IBM Tivoli Storage Productivity Center Administrator as a member.

## Note:

Ensure that you use the correct case when entering the values for the LDAP TPC Administrator username and LDAP TPC Administrator group. If you use the incorrect case when entering these values, then you will not be able to login to Tivoli Storage Productivity Center for Replication with the user name you expected to use.

- 11. The IBM Tivoli Storage Productivity Center role to group mapping panel is displayed. For information about authorizing users, see "Role-to-Group Mappings" on page 279.
- 12. The Summary information panel is displayed. Review the components to be installed. Click **Install**.
- **13**. You will see the installing panel. When Tivoli Integrated Portal has finished installing, Tivoli Storage Productivity Center will start the Tivoli Storage Productivity Center for Replication installation.

**Note:** When you are upgrading the system, you might see several windows prompting you with the text **Replace Existing File**. Reply **Yes to All** to these prompts.

- 14. If you elected to upgrade the agents on this server, you do not have to upgrade the agents separately. The upgrade procedure will handle upgrading the agents on this server. If you need to upgrade the agents on different computers, see "Upgrading the IBM Tivoli Storage Productivity Center agents" on page 369.
- **15.** Tivoli Storage Productivity Center starts the IBM Tivoli Storage Productivity Center for Replication installation program.
  - a. The Welcome panel is displayed. Click Next.
  - b. The System prerequisites check panel is displayed. The installation wizard checks whether the prerequisites are installed, then confirms whether your operating system is supported and is at the appropriate fix pack or update level. Click **Next**.
  - c. The License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select I accept the terms of the license agreement. Click Next.
  - d. The Directory Name panel is displayed. Accept the default installation directory by clicking **Next**, or specify a different installation directory and click **Next**.
  - e. The IBM Tivoli Storage Productivity Center for Replication Administrator ID and Password panel is displayed. Enter the administrator user ID and password. This ID is usually the operating system administrator user ID. If you use a different ID, create it beforehand and ensure that it has administrator rights.

**Note:** There is a limitation on the number of characters for the user name and password on AIX. At the time this document was written, AIX did not properly validate passwords that are longer than eight characters.

f. The Default ports panel is displayed. Accept the defaults. Click Next.

- g. The settings panel is displayed. Review the settings and change them if needed by clicking **Back**. Otherwise, click **Install** to begin the installation.
- h. You will see the status panel. Wait for installation to complete.
- i. You will see the summary information panel. Review the information. Click **Finish**.
- 16. The successfully installed panel is displayed. Click Finish.
- 17. Migrate the Tivoli Storage Productivity Center database. This step can be performed right after upgrading or at a later time. The database migration tool can run a long time depending on the size of your database. You must, however, run the database migration tool before you install any Tivoli Storage Productivity Center patches or PTFs. To run the database migration tool, go to the following directory:

<disk1\_image\_directory>\data\scripts

Run this command: partitiontables.bat (for Windows) partitiontables.sh (for UNIX and AIX)

The database connection information is automatically obtained and the migrateTable.log file is created under the following directory: <TPC\_install\_directory>\data\server\tools

If the database migration tool is interrupted for some reason, it is safe to run the migration tool again. The tool will pick up where it left off the last time. If the database migration has been completed and the command is run again, this tool returns immediately.

## Upgrading the remote database

If the TotalStorage Productivity Center database is on a remote system from the server, you must also upgrade the remote database.

**Note:** If you are upgrading the database schema from TotalStorage Productivity Center 3.3.x to Tivoli Storage Productivity Center 4.1 on Windows Server 2003, there is an issue with the maximum size of environment variables like the PATH variable. The maximum size of the PATH variable is 2048 . However, in some cases, the PATH variable is truncated to 1024 characters. You need to install a hot fix from Microsoft. For information about the hot fix, go to http://support.microsoft.com/kb/906469.

To upgrade the remote database, follow these steps:

- 1. Start the Tivoli Storage Productivity Center installation program.
- 2. The Select a language panel is displayed. Select a language and click OK.
- **3**. The Software License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select I accept the terms of the license agreement. Click **Next**.
- 4. The Select the type of installation you want to run panel is displayed. Select **Custom installation**. Click **Next**.
- 5. The Select one or more components to install on the local or remote computer panel is displayed. Select **Database schema**. Click **Next**.
- 6. Wait for installation to complete.
- 7. If you have upgraded the database from DB2 V8 to DB2 V9.5, you must migrate the database after upgrading it. See "Migrating the database repository" on page 349.
- 8. Migrate the Tivoli Storage Productivity Center database. This step can be performed right after upgrading or at a later time. The database migration tool can run a long time depending on the size of your database. You must, however, run the database migration tool before you install any Tivoli Storage Productivity Center patches or PTFs. To run the database migration tool, go to the following directory:

<disk1\_image\_directory>\data\scripts

Run this command:

partitiontables.bat (for Windows)
partitiontables.sh (for UNIX and AIX)

The database connection information is automatically obtained and the migrateTable.log file is created under the following directory: <TPC\_install\_directory>\data\server\tools

## Upgrading the IBM Tivoli Storage Productivity Center agents

This section describes how to upgrade an existing or older version of IBM Tivoli Storage Productivity Center agents to the current release.

When upgrading agents, note the following:

- Once you upgrade the Tivoli Storage Productivity Center server to the current release, you can only install agents that are at the same release level of that server (Common agent version 1.2.3). If you attempt to install agents of a previous release, the installation will fail. For example, if you upgrade the server to V3.3, you can install common agents at version 1.2.3 only. If you attempt to install a pre-V1.2.3 common agents, the installation will fail.
- Before upgrading the common agents V1.2.3, make sure those agents are registered with the Tivoli Storage Productivity Center server. If you point a pre-V1.2.3 unregistered Common agent to a new V3.3 server, the upgrade will fail for that agent.
- You must close any running sessions of the GUI before performing an upgrade.
- The agent machines must have fully qualified host names, for example: ddunham.myorg.mycompany.com.
- When you upgrade the Common agent, you will automatically upgrade the Common agent if you have a down-level agent.

## Upgrading Storage Resource agents manually

This section describes how to upgrade the Storage Resource agents manually.

To upgrade the Storage Resource agent agent, follow these steps:

1. Go to the DVD location of the installation program (using the disk1 image) and go to the bin directory:

cd <DVD\_image\_location>/data/sra/<operating\_system\_name>

Where *<DVD\_image\_location>* is the Storage Resource agent installation image location.

2. Run the upgrade command:

bin/Agent -upgrade
-installLoc <agent\_install\_directory>

Paramater for daemon service: -commType Daemon

The parameters are:

-installLoc <agent\_install\_dir>
 Location where the agent will be installed.

#### -commType Daemon

If the agent is run as a daemon service, then this parameter must be specified.

Here is an example for a daemon-based service:

bin/Agent -upgrade
-installLoc /opt/IBM/TPC/agent
-commType Daemon

Here is an example for a non-daemon service: bin/Agent -upgrade -installLoc /opt/IBM/TPC/agent

#### Note:

If you run the upgrade program outside of the *<DVD\_image\_location>* installation directory, then you must specify the full path.

If the upgrade fails, see the return codes in the Information Center. Search for **Return codes used by Storage Resource agent**.

#### Upgrading the Data agents

This section describes how to upgrade the Data agents.

You have two options for upgrading Data agents:

- Upgrading the Data agents through the GUI. This is also called a scheduled upgrade because you can specify to upgrade the agents at a time when network activity will not be impacted by the upgrades.
- Performing a local install of the Data agent, where the upgrade is actually done through the installation program.

#### Upgrading the Data agents using the GUI

This topic describes how to upgrade the Data agents using the GUI.

To schedule a Data agent upgrade through the GUI, complete the following steps:

- 1. Open the IBM Tivoli Storage Productivity Center GUI.
- 2. Go to Administrative Services → Configuration → Data Agent Upgrades.
- 3. Right-click the Data Agent Upgrades node.
- 4. Click Create Data Agent Upgrade.
- 5. Specify the information for the upgrade job in the appropriate fields.
- Click File → Save in the menu bar to save the upgrade definition. The agents you specified will be upgraded at the scheduled time.

#### Upgrading the Data agents using the installation program

This topic describes how to upgrade the Data agent locally using the installation program.

To upgrade a Data agent using local installation, complete the following steps:

- 1. Log in the system with administrator authority on Windows or root authority on UNIX or Linux operating system.
- 2. If the login user specifies the account name for the Tivoli Common Agent Services account on Windows and that user ID exists, then the user must have administrator authority and Log on as a service rights.
- 3. Start the IBM Tivoli Storage Productivity Center installation program.
- 4. The Select a language panel is displayed. Select a language and click OK.
- 5. The Software License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select I accept the terms of the license agreement. Click **Next**.
- 6. The Select the type of installation panel is displayed. Select Custom installation. Click **Next**.
- 7. The Select one or more components to install panel is displayed. Select **Data Agent** to upgrade the Data agent. Click **Next**.
- **8**. The Data server, Device server, Data agent, and Agent Information panel is displayed. This panel should have the following information filled in for:

Data Server Name Data Server Port Device Server Name Device Server Port

Click Next.

If you click Data **Agent Options**, you will be able to select whether or not you want the agent to perform an initial scan when first brought up. You can also select whether or not the agent can run scripts sent by the server. Make your selections and click **OK**. The options are:

#### Agent should perform a scan when first installed

Clear the check box for this option if you do not want Data Manager to perform an initial scan of your storage upon installation. This option is checked by default and gathers default statistics.

#### Agent may run scripts sent by server

Leave this option checked if you want to store scripts in the server's \scripts directory that will run on all agents. When a script needs to be run on a particular agent, the server will access that script from its local \scripts directory and send it to the appropriate agent.

If you clear the check box for this option, the agents will ignore scripts sent by the server. You will have to store a copy of every script in every agent's \scripts directory.

The default **\scripts** directory for an agent behaves as described below:

If a script with the same name exists on both the server and the agent, the script stored on the agent will take precedence. This is useful if you want to run a special version of a script on one agent that is different from the version you are running on all the other agents.

The following example demonstrates the advantage of storing scripts at the server level. To monitor a computer's file system free space, you can store a script on the server that runs when any computer on the network meets a specified low file system free space threshold condition. But you could also store a special script on one computer that defined a different threshold for that computer. This script would take precedence over the script stored on the server.

The default directory for the \scripts directory is as follows: C:\Program Files\IBM\TPC\data\scripts (for Windows)

/opt/IBM/TPC/data/scripts (for UNIX or Linux)

**9**. The Agent Manager information panel is displayed. This information should be filled in by the installation program:

Hostname or IP Address Port (Secured) Port (Public) Password

Click Next.

- 10. The Common agent selection panel is displayed. You can install a new Common agent or use an existing Common agent. Select Select an existing Common agent from the list below. Enter the port that the Data agent will use to listen and communicate with the Common agent. The default port is 9510. You can also specify to download the truststore certificate from the Agent Manager. Click Next. If you have an existing Common agent already installed, select Select existing Common agent from the list below. The table will list the Common agents you have installed. Select a Common agent and click Next.
- 11. If you want to enter Windows service information, click Windows Service Info. The Tivoli Common Agent Services Information panel is displayed. This information is optional. You can enter a Tivoli Common Agent Services name, user ID and password that the installation program will use to create a Windows service for the Common agent. Enter the information and click OK. Click Next on the Common agent information panel.
- **12.** The Summary Information panel is displayed. Review the information. Click **Install**.
- 13. You will see the installing panel. Wait for installation to complete.
- 14. The Successfully Installed panel is displayed. Click Finish.

## **Upgrading the Fabric agents**

This topic describes how to upgrade the Fabric agents using the local installation program.

To upgrade a Fabric agent using local installation, complete the following steps:

- 1. Log in the system with administrator authority on Windows or root authority on UNIX or Linux operating system.
- 2. If the login user specifies the account name for the Common agent Service account on Windows and that user ID exists, then the user must have administrator authority and Log on as a service rights.
- 3. Start the IBM Tivoli Storage Productivity Center installation program.
- 4. The Select a language panel is displayed. Select a language and click OK.
- 5. The Software License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select I accept the terms of the license agreement. Click **Next**.

- 6. The Select the type of installation panel is displayed. Select Custom installation. Click **Next**.
- 7. The Select one or more components to install panel is displayed. Select Fabric Agent. Click Next.
- **8**. The Data server, Device server, Data agent, and Agent Information panel is displayed. This panel should have the following information filled in for:

Data Server Name Data Server Port Device Server Name Device Server Port

Click Next.

**9**. The Agent Manager information panel is displayed. This information should be filled in by the installation program:

Hostname or IP Address Port (Secured) Port (Public) Password

Click Next.

- 10. The Common agent selection panel is displayed. You can install a new Common agent or use an existing Common agent. Select Select an existing Common agent from the list below. Enter the port that the Data agent will use to listen and communicate with the Common agent. The default port is 9510. You can also specify to download the truststore certificate from the Agent Manager. Click Next. If you have an existing Common agent already installed, select Select existing Common agent from the list below. The table will list the common agents you have installed. Select a Common agent and click Next.
- 11. If you want to enter Windows service information, click **Windows Service Info**. The Common agent Service Information panel is displayed. This information is optional. You can enter a Common agent service name, user ID and password that the installation program will use to create a Windows service for the Common agent. Enter the information and click **OK**. Click **Next** on the Common agent information panel.
- 12. The Summary Information panel is displayed. Review the information. Click **Install**.
- **13**. You will see the installing panel. Wait for installation to complete.
- 14. The Successfully Installed panel is displayed. Click Finish.

## Upgrading the Fabric agents remotely

This topic describes how to upgrade the Fabric agents remotely.

To upgrade a Fabric agent remotely, complete the following steps:

- 1. Log in the system with administrator authority on Windows or root authority on UNIX or Linux operating system.
- 2. Start the IBM Tivoli Storage Productivity Center installation program.
- 3. The Select a language panel is displayed. Select a language and click OK.
- 4. The Software License Agreement panel is displayed. Read the terms of the license agreement. If you agree with the terms of the license agreement, select I accept the terms of the license agreement. Click **Next**.
- 5. The Select the type of installation panel is displayed. Select Custom installation. Click **Next**.

- 6. The Select one or more components to install panel is displayed. Select **Remote Fabric Agent**. Click **Next**.
- 7. The List or Remote Hosts panel is displayed. The remote hosts listed have common agents installed on them, and are running under the operating systems that support the Fabric agent. You can select some or all of the remote hosts that you want to deploy your agents to. Make your selection and click **Next**.
- **8**. The Confirmation panel is displayed showing the list of remote hosts you have selected. Read the information and click **Next**.
- **9**. A Progress panel is displayed. When the agents have been deployed, click **Next** to continue.
- **10.** The Summary Information panel is displayed which shows a list of successful and failed deployments. Click **Next** to exit the installation program.

#### Migrating a Storage Resource agent to a Data agent

This topic provides information about how to migrate a Storage Resource agent to a Data agent when the Storage Resource agent is running as a non-daemon or daemon service.

You can migrate a Storage Resource agent to a Data agent in the following ways:

- A remote installation of a Data agent from the server (on a system where a Storage Resource agent resides)
- Local installation of the Data agent on a system (on a system where a Storage Resource agent resides)
- Through silent installation of the Data agent (on a system where a Storage Resource agent resides)

When you install a Data agent on the system that has a Storage Resource agent, the installation program informs you that there is a Storage Resource agent installed. The program also informs you that if you continue with the installation, the Data agent will replace the Storage Resource agent.

After the Data agent is installed, a probe is invoked as part of the installation process. Wait for the probe to finish. After the probe has completed successfully, the Data server information from the Storage Resource agent is deleted. If there are no Data servers in the Storage Resource agent configuration file, then the Storage Resource agent is uninstalled from the system. The IBM Tivoli Storage Productivity Center database is updated to reflect the Data agent installation.

If the Storage Resource agent is running as a non-daemon service, select an available port for the Data agent before migrating.

If the Storage Resource agent is running as a non-daemon service and points to multiple servers, select an available port for the Data agent before migrating. You cannot use the same port as the Storage Resource agent because this agent will be pointing to other servers.

If the Storage Resource agent is running as a daemon service and points to a single server, you can use the same port for the Data agent as is used for the Storage Resource agent. If the Storage Resource agent is running as a daemon service and points to multiple servers, select an available port for the Data agent before migrating. You cannot use the same port as the Storage Resource agent because this agent will be pointing to other servers.

For information about installing a Data agent using the installation wizard, see "Installing the agents" on page 241.

## Upgrading the CIM agent for storage subsystems

This topic provides information about upgrading the CIM agent for the storage subsystems.

Before you upgrade the CIM agent, review the "Supported Products" list for Tivoli Storage Productivity Center 4.1. Go to http://www-304.ibm.com/systems/ support/storage/software/. Click **Install** and you will see a "Supported Products" list on the left side of the pane. Make sure that Tivoli Storage Productivity Center supports the CIM agent you want and is compatible with the firmware versions of your storage subsystems. If you are uncertain about the CIM agent support, it is suggested that you contact IBM customer support to help you with your upgrade plans.

To upgrade the CIM agent, follow these steps:

- 1. Stop all Tivoli Storage Productivity Center server activity that might be dependent on the CIM agent (for example, performance monitor jobs, and discovery or probe jobs).
- 2. Stop the Tivoli Storage Productivity Center server services.
- **3.** If any Tivoli Storage Productivity Center server processes remain, shut down the Tivoli Storage Productivity Center server for the duration of the CIM agent upgrade. If it is not possible to shut down the Tivoli Storage Productivity Center server, stop or kill the running processes.
- 4. Upgrade the CIM agent.
  - a. Refer to the CIM agent provider's instructions to perform the upgrade.
  - b. Verify that the CIM agent configuration is intact after the upgrade (make sure that user accounts and passwords used with Tivoli Storage Productivity Center are still in place, and that all devices managed by the CIM agent are still listed).
- **5**. Restart the Tivoli Storage Productivity Center server and Tivoli Storage Productivity Center server services.
- 6. Open the IBM Tivoli Storage Productivity Center GUI.
- 7. Run a CIMOM discovery job.
- 8. Run a probe job for each storage subsystem that is managed by the CIM agent.

After the probe job is finished, you will see the following changes or limitations:

- The CIM agents for 5.3 and 5.2.1 model only logical disk drives. The Tivoli Storage Enterprise Storage Server used eight disk drives in a V8Pack in the CIM agent for 5.1. The CIM agents for 5.3 and 5.2.1 show only seven usable disk drives and do not care about the parity disk drive.
- If you upgraded to the CIM agent for 5.3, note that Tivoli Storage Productivity Center does not show configuration information or performance data for space efficient volumes.

## Upgrading the SAN Volume Controller CIM agents

This topic provides information about upgrading the CIM agent for the SAN Volume Controller.

IBM Tivoli Storage Productivity Center enables you to upgrade your SAN Volume Controller CIM agent directly from an older version to a newer version. After the upgrade, Tivoli Storage Productivity Center will identify the SAN Volume Controller cluster again and keep all data in the database associated with this SAN Volume Controller cluster. You can do one of the following:

- Upgrade the agent directly. See "Upgrading the SAN Volume Controller CIM agents directly."
- Install the newer agent from a different master console, and then remove the older agent. See "Adding a SAN Volume Controller CIM agent on a different master console."

Do not manage the same SAN Volume Controller cluster with SAN Volume Controller CIM agents of different release versions. For example, if you have a cluster named "Einstein" you can manage Einstein with two SAN Volume Controller CIM agents on 4.2.0, or with two SAN Volume Controller CIM agents on 4.3.1. Do not attempt to manage Einstein or any other SAN Volume Controller cluster with one SAN Volume Controller CIM agent on 4.2.0 and the other CIM agent on 4.3.1.

Starting with SAN Volume Controller 4.3.1 or later, the CIM agent is embedded in the hardware.

## Upgrading the SAN Volume Controller CIM agents directly

This topic provides information about upgrading the CIM agent for the SAN Volume Controller from version 4.2 to version 4.3.1 by directly upgrading the SAN Volume Controller CIM agent.

After upgrading the SAN Volume Controller CIM agent to version 4.3.1, complete the following steps inIBM Tivoli Storage Productivity Center. See the SAN Volume Controller information center at http://publib.boulder.ibm.com/infocenter/svcic/v3r1m0/index.jsp for information about upgrading SAN Volume Controller CIM agents.

- 1. Upgrade or install Tivoli Storage Productivity Center to 4.1.
- 2. Open the Tivoli Storage Productivity Center user interface.
- 3. Run a CIMOM discovery job. In the navigation tree, expand Administrative Services → Discovery, right-click CIMOM, and click Run Now. For detailed instructions, see the section about discovering CIM agents automatically in the *IBM Tivoli Storage Productivity Center User's Guide*.
- 4. Run a probe job for the upgraded CIM agent. In the navigation tree, expand Tivoli Storage Productivity Center → Monitoring → Probes. For detailed instructions, see the section about creating probes in the *IBM Tivoli Storage Productivity Center User's Guide*.

## Adding a SAN Volume Controller CIM agent on a different master console

This topic provides information about upgrading the CIM agent for the SAN Volume Controller from an older version to a newer version from a different

master console. You would then remove the old CIM agent. This enables you to ensure that the upgrade runs smoothly before uninstalling the older version.

Complete the following steps to upgrade the SAN Volume Controller CIM agent to a new version by first installing the newer version, and then removing the older version:

- 1. Install or upgrade to IBM Tivoli Storage Productivity Center to 4.1.
- 2. Install (add) the new version of SAN Volume Controller CIM agent from a different master console. Follow the instructions provided with your SAN Volume Controller.
- 3. Open the Tivoli Storage Productivity Center user interface.
- 4. Add the new SAN Volume Controller CIM agent. In the navigation tree, expand Administrative Services → Data Sources and click CIMOM Agents. In the right pane, click Add CIMOM. For detailed instructions, see "Adding a CIM agent manually" on page 430.
- Run a CIMOM discovery job. Expand Administrative Services → Discovery, right-click CIMOM, and click Run Now. For detailed instructions, see "Discover CIM agents automatically" on page 432.
- 6. Remove the old version of the SAN Volume Controller CIM agent. Follow the instructions provided with your SAN Volume Controller.
- 7. Run a CIMOM discovery job as described in step 5.
- Run a probe job for the upgraded CIM agent. In the navigation tree, expand IBM Tivoli Storage Productivity Center → Monitoring → Probes. For detailed instructions, see the section about creating probes in the IBM Tivoli Storage Productivity Center User's Guide.

### Configuring IBM System Storage N Series Gateway servers

Follow this procedure to configure IBM Tivoli Storage Productivity Center before adding N Series Gateway servers using the **Other NAS** node.

#### Deleting and un-licensing existing N Series Gateway servers

If you are upgrading IBM Tivoli Storage Productivity Center from IBM TotalStorage Productivity Center 3.3.x, there are specific steps to follow. You must first delete and un-license existing N Series Gateway servers before adding the N Series Gateway servers.

Follow these steps:

- 1. Stop all IBM Tivoli Storage Productivity Center services.
- 2. Make a backup copy of the IBM Tivoli Storage Productivity Center database.
- 3. Open the IBM Tivoli Storage Productivity Center GUI.
- 4. Manually delete all N Series Gateway servers.
  - a. Expand Administrative Services > Configuration > Manual NAS/Netware Server Entry.
  - b. Select a NAS gateway server (for example, ratbert1) from the Manual NAS/Netware Server table.
  - c. Click **Delete**.
  - d. Click Yes to Delete Manual NAS/Netware Server Entry prompt.
  - e. Repeat steps b through d for other manually added NAS gateway servers.

rigation Tree					Add NAS Server	Add No	tware Server	Delet
Services	-	Server	Network Name	OS Type	Domain or N	DS Tree	Unix Computer	
Data Sources		ratbert1.srm.storage tu	cson.lom.com.inatbert1	NetApp De	ta ONTAP SRM	-248.005		
Discovery								
-Configuration		Delete Manual N	AS/Netware Server Entry			×		
License Keys								
Alert Disposition		Peleting	this entry will cause the deletion	of all collecte	d statistics for server rat	sert1.		
August Dispusation						#20.563		
-Log-File Retention								
Log-File Retention Quota and Constraint e-mail Address Rules			[Ver]	No. 1				

Figure 78. Delete Manual NAS/Netware Server Entry prompt

- 5. Un-license all NAS gateway servers that were automatically discovered
  - a. Click Administrative Services > Configuration > License Keys.
  - b. Expand IBM TPC for Data under the Licensing tab.
  - **c.** Clear the Licensed check box for all automatically discovered NAS gateway servers (for example, zinc).
  - d. Click on the disk icon to save the changes.
  - e. Click Yes to the Save Confirmation prompt.

angaior nee	Licensing Filer Logins					
Administrative Services	IBM TPC for Data Purchased Licen	ses: Unimited Uni	used Licen	ises: Unlimited		
Usta Sources Discovery				Se	siect All	Deselect
Out of Band Fabric	Computer 🛦	OS Type	Domain	Tree Name	Licensed	
Hetware Filer	Gong storage tucson ibm.com	AIX	1	1	<b>V</b>	
-Windows Domain, NAS, and SAN FS	tpcblade1-2.srm.storage.tucson.ibm.com	Windows	SRM		R.	
Where VI Data Source	zinc.srm.storage.tucson.ibm.com	NetApp Data ONTAP	SRM			
Configuration						
- Role-to-Group Mappings - Konos Koys - Alert Disposition - Log-file Retention - Quota and Constraint e-mail Address Rules - Scan Brobe Agent Administration - Manual HASNetware Server Entry - Manage Element Manager - Agent Manage Server Entry	Save Confirmation  Configuration  Co	r will result in the dek . Data Agent will be s t to save your change	etion of uninstalled a is?	s well.		

Figure 79. Save Confirmation prompt

**Note:** The OS Type and Licensed fields of existing NAS gateway servers are updated once it is manually added as **Other NAS**. See "Manually adding an N Series Gateway server ."

- 6. Exit the IBM Tivoli Storage Productivity Center GUI.
- 7. Make another backup of the IBM Tivoli Storage Productivity Center database after the N Series Gateway servers are deleted and unlicensed (make sure all IBM Tivoli Storage Productivity Center services are stopped).
- 8. Restart all the IBM Tivoli Storage Productivity Center services.
- 9. Go to "Manually adding an N Series Gateway server ."

#### Manually adding an N Series Gateway server

- 1. Start the IBM Tivoli Storage Productivity Center GUI.
- 2. Manually add the N Series Gateway server as Other NAS.
  - a. Click Administrative Services > Configuration > Manual NAS/Netware Server Entry.
  - b. Click Add NAS Server.

- c. Enter information for the Network Name, Accessible from, SNMP Community, Login ID, and Password fields for an N Series Gateway server (for example, **ratbert1**).
- d. Check the Add as Other NAS check box.
- e. Enter the NAS Server Vendor Name or accept the Network Appliance as the default.
- f. Click **OK** to save the input. This enables IBM Tivoli Storage Productivity Center to verify the NAS gateway server information and discover CIFS or NFS shares accessible to the selected Data agent.

vigation Tree		Add MAC County	Ander Aberbaumen Company	f in reason
Administrative Services		Multi Ners Server	Auto Necertare Server	
Services			No Data to Display	
Date Sources	Add NAS Source			
Oiscovery				
	Network name:			
Out of Band Fabric	ratbert1			
Netware Filer	-Data Manager Agent OS Type			
Windows Domain, NAS, and SAN FS				
VMware VI Data Source	Windows C Unix			
Configuration				
-Role-to-Group Mappings	Accessible from			
-License Keys	tocklade1-2.srm.storage.tucson.ibm.com *			
Alert Disposition	State Community			
Log-File Retention	Dura to			
Quota and Constraint e-mail Address Rules	PUBL			
-ScanProbe Agent Administration	Login ID:			
Manual NAShetware Server Entry	administrator			
Manage Element Manager				
Agent Manager Registration	Pessword			
History Aggregator	******			
- Luta Agent upgrades				
Metware tree Logins	Add as Other NAS			
Resource history Retention	NAC Conver Vander Name			
Removed Resource Retention	Net server verkur Narie			
Descend Descences Detection for Detabases	Interwork Apparance			
Configuration History Settings				
10M TotalStorage Productinity Center				
Configuration Ibility				
Rollup Reports	OK Carral			
- Auget				
E Database Asset				

Figure 80. Add NAS Server panel

g. Verify that the N Series Gateway server is added and listed with **Other NAS** as OS Type.

Element Management						
rvigation Tree				Add NAS Server	Add Netware Server	Delete
Services	Server	Network Name	OS Type	Domain or HDS Tree	Unix Computer	
-Data Sources	Fatbert1.storage tu	coon ibm.com retbert1	Other NAS	SRM		
Discovery						
Configuration						
Role-to-Group Mappings						
-License Keys						
Alert Disposition						
-Log-File Retention						
-Quota and Constraint e-mail Address Rules						
Scan,Probe Agent Administration						
Manual NAS.Netware Server Entry						

Figure 81. Verify that the N Series Gateway server is added

- h. Repeat steps b to g for other N Series Gateway servers.
- **3**. Assign a Scan/Probe agent or agents to the exported CIFS or NFS shares accessible to the selected Data agent or agents.
  - a. Click Administrative Services > Configuration > Scan/Probe Agent Administration.
  - b. Select one or more file systems (for example, /vol/tpc1, /vol/tpc2, and /vol/vol0 for ratbert1) and assign the Data agent by clicking **Set agent per row** or **Set agent** for all the selected rows.

vigation Tree				Set a	gent per row	Set egent for all selected ro
Services	Server	Domain	Tree Name	Filesystem	Scan.Probe A	Vgent
Data Sources	oxide srm storage tucson ibm.com	SRM	1	NolvolD		
Discovery	oxide srm storage tucson ibm.com	SRM		Avail/val2		
-Configuration	rativent1 storage tucson ibm.com	SEM	-	Noitec1		
-Role-to-Group Mappings	rativent1 storage tucson iten com	SRM		Noition2		
-License Keys	rativenti, storage tuccon ites com	SSM		-		
-Alert Disposition						
-Log-File Retention						
Quota and Constraint e-mail Address Rules	- Michtypice	n Agent Le	litor			
ScanProbe Agent Administration	Select an	agent a	wd click 'OK	5		
Manual NASINetware Server Entry	Use the s	ave butte	on on the to	ol bar to sa	we	
Manage Element Manager	your edit:	s.				
Winters Americanter						
C Data Acast Dogrados	Server	ratbe	rt1.storage.tucso	n.lbm.com		
HelWare Tree Loging	Domain	SRM				
Resource History Retention	Tree Name					
Removed Resource Retention						
Resource History Retention for Databases	Filesystem	Noltp	xc1			
Removed Resource Retention for Databases	Scen/Probe A	nent Itochi	lacie1-2 arm store	age bucson ibm co	m w	
Configuration History Settings	2022/01/2022/2	Saura Taran				
BM TotalStorage Productivity Center						
-Configuration Utility						
Rollup Reports		0	K Cancel	12		
(i) Areat						

Figure 82. Filesystem Agent Editor panel

c. Click OK to save the assignment.

igation Tree					Set a	pent per row	Set agent for all selected n
Administrative Services	-	Server	Domain	Tree Name	Filesystem	ScanProbe	Agent
Data Sources		oxide.sm.storage.tucson.ibm.com	SRM		Nol/vol0	1	
Discovery		oxide.sm.storage.tucson.ibm.com	SRM		Nol/vol2		
Configuration		ratbert1.storage.tucson.ibm.com	SRM		Avolitpc1	tpcblade1-2.s	rm.storage tucson ibm.com
Role-to-Group Mappings		ratbert1.storage.tucson.ibm.com	SRM		Nolfpc2	tpcbiade1-2.s	rm.storage tucson lom.com
License Keys		ratbert1.storage.tucson.ibm.com	SRM		Nol/volD	tpcblade1-2.s	rm.storage tucson lom.com

Figure 83. Scan/Probe Agent Administration panel

- d. Repeat steps b and c for other file systems (for example, /vol/vol0 and /vol/vol2 for oxide).
- e. Click the disk icon to save the **Scan/Probe Agent assignment** (so that the N Series Gateway servers and their file systems can be displayed when a probe or scan job is run).
- 4. Create a probe job to probe one or more N Series Gateway servers.
- 5. Create a scan job to scan one or more file systems from the N Series Gateway servers.
- 6. View asset report on a NAS gateway server and its file systems as Other NAS.
  - a. Click Administrative Services > Data Manager > Reporting > Asset > By OS Type > Other NAS.
  - b. Click on an N Series Gateway server (for example, ratbert1) to view information for the server.



Figure 84. View information for N Series Gateway server

**c**. Click on a file system (for example,, /vol/tpc2) to view file system information.

Navigațion Tree	File System	
Alerting     Alerting     Alerting     Policy Wangement     Reporting     Groups     Asset     Policy Wangement     Begruiter     Poly Computer     Poly Opporter     Poly Oppoly     Poly Oppoly     Poly Opporter     Poly Oppoly     Poly Oppo	Computer File System Type Use Court Mourt Port Physical Size Capachy Probe Last Run Scan Last Run Descene The Reaching File Maximum File Court Used Houtes Used Space	ratbert1 storage tucson.km.com NTFS4 1 Not6pc2 0 12000 MB Nov 10, 2000 10.38 27 MA Nov 10, 2000 10 MA Nov 1

Figure 85. View information for a file system

- 7. You can see the following information and reports for Other NAS:
  - a. Dashboard
  - b. System reports
  - c. Batch reports
  - d. Asset reports
  - e. Capacity reports
    - Capacity reports Charting
  - f. Usage reports
    - Usage reports Filesystem Quota Violation

- Capacity reports Charting
- 8. You can monitor the N Series Gateway servers and create and monitor alerts for **Other NAS**:
  - Monitoring
    - Monitoring Assign a Scan agent to a Filesystem
    - Monitoring Grouping
    - Monitoring Scan job
    - Monitoring Filesystem Quotas
  - Alerting
    - Filesystem Alert definition
    - Alerting Directory Alerts
    - Alerting Alert Log
    - Alerting Alerts shown on the topology

# Chapter 5. Uninstalling the IBM Tivoli Storage Productivity Center family

This section provides procedures for uninstalling the IBM Tivoli Storage Productivity Center family. The programs must be uninstalled in a specific order.

Uninstall the components and related software in this order:

- 1. IBM Tivoli Storage Productivity Center:
  - Data agent, Fabric agent, GUI, or CLI (these components are uninstalled using the Tivoli Storage Productivity Center uninstallation program)
  - Data Server or Device server (these components are uninstalled using the Tivoli Storage Productivity Center uninstallation program). When you are uninstalling the Device server and Data Server, you must also uninstall the DB2 database (remote or local) that was used by the Device server and Data Server.
  - DB schema (this is uninstalled using the Tivoli Storage Productivity Center uninstallation program)
  - Agent Manager
- 2. IBM Tivoli Storage Productivity Center for Replication
- 3. DB2 (optional)

The agents are composed of the Common agent and one or more Data agents and Fabric agents. When you uninstall the Data agent and Fabric agent, the last agent to be uninstalled will also uninstall the Common agent.

#### Note:

- When uninstalling Tivoli Storage Productivity Center on AIX and Linux systems, you must have some free space on the hard drive to start the uninstall program. This space is not checked by the uninstall program. You must have at least 50 KB of free space in /tmp and 10 KB of free space in /etc.
- When you uninstall Tivoli Storage Productivity Center on Windows, there might be some directories or files that remain even if the uninstallation indicates that the operation was successful. If you do not delete all Tivoli Storage Productivity Center entries, you will not be able to reinstall Tivoli Storage Productivity Center. After uninstalling Tivoli Storage Productivity Center, check the C:\Program Files\IBM directory for any TPC entries. Delete any TPC entries and then reinstall Tivoli Storage Productivity Center.

## Uninstalling the IBM Tivoli Storage Productivity Center family using the uninstallation program

This procedure provides information about uninstalling IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication.

#### Note:

• If you are using the LDAP server for authentication, you must make sure that the LDAP server is up and running before uninstalling IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication.

To uninstall Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication, complete the following steps:

- 1. Log on to the system as a local administrator with administrative authority on Windows. You must also have database administrative authority if you are removing the database schema. For UNIX and Linux, you must have root authority.
- 2. Exit the Tivoli Storage Productivity Center GUI.
- **3**. Before uninstalling, you must also make sure that the IBM ADE Service is running. To check for this service on Windows, click **Start > Control Panel > Administrative Tools > Services**. To check for this service on AIX or Linux, run the following command:

```
ps -aef | grep acsi
```

For information about starting the IBM ADE Service, see "Starting the IBM Tivoli Storage Productivity Center services" on page 465.

 For Windows, click Start > Settings > Control Panel > Add/Remove Programs. Highlight IBM Tivoli Storage Productivity Center and click Remove.

When you run the uninstallation program for AIX or Linux, run the uninstallation program **outside** of the installation directory tree. For example, if you installed Tivoli Storage Productivity Center on /opt/IBM/TPC, run the uninstallation program from another directory:

```
. ~db2inst1/sqllib/db2profile # (source the file)
/opt/IBM/TPC/_uninst/uninstall
```

- 5. The select a language panel is displayed. Select a language and click OK.
- 6. The Welcome panel is displayed. Click Next.
- 7. Select one or more components to uninstall panel is displayed. Select the components you want to uninstall. Click **Next**.

🕲 IBM Tivoli Storage Pro	ductivity Center - Installer	
	Select one or more components	to uninstall from your local computer.
IBK.	🗹 Drop database schema 4.1	.0.73
0		DB Admin Info
A	🔽 Data Server 4.1.0.73	Device Server4.1.0.73
	🔽 GUI 4.1.0.73	CLI 4.1.0.73
	🔽 Data Agent 4.1.0.73	🔽 Fabric Agent 4.1.0.73
	Replication Server	
	🗖 Unregister Launch Informa	ion With Other Applications
WEE	By default, the Common Agent the option below to force the rea local computer.	s uninstalled when the last subagent is uninstalled. Check noval of the common agent and its subagents from your
AND -	Force uninstallation of Com	mon Agent
	< <u>B</u> ack	<u>N</u> ext ≻ <u>C</u> ancel

Figure 86. Select one or more components to uninstall panel

If you click **DB** Admin Info, a panel is displayed allowing you to enter the DB2 administrator user ID and password.

You normally do not need to select the **Force uninstallation of the common agent** option. You might use this option in cases where the Data agents and Fabric agents have been manually uninstalled and there are currently no agents running on the system. Only select this option if you wish to remove (or have removed) all Tivoli agents from the system. Another case in which you might use this option would be if you have a failed uninstallation and need to clean up the system.

The Unregister Launch Information With Other Applications option lets you uninstall the Tivoli Storage Productivity Center portlets in a non-Tivoli Integrated Portal instance that was not installed by Tivoli Storage Productivity Center. This is useful for users who have other instances of Tivoli Integrated Portal installed (a Tivoli Integrated Portal that is not installed by Tivoli Storage Productivity Center). If you select this option, the Tivoli Storage Productivity Center portlets will be uninstalled from the instance of Tivoli Integrated Portal that was not installed by Tivoli Storage Productivity Center.

- 8. The Summary Information panel is displayed. Review the information and click **Uninstall**.
- **9**. The Uninstalling panel is displayed. This panel indicates what component is being uninstalled.
- When the program uninstalls Tivoli Storage Productivity Center for Replication, you will see the following panel. Select IBM Tivoli Storage Productivity Center for Replication. Click Next.



Figure 87. Select the features for IBM Tivoli Storage Productivity Center for Replication uninstall panel

- 11. The summary panel for IBM Tivoli Storage Productivity Center for Replication is displayed. Review the information and click **Uninstall**.
- 12. The status panel for uninstallation is displayed.
- 13. The successfully uninstalled panel is displayed. Click Finish.
- 14. The panel for uninstalling other components is displayed. The following components are uninstalled:
  - IBM Tivoli Integrated Portal
  - Fabric agent
  - Data agent
  - Device server
  - Database schema
- 15. The successfully uninstalled panel is displayed. Review the information. Click **Finish**.
- **16**. The Restart Your Computer panel is displayed (for Windows only). To restart your computer, click **Yes**, **restart my computer**. Click **Finish** to complete the uninstallation operation.

#### Note:

- If the JRE directory remains after a successful uninstall on Windows, manually delete the JRE directory.
- The IBM Tivoli Integrated Portal will be uninstalled along with IBM Tivoli Storage Productivity Center unless another application is using the program. If another application is using IBM Tivoli Integrated Portal, then restart IBM Tivoli Integrated Portal after the IBM Tivoli Storage Productivity Center uninstallation operation.

To restart IBM Tivoli Integrated Portal:

#### On Windows

Restart the IBM Tivoli Integrated Portal service.

#### On AIX or Linux

Go to the following directory: <install\_dir>\tip\profiles\TIPProfile\bin\ Enter the following command:
startServer server1 -username <tipadmin> <mypassword>

Where *<tipadmin>* is the administrator user ID and *<mypassword>* is the administrator password. Wait for the server to complete the operation.

17. After you uninstall IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication, and if no other applications are using IBM Tivoli Integrated Portal, you must make sure that IBM Tivoli Integrated Portal is also uninstalled. If IBM Tivoli Integrated Portal has not been uninstalled, you must manually remove the files left by IBM Tivoli Integrated Portal. For the IBM Tivoli Integrated Portal cleanup procedure, see "Tivoli Integrated Portal cleanup procedure on Windows" on page 591 or "Tivoli Integrated Portal cleanup procedure on UNIX or Linux" on page 592.

## Uninstalling IBM Tivoli Storage Productivity Center for Replication with InstallShield

InstallShield is the recommended method for uninstalling IBM Tivoli Storage Productivity Center for Replication.

Tivoli Storage Productivity Center has its own uninstallation wizard. Ensure you have completed the Tivoli Storage Productivity Center uninstalling procedures before completing the IBM Tivoli Storage Productivity Center for Replication uninstalling wizards.

#### Note:

- If you are using the LDAP server for authentication, you must make sure that the LDAP server is up and running before uninstalling IBM Tivoli Storage Productivity Center for Replication.
- Windows users can also uninstall IBM Tivoli Storage Productivity Center for Replication by clicking Start -> Settings -> Control Panel -> Add or Remove Programs.

To uninstall IBM Tivoli Storage Productivity Center for Replication:

- To start the uninstallation wizard, go to the *base\_installation\_dir*\TPCRM\_uninst folder, where *base\_installation\_dir* is the directory in which you installed the product. Then run the uninstaller.bin file (AIX and Linux) or the uninstaller.exe (Windows).On Windows, the default location is C:\Program Files\IBM\replication\TPCRM\_uninst. On AIX and Linux, the default location is /opt/IBM/replication/TPCRM\_uninst.
- 2. InstallShield displays the welcome page. Click Next to continue.
- **3**. InstallShield displays a list of the features that can be uninstalled. There is only one feature, IBM Tivoli Storage Productivity Center for Replication. A summary of the previous steps including the features that you selected to uninstall. If the summary is correct, click **Uninstall**. A progress bar shows percentage complete.

## Uninstalling IBM Tivoli Storage Productivity Center for Replication manually

You can manually uninstall IBM Tivoli Storage Productivity Center for Replication.

## Uninstalling IBM Tivoli Storage Productivity Center for Replication manually on Windows

You can manually uninstall IBM Tivoli Storage Productivity Center for Replication on Windows.

IBM Tivoli Storage Productivity Center has its own uninstallation program. Ensure you have completed the IBM Tivoli Storage Productivity Center uninstalling procedures before completing the IBM Tivoli Storage Productivity Center for Replication uninstalling procedure.

**Note:** If you are using the LDAP server for authentication, you must make sure that the LDAP server is up and running before uninstalling IBM Tivoli Storage Productivity Center for Replication.

- 1. Click Start-> Settings > Control Panel->Administrative Tools -> Services.
- **2.** If IBM WebSphere Application Server V6.1 -CSM is listed, stop the service by right-clicking and selecting **Stop**.
- 3. From a command prompt, issue the following command: <install\_location>/eWAS/bin/wasservice.exe -remove CSM

where *<install\_location>* is the directory where you installed IBM Tivoli Storage Productivity Center for Replication.

**Note:** The default installation directory is c:\Program Files\IBM\replication\ eWAS\bin.

- 4. Delete the directory where you installed IBM Tivoli Storage Productivity Center for Replication.
- 5. If you want to delete the IBM Tivoli Storage Productivity Center for Replication database, connect to DB2 and issue the following command: drop database *dbname*, where *dbname* is the name of the IBM Tivoli Storage Productivity Center for Replication database.

## Uninstalling IBM Tivoli Storage Productivity Center for Replication manually on AIX and Linux

You can manually uninstall IBM Tivoli Storage Productivity Center for Replication on AIX and Linux.

IBM Tivoli Storage Productivity Center has its own uninstallation wizard. Ensure you have completed the IBM Tivoli Storage Productivity Center uninstalling procedures before completing the IBM Tivoli Storage Productivity Center for Replication uninstalling procedure.

**Note:** If you are using the LDAP server for authentication, you must make sure that the LDAP server is up and running before uninstalling IBM Tivoli Storage Productivity Center for Replication.

1. From a command prompt, issue the following command to stop the WebSphere Application Server process:

<installRoot>/eWAS/profiles/CSM/bin/stopServer.sh server1

where *<installRoot>* is the location where WebSphere Application Server is installed. If this command fails, perform the following steps:

- a. From a command prompt, issue the following command to obtain the process ID (PID) for the IBM Tivoli Storage Productivity Center for Replication service: ps -ef | grep CSM
- b. To stop the service, issue the following command: kill -9 <*pid>*, where <*pid>* is the PID obtained in the previous step.
- 2. Delete the directory where the IBM Tivoli Storage Productivity Center for Replication was installed.
- 3. If you want to delete the IBM Tivoli Storage Productivity Center for Replication database, connect to DB2 and issue the following command: drop db *<dbname>*, where *<dbname>* is the name of the IBM Tivoli Storage Productivity Center for Replication database.
  - **a**. Change to the following directory:
    - . /home/<db2\_instance\_name>/sqllib/db2profile
  - b. Issue the following command:
    - db2 drop db <*dbname*>
- 4. Go to the /etc/inittab directory and edit the inittab file by removing the following entry:

On AIX: /opt/IBM/replication/eWAS/bin/startServer.sh
On Linux: /opt/IBM/replication/eWAS/bin/startServer.sh

## Uninstalling the agents

When you installed the agents, you installed them locally or remotely. These topics describe how to uninstall these agents, both locally or remotely.

These topics describe how to uninstall a local agent and a remote agent.

The Storage Resource agents are uninstalled using the IBM Tivoli Storage Productivity Center GUI.

The Data agents and Fabric agents are composed of the Common agent and one or more Data agent or Fabric agent. When you uninstall the Data agent and Fabric agent, the last agent to be uninstalled will also uninstall the Common agent.

For information about uninstalling the Data agent and Fabric agent in silent mode, see "uninstall.iss file" on page 625.

#### Deleting or uninstalling an agent using the GUI

You can delete or uninstall a Data agent or Storage Resource agent and all the data that is collected by that agent from the database repository. The information that is collected by the agent will no longer be available within IBM Tivoli Storage Productivity Center reports. When you delete an agent, the agent is uninstalled and you can no longer activate the agent.

To delete or uninstall a Data agent or Storage Resource agent, complete the following steps:

- In the navigation tree, click Administrative Services > Data Sources. Left-click Data/Storage Resource Agents.
- 2. In the right pane, select an agent and click **Delete**.

## Uninstalling the Storage Resource agent manually

This section describes how to uninstall the Storage Resource agent manually.

To uninstall the Storage Resource agent, follow these steps:

 Go to the directory where the agent has been installed: <SRA\_install\_location>

Where *<agent\_install\_location>* is where the Storage Resource agent has been installed.

2. Run the uninstallation command:

bin/Agent -uninstall
-serverName <TPC\_server\_name>
-force
-debug MAX

Where:

-force This is an optional parameter that forces an uninstallation. If you use this parameter, you should not provide the server name.

-serverName <TPC\_server\_name>

<*TPC\_server\_name>* is the Data server name as defined in IBM Tivoli Storage Productivity Center. You can check the configuration file for the server name:

<agent\_install\_location>/config/Agent.config

#### -debug MAX

This is an optional parameter for debugging purposes. If you set the **-debug** parameter, then some files will not be deleted.

**Note:** If you run the uninstallation program from the bin directory, then the bin directory will not be deleted.

If you run the uninstallation program outside of the agent installation directory, then you must specify the full path.

If the uninstallation fails, see the return codes in the Information Center. Search for **Return codes used by Storage Resource agent**.

#### Uninstalling the Data agents or Fabric agents locally

This procedure provides information about uninstalling the Data agents for Fabric agents that you have installed locally on your computer.

For agents that have been installed locally, complete the following steps to uninstall the agents:

- 1. Log on to the system as a local administrator with administrative authority on Windows. For UNIX and Linux, you must have root authority.
- For Windows, go to Add/Remove Programs → IBM Tivoli Storage Productivity Center → Remove. This will remove both agents (Data agent and Fabric agent) and the Common agent.
- **3**. Through the uninstallation wizard, options are available to uninstall either the Data agent or Fabric agent or both. The default is set to uninstall both agents. Select the agent to uninstall and click **Next**.
- 4. The Select a language panel is displayed. Select a language and click **OK**.
- 5. The Welcome panel is displayed. Click Next.

6. The Select one or more products to uninstall panel is displayed. Select the agents you want to uninstall. Click **Next**.

You normally do not need to select the Force uninstallation of the Common agent option. You might use this option in cases where the Data agents and Fabric agents have been manually uninstalled and there are currently no agents running on the system. Only select this option if you wish to remove (or have removed) all Tivoli Storage Productivity Center agents from the system. Another case in which you might use this option would be if you have a failed uninstallation and need to clean up the system.

- 7. The Summary Information panel is displayed. Review the information and click **Uninstall**.
- 8. The Uninstalling panel is displayed. Wait for the uninstallation to complete.
- 9. The Successfully uninstalled panel is displayed. Click Finish.
- 10. The Restart Your Computer panel is displayed (for Windows only). To restart your computer, click **Yes, restart my system**. Click **Finish** to complete the uninstallation.

## Uninstalling the Data agents or Fabric agents remotely

This section describes how to uninstall the Data agents or Fabric agents remotely.

#### Uninstalling the remote agents

This procedure provides information about uninstalling the agents on the computer where the agent is installed.

If you have both the Data agent and Fabric agent installed, uninstall the Fabric agent first.

To uninstall the remote agent, complete the following steps:

- 1. Log on to the system as a local administrator with administrative authority on Windows. For UNIX and Linux, you must have root authority.
- 2. Follow these steps for Windows:
  - a. Go to the Add/Remove Programs window and select **IBM Tivoli Storage Productivity Center**. Click **Remove** to start the uninstallation program. This will remove the Fabric agent.
  - b. Then uninstall the Data agent and Common agent. Go to the Add/Remove Programs window and select IBM Tivoli Storage Productivity Center for Data - Agent. Click Remove to start the uninstallation program.
- 3. Follow these steps for UNIX or Linux:
  - a. Go to the following directory and run the ./uninstall command: cd /<usr or opt>/IBM/TPC/\_uninst ./uninstall

This will remove the Fabric agent.

b. Go to the following directory and run the ./uninstall command:

cd /<usr or opt>/IBM/TPC/ca/subagents/TPC/Data ./uninstall.sh (for UNIX) cd /opt/IBM/TPC/ca/subagents/TPC/Data ./uninstall.sh (for Solaris)

- 4. The Select a language panel is displayed. Select a language and click OK.
- 5. The Welcome panel is displayed. Click Next.
- 6. The Select one or more products to uninstall panel is displayed. Select the agents you want to uninstall. Click **Next**.

You normally do not need to select the Force uninstallation of the Common agent option. You might use this option in cases where the Data agents and Fabric agents have been manually uninstalled and there are currently no agents running on the system. Only select this option if you wish to remove (or have removed) all Tivoli Storage Productivity Center agents from the system. Another case in which you might use this option would be if you have a failed uninstallation and need to clean up the system.

- 7. The Summary Information panel is displayed. Review the information and click **Uninstall**.
- 8. The Uninstalling panel is displayed. Wait for the uninstallation to complete.
- 9. The Successfully uninstalled panel is displayed. Click Finish.
- 10. The Restart Your Computer panel is displayed (for Windows only). To restart your computer, click **Yes, restart my system**. Click **Finish** to complete the uninstallation.

#### Uninstalling the remote Data agent through the GUI

This topic provides information on how to uninstall the remote Data agent through the GUI.

To uninstall a Data agent from the IBM Tivoli Storage Productivity Center GUI, follow these steps:

- 1. Open the Tivoli Storage Productivity Center GUI on the server machine.
- 2. Select the Data agent you want to uninstall.
- 3. Right-click on the Data agent and select Delete. If the Data agent is the last agent on the machine, it will correctly uninstall the Common agent as well. If you uninstall the Data agent first on a machine which had other agents installed remotely, you will have to uninstall the Common agent manually on

the machine.

#### Uninstalling the Common agent manually

If you uninstall the Data agent first on a machine which had other agents installed remotely, you will have to uninstall the Common agent manually on the machine.

To uninstall the Common agent, follow these steps:

- For Windows, go to the Add/Remove Programs window and select: IBM Tivoli Common Agent - C:\Program Files\tivoli\ep
- 2. Select Remove.
- **3**. For UNIX or Linux, go to the following directory and run the ./uninstall command:

```
cd /<usr or opt>/tivoli/ep/_uninst
./uninstall (for UNIX or Linux)
cd /opt/tivoii/ep/_uninst
./uninstall (for Solaris)
```

#### Uninstalling agents that were remotely deployed

If you have remotely deployed agents, you must follow a particular sequence to remove the agents. This topic provides information on the sequence.

To uninstall the agents from the agent computer, follow these steps:

1. Uninstall the Data agent. Run this command from the command line:

```
Unix:
    cd /<usr or opt>/IBM/TPC/ca/subagents/TPC/Data/
    ./uninstall.sh
Windows: C:\Program Files\IBM\TPC\ca\subagents\TPC\Data\setup -u
```

2. Through the uninstallation wizard, options are available to uninstall either the Data agent or Fabric agent or both. The default is set to uninstall both agents. Run this command from the command line:

```
Unix:
```

```
/<usr or opt>/IBM/TPC/_uninst/uninstall.sh
Windows:
    C:\Program Files\IBM\TPC\_uninst\uninstall.exe
```

## Uninstalling agents on a Virtual I/O Server

Use the **U** attribute in the **cfgsvc** command to uninstall IBM Tivoli Storage Productivity Center agents on a Virtual I/O Server.

You must log into a Virtual I/O Server as the **padmin** user ID to use this command.

The parameters for uninstalling the agents are:



TPC Required parameter for Tivoli Storage Productivity Center.

-attr U=attribute\_value

*attribute\_value* can be:

- All Uninstalls the Fabric agent and Data agent.
- data Uninstalls the Data agent.

fabric Uninstalls the Fabric agent.

Note: The agent name is case sensitive.

#### Examples

To uninstall the Data agent, enter the following command: cfgsvc TPC -attr U=data

To uninstall the Fabric agent, enter the following command: cfgsvc TPC -attr U=fabric

To uninstall both the Data agent and Fabric agent, enter the following command: cfgsvc TPC -attr U=A11

## **Uninstalling the Language Pack**

This procedure describes how to uninstall the Language Pack.

You must have administrator authority on Windows or root authority on UNIX or Linux to uninstall the Language Pack.

To uninstall the IBM Tivoli Storage Productivity Center components, follow these steps:

1. Log on to the system as a local administrator with the "Act as part of the operating system " user right on Windows. You must also have database administrative authority.

- 2. Exit the Tivoli Storage Productivity Center GUI.
- **3**. Go to the following installation directory:

<TPC\_install\_dir>/\_uninst\_langpack

For UNIX and Linux, run the following command: **./uninstall**. For Windows, run the following command: **uninstall.exe**.

- 4. The Select a language panel is displayed. Select a language and click OK.
- 5. The Welcome panel is displayed. Click Next.
- 6. The Select one or more Tivoli Storage Productivity Center products to uninstall panel is displayed. Select the components you want to uninstall. Click **Next**.

**Note:** Tivoli Storage Productivity Center will detect the language pack you installed and will preselect the language pack to uninstall. You do not have to select a language pack to uninstall.

- 7. The summary information panel is displayed. Review the information and click **Uninstall** to uninstall the components.
- 8. The successfully uninstalled panel is displayed. Click Finish.

#### Uninstalling the Agent Manager

Uninstalling the Agent Manager uninstalls the application from your operating system and removes the Agent Manager servlets from WebSphere Application Server. The uninstallation wizard does not drop the registry database or delete the Agent Manager objects from the database. That is an optional step you can perform before running the uninstallation program.

**Note:** To prevent the loss of important data:

- Do not uninstall the Agent Manager until all products that use it have been uninstalled.
- Do not clean the Agent Manager tables from the database or drop the registry database until all products that use the registry are uninstalled.

To uninstall the Agent Manager, follow these steps:

- 1. On AIX, Linux, and Solaris systems, be sure that the root user has logged off and logged on after installing the Agent Manager. If the user has not logged off, the component cannot be removed from the WebSphere configuration.
- 2. Drop the database or tables. This is an optional step. Make sure no other application is using this database or the tables before dropping the database or tables. Follow these steps:
  - a. Stop the Agent Manager server if it is running. Run the following command:
    - On Windows systems:
      - <Agent\_Manager\_install\_dir>\embedded\bin\stopServer.bat <app\_server\_name>
    - On AIX, Linux,, or Solaris systems:
       <Agent\_Manager\_install\_dir>/embedded/bin/stopServer.sh <app server name>

Replace <app\_server\_name> with the name of the application server where the Agent Manager is installed. By default, this is **AgentManager**. The server name is case-sensitive.

b. Remove the Agent Manager objects from the registry database.

- If the registry database is used only by the Agent Manager and is not shared with another program, drop the database using the database administration tools for your type of database.
- If the database is shared with other programs, remove the Agent Manager-specific tables from the database by following this procedure:
  - In a command line window, change to the <Agent\_Manager\_install\_dir>/db/db2 directory.
  - 2) Run the following command: db2cmd /c /i /w "RemoveCASTables.bat <database\_password>

Where <database\_password> is the DB2 database password.

- 3. Start the uninstallation program for your operating system:
  - On Windows systems, either use the Add/Remove Programs windows to uninstall the Agent Manager, or run the following command from a command prompt:

<Agent\_Manager\_install\_dir>\\_uninst\uninstall.exe

When you run the uninstall program, you need to pass the **javahome** parameter with the path to the JVM. For example:

uninstall.exe -is:javahome "C:\Program Files\IBM\AgentManager\ embedded\java"

 On AIX, Linux, and Solaris systems, run the following command from the <Agent\_Manager\_install\_dir>/\_uninst directory: uninstall.bin

The program does not delete the registry database or files created in the Agent Manager installation directory after installation.

The Agent Manager is now uninstalled.

### Uninstalling DB2

Uninstall DB2 after you have uninstalled IBM Tivoli Storage Productivity Center and Agent Manager. Use the DB2 uninstallation program to uninstall DB2.

For information about uninstalling DB2 V9.1 on Windows systems, go to http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=/ com.ibm.db2.udb.uprun.doc/doc/t0007436.htm.

For information about uninstalling DB2 V9.5 on Windows systems, go to http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp?topic=/ com.ibm.db2.luw.qb.server.doc/doc/t0007436.html.

## Uninstalling DB2 on UNIX or Linux

Use these steps to uninstall DB2 on UNIX or Linux systems.

To uninstall DB2 on UNIX and Linux, complete these steps:

- 1. Log in with a user ID or name that has DB2 admin authority and is in the db2iadm1 group.
- 2. Source your DB2 profile, as follows:
  - At a Bourne or Korn shell, type . HOME/sqllib/db2profile.
  - At a C shell, type source HOME/sqllib/db2cshrc.

where HOME is the home directory of the instance you want to use.

- **3**. Drop all databases from the DB2 instance db2inst1:
  - a. Run db2 drop db ibmcdb. The following message is displayed: DB20000I The DROP DATABASE command completed successfully.
  - b. Run **db2 drop db tpcdb**. The following message is displayed: DB200001 The DROP DATABASE command completed successfully.
- 4. Drop the DB2 instance db2inst1:
  - Run db2stop force. The following messages are displayed: SQL1064N DB2STOP processing was successful.
     SQL1064N DB2STOP processing was successful.
  - b. Run db2 terminate. The message is displayed: DB20000I The TERMINATE command completed successfully.
  - c. Run cd /opt/IBM/db2/V9.5/install.
  - d. Run ./db2idrop -f db2inst1. The following messages are displayed:

db2inst1, today is Thu Apr 17 13:53:54 PDT 2008. Your last login was 0 Apr 17 12

db2inst1, today is Thu Apr 17 13:53:55 PDT 2008. Your last login was 0 Apr 17 13

DBI1070I Program db2idrop completed successfully.

- 5. Stop and drop the DB2 administration server. You must stop the DB2(R) administration server (DAS) before you remove your DB2 product.
  - a. Switch to dasusr1 by typing the following command: su dasusr1
  - b. Type cd /home/dasusr/das/bin.
  - c. Run ./db2admin stop. The following message is displayed: SQL4407W The DB2 Administration Server was stopped successfully.
  - d. Type exit.
- 6. Remove the DB2 administration server. You must remove the DB2(R) administration server (DAS) before you remove your DB2 product.
  - a. Enter the following command: cd /opt/IBM/db2/V9.5/install
  - b. Run ./dasdrop. The following messages are displayed: SQL4410W The DB2 Administration Server is not active. DBI1070I Program dasdrop completed successfully.
- Uninstall DB2. Use the db2\_deinstall command to remove DB2 products or DB2 components. The db2\_deinstall command removes all DB2 products from your system.
  - **a**. Log in as a user with root authority.
  - b. Enter the following command:

cd /opt/IBM/db2/V9.5/install

- c. Run ./db2\_deinstall -a. The following message is displayed: DBI1016I Program db2\_deinstall is performing uninstallation. Please wait. The execution completed successfully.
- 8. Delete DB2 users and groups.
  - a. Log in as a user with root authority.
  - b. Run rmuser -p db2inst1.
  - c. Run rm -r /home/db2inst1.
  - d. Run rmuser -p dasusr1.
  - e. Run rm -r /home/dasusr1.

- f. Run rmuser -p db2fenc1.
- g. Run rm -r /home/db2fenc1.
- h. Run rmgroup dasadm1.
- i. Run rmgroup db2iadm1.
- j. Run rmgroup db2fadm1.
- 9. Remove the DB2 directory.
  - a. Log in as a user with root authority.
  - b. Run rm -r /opt/IBM/db2.
- 10. Remove any DB2 definitions from /etc/services.

## Chapter 6. Administering IBM Tivoli Storage Productivity Center

This topic provides information on how to administer IBM Tivoli Storage Productivity Center.

#### Administering DB2

Administer DB2 by backing up the IBM Tivoli Storage Productivity Center database, starting the control center, and starting and stopping DB2.

## Backing up the IBM Tivoli Storage Productivity Center database

IBM Tivoli Storage Productivity Center uses circular logs for the DB2 database. Therefore, only an offline database backup is supported. When an offline database backup is performed, the database connections are terminated. Therefore, the Tivoli Storage Productivity Center servers need to be stopped and then restarted.

- 1. Close the IBM Tivoli Storage Productivity Center GUI.
- 2. Stop the IBM Tivoli Storage Productivity Center servers.
- 3. Back up your database.
  - a. Open the DB2 Control Center.
  - b. The Control Center View panel is displayed. Select **Basic** and click **OK**.
  - c. In the Control Center navigation tree, click All Databases.
  - d. Under the **All Databases** node, you will see **TPCDB**. This is the IBM Tivoli Storage Productivity Center database. Highlight **TPCDB** and right-click on it. Click **Backup**.
  - e. The Confirm the details of your database panel is displayed. Click Next.
  - f. The Specify where to store your backup image panel is displayed. For Media Type, enter **File System**. If you want to add a new folder, click **Add**.
  - g. On the Path Browser LOCALHOST panel, click the **Create New Folder** icon. Enter the name of your new folder (for example, TPCbackup1). Click **OK**.
  - h. On the Specify where to store your backup image panel, you will see your new folder listed (TPCbackup1). Click **Finish**. The database backup will run.
  - i. When the database backup is completed, you will see a DB2 Message window indicating that the database backup completed successfully.
  - j. Close the DB2 Message window.
- 4. Restart the IBM Tivoli Storage Productivity Center servers.

If you want to do an online backup of the database, you will need to change the use of circular logs to linear logs. The use of linear logs can fill up the file system quickly if the database is not maintained properly. For information about how to change the use of circular logs to linear logs, see the DB2 Information Center. Click **Designing > Backups**.

## **Starting the Control Center**

This topic describes how to start the DB2 Control Center.

On Linux	From a console window, run the <b>db2cc</b> command.
On UNIX	Open the <b>IBM DB2</b> folder on the desktop and click <b>Control Center</b> .
On Windows	Click Start → Programs → IBM DB2 → General Administration Tools → Control Center

To start the Control Center, perform the following action:

## Using the command line on UNIX and Linux

This topic describes how to use a command line to perform actions against a DB2 instance under UNIX or Linux.

If the DB2 control center is unavailable or you do not have access to a graphical user interface, you can use a command line to execute DB2 commands such as starting and stopping an instance. To use a command line to perform actions against an instance of DB2, complete the following steps:

- 1. Log in with a user ID or name that has ROOT, SYSADM, SYSCTRL, or SYSMAINT authority on the instance; or log in as the instance owner.
- 2. Run the startup script as follows:
  - For Bourne or Korn shell, type: . HOME/sqllib/db2profile
  - For C shell, type: source HOME/sqllib/db2cshrc

where HOME is the home directory of the instance you want to use.

3. To start the instance using the command line, type db2start.

**Note:** When you run commands to start an instance's database manager, the DB2 database manager applies the command to the current instance.

4. To stop the instance using the command line, type db2stop.

**Note:** When you run commands to stop an instance's database manager, the DB2 database manager applies the command to the current instance.

## Manually starting DB2 running on Windows

This topic describes how to manually start DB2 running on Windows.

To start DB2 manually, complete the following steps:

- 1. Start the following Windows services:
  - DB2 DB2-0
  - DB2DAS DB2DAS00
  - DB2 JDBC Applet Server
  - DB2 License Server
  - DB2 Security Server
- 2. To open a DB2 command window, click Start → Programs → IBM DB2 → Command Line Tools → Command Window.
- 3. From the DB2 Command window, run the db2start command.

## Manually stopping DB2 running on Windows

This topic describes how to manually stop DB2 running on Windows.

To stop DB2 manually, complete the following steps:

- 1. Stop the following Windows services:
  - DB2 Security Server
  - DB2 License Server
  - DB2 JDBC Applet Server
  - DB2DAS DB2DAS00
  - DB2 DB2-0

**Note:** When you stop the **DB2 Security** Server service, you are prompted to stop the Warehouse logger and Warehouse Serve; click **Yes**.

- 2. To open a DB2 command window, click Start → Programs → IBM DB2 → Command Line Tools → Command Window.
- 3. From the DB2 Command window, run the db2stop command.

To restart DB2, enter the **db2start** command from the DB2 Command window. Before you can issue the command, you must first start these services from the Windows Services panel:

DB2 - DB2-0 DB2DAS - DB2DAS00 DB2 JDBC Applet Server DB2 License Server DB2 Security Server

#### Monitoring DB2

The minimum user authority level needed for monitoring DB2 instances is a user with DB2 system maintenance authority (SYSMAINT).

To check and set SYSMAINT authority, follow these steps:

 Run this command in the DB2 command prompt window to check to see if there is an operating system user group defined to have SYSMAINT authority: db2 get dbm cfg

In the output file, look for this information:

(SYSADM_GROUP) =
(SYSCTRL GROUP) =
(SYSMAINT_GROUP) =
(SYSMON_GROUP) =

If the setup for the operating system group has not been done, you will not see a value set.

If the setup has been done, this example shows what you can expect to see:

SYSADM group name	(SYSADM GROUP) =
SYSCTRL group name	(SYSCTRL GROUP) =
SYSMAINT group name	(SYSMAINT GROUP) = ADMINISTRATORS
SYSMON group name	(SYSMON_GROUP) =

In this example, the "ADMINISTRATORS" group has SYSMAINT\_GROUP authority.

2. If the setup has been done, add the user you want to use to the ADMINISTRATORS group using the operating system utilities or use a user that already belongs to the ADMINISTRATORS group.

If you want to give a user group "SYSMAINT\_GROUP" authority, follow these steps:

a. If a user (for example userA) belongs to an operating system group called "db2monitor", here is an example of setting the db2monitor group with SYSMAINT authority. From the DB2 command prompt window, run the following command:

db2 update dbm cfg using SYSMAINT\_GROUP db2monitor

b. After issuing the **db2 update** command, restart DB2 by running the following command from the DB2 command prompt window or restarting the system:

db2 force application all

This command might need to be issued a few times to stop all the database connections.

- Run the following commands from the DB2 command prompt window: db2stop db2start
- d. UserA will now be able to monitor the DB2 database.

#### Administering Tivoli Integrated Portal

This topic provides information on how to perform administrative tasks in IBM Tivoli Integrated Portal that are reflected in IBM Tivoli Storage Productivity Center.

#### Changing the user authentication method

The IBM Tivoli Storage Productivity Center installation program enables you to select a user authentication method that is used by Tivoli Storage Productivity Center, IBM Tivoli Storage Productivity Center for Replication, and IBM Tivoli Integrated Portal. You can choose to authenticate users against the users defined for the local operating system or to authenticate users against the users defined in a Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory repository. You can change the user authentication method after installation using Tivoli Integrated Portal.

You can select the following user authentication methods in Tivoli Integrated Portal:

- Federated repositories. This method authenticates the Tivoli Storage Productivity Center user against a Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory, directory service.
- Local operating system. This authentication method authenticates the Tivoli Storage Productivity Center user against the users defined for the local operating system. If you use operating system authentication, the use of the single sign-on feature is limited. OS authentication does not support single sign-on for element managers, even when the element manager is installed on the same computer as Tivoli Storage Productivity Center.

The following topics describe how to select and configure each user authentication method.

## Changing the authentication method from local operating system to LDAP federated repositories

You can configure IBM Tivoli Storage Productivity Center to communicate with an external Lightweight Directory Access Protocol (LDAP) repository such as IBM Tivoli Directory Server or Microsoft Active Directory. To change the authentication method from local operating system to LDAP, you must use IBM Tivoli Integrated Portal.

To change the user authentication method from local operating system to LDAP, complete the following steps. Contact your LDAP server administrator for assistance.

1. Start an Internet Explorer or Firefox Web browser, and type the following information in the address bar:

http://hostname:port

Where *hostname* defines the server that is running Tivoli Integrated Portal such as the server name or IP address and *port* defines the port number for Tivoli Integrated Portal. If the default port was accepted during the installation of Tivoli Integrated Portal, the port number is 16310. Contact your Tivoli Storage Productivity Center administrator if you need to verify the host name and port number.

- 2. On the Tivoli Integrated Portal logon page, log on using the appropriate user ID and password. Your user ID must have administrator permissions.
- 3. In the Tivoli Integrated Portal navigation tree, click Security → Secure administration, applications, and infrastructure.
- 4. On the Secure administration, applications, and infrastructure page, select **Federated Repositories** from the **Available Realm Definitions** list.
- 5. Click Configure. The Federated repositories page is displayed.
- 6. Under Related Items, click Manage repositories.
- 7. On the Manage repositories page, add the LDAP repository that you want to use for authentication as follows:
  - a. Click Add to add a new repository.
  - b. Enter the values for the following fields:
    - **Repository identifier**. A unique identifier for the LDAP repository. This identifier uniquely identifies the repository within the cell, for example: LDAP1.
    - Directory type. The type of LDAP server to which you want to connect.
    - **Primary host name**. The host name of the primary LDAP server. This host name is either an IP address or a domain name service (DNS) name.
    - **Port**. The LDAP server port. The default value is 389, which is not a Secure Sockets Layer (SSL) connection. You can use port 636 for a Secure Sockets Layer (SSL) connection. For some LDAP servers, you can specify a different port for a non-SSL or SSL connection. If you do not know the port to use, contact your LDAP server administrator.
    - **Bind distinguished name**. The distinguished name (DN) for the application server to use when binding to the LDAP repository. If no name is specified, the application server binds anonymously. In most cases, bind DN and bind password are needed. However, when anonymous bind can satisfy all of the required functions, bind DN and bind password are not needed.

- **Bind password**. The password for the application server to use when binding to the LDAP repository.
- c. Click OK.
- d. In the **Messages** box on the Manage repositories page, click the **Save** link in **Save to the master configuration**.
- 8. On the Manage repositories page, click the identifier for the repository that you want to use in the **Repository identifier** column.
- 9. On the configuration page for the repository, configure the following items:
  - a. Click **LDAP entity types** under **Additional Properties**. The LDAP entities page is displayed.
  - b. In the Entity type column, click the link for Group, OrgContainer, and PersonAccount and complete the Search bases field. This field specifies the search bases that are used to search this entity type. The search bases specified must be subtrees of the base entry in the repository. The following are example search bases, where o=ibm,c=us is the base entry in the repository:

o=ibm,c=us or cn=users,o=ibm,c=us or ou=austin,o=ibm,c=us

Delimit multiple search bases with a semicolon (;). For example: ou=austin,o=ibm,c=us;ou=raleigh,o=ibm,c=us

- c. Click **OK** and then click the **Save** link in **Save to the master configuration** each time that you update the **Search bases** field.
- **10.** Return to the Federated repositories page and click **Supported Entity Types** under **Additional Properties**.
- 11. On the Supported entity types page, configure the following items:
  - a. In the Entity type column, click the link for **Group**, **OrgContainer**, and **PersonAccount** and complete the **Base entry for the default parent** and **Relative Distinguished Name properties** fields.
    - In the **Base entry for the default parent** field, enter the same value that you entered in the **Search bases** field in step 9.
    - In the **Relative Distinguished Name properties** field, enter the appropriate LDAP attribute name. In most cases, the values for this field will be cn for **Group**, o;ou;dc;cn for **OrgContainer**, and uid for **PersonAccount**.
  - b. Click **OK** and then click the **Save** link in **Save to the master configuration** each time that you update the **Base entry for the default parent** field.
- 12. Return to the Federated repositories page and click **Apply** and then click the **Save** link in **Save to the master configuration**.
- 13. Under Repositories in the realm, click Add base entry to Realm.
- 14. On the Repository reference page, configure the following items:
  - a. In the **Repository** list, select the repository that you created in step 7.
  - b. In the **Distinguished name of a base entry that uniquely identifies this set of entries in the realm** field, enter the distinguished name of a base entry that uniquely identifies the repository in the realm. In most instances, this value will be the same value that you entered in the **Search bases** field in step 9.
  - c. In the **Distinguished name of a base entry in this repository** field, enter the distinguished name of the base entry within the repository. In most instances, this value will be the same value that you entered in the **Distinguished name of a base entry that uniquely identifies this set of entries in the realm** field.
- d. Click **OK** and then click the **Save** link in **Save to the master configuration** each time that you update the **Distinguished name of a base entry that uniquely identifies this set of entries in the realm** field.
- 15. On the Federated repositories page, there are now two repositories that are displayed under **Repositories in the realm**: the repository that you have added and a default repository that shows **File** in the Repository type column. Configure the following items:
  - **a**. Leave the value in the **Realm name** field as is or change the name of the realm name.
  - b. In the **Primary administrative user name** field, enter the name of a user in the repository that you added. This user will be granted administrative privileges in the Tivoli Integrated Portal server, the Tivoli Storage Productivity Center Device server, and the IBM Tivoli Storage Productivity Center for Replication server.
  - c. Click Server identity that is stored in the repository.
  - d. In the **Server user ID or administrative user on a Version 6.0.x node** field, enter the same ID that you entered in the **Primary administrative user name** field and enter the password for the user ID in the **Password** field.
  - e. Select the default file repository that shows **File** in the Repository type column and click **Remove**.
  - f. Click **OK** and then click the **Save** link in **Save to the master configuration**.
- **16**. Return to Secure administration, applications, and infrastructure page and configure the following items:
  - a. In the **Available realm definitions** list, select Federated repositories and then click **Set as current**.
  - b. Click **Apply** and then click the **Save** link in **Save to the master configuration**
- **17**. Stop and restart the Tivoli Integrated Portal, IBM Tivoli Storage Productivity Center for Replication servers and the IBM Tivoli Storage Productivity Center Data and Device servers. For information regarding stopping and starting a server, go to the Tivoli Storage Productivity Center Information Center and search for *starting and stopping services*.

To verify that the federated repository is configured correctly, complete the following steps:

- 1. Log on to Tivoli Integrated Portal as the new super user ID (the administrative account is no longer the OS credentials, but is now configured to use the LDAP server super user credentials).
- In the Tivoli Integrated Portal navigation tree, click Users and Groups → Manage Users .
- 3. In the Search by list, select User ID.
- 4. Click **Search** to search for users in the federated repository. The list of users includes users from both the LDAP and the local file registry.

## **Related tasks**

"Enabling secure communication between Tivoli Storage Productivity Center and the LDAP repository"

You can use the Secure Socket Layer (SSL) protocol to secure the communication between IBM Tivoli Storage Productivity Center and the LDAP repository that you are using for user authentication. The SSL protocol provides security and data integrity for communications over Transmission Control Protocol/Internet Protocol (TCP/IP) networks.

"Disabling secure communication between Tivoli Storage Productivity Center and the LDAP repository" on page 408

You can disable the Secure Socket Layer (SSL) protocol between the LDAP repository and the IBM Tivoli Storage Productivity Center system at any time.

# Enabling secure communication between Tivoli Storage Productivity Center and the LDAP repository:

You can use the Secure Socket Layer (SSL) protocol to secure the communication between IBM Tivoli Storage Productivity Center and the LDAP repository that you are using for user authentication. The SSL protocol provides security and data integrity for communications over Transmission Control Protocol/Internet Protocol (TCP/IP) networks.

To configure for SSL, you must complete the following steps in IBM Tivoli Integrated Portal:

1. Start an Internet Explorer or Firefox Web browser, and type the following information in the address bar:

http://hostname:port

Where *hostname* defines the server that is running Tivoli Integrated Portal such as the server name or IP address and *port* defines the port number for Tivoli Integrated Portal. If the default port was accepted during the installation of Tivoli Integrated Portal, the port number is 16310. Contact your Tivoli Storage Productivity Center administrator if you need to verify the host name and port number.

- 2. On the Tivoli Integrated Portal logon page, log on using the appropriate user ID and password. Your user ID must have administrator permissions.
- 3. In the Tivoli Integrated Portal navigation tree, click Security → SSL certificate and key management → Key stores and certificates → NodeDefaultTrustStore → Signer certificates.
- 4. On Signer certificates page, click Retrieve from port.
- 5. On the Retrieve from port page, enter values for the following fields:
  - **Host**. The fully qualified host and domain name of your LDAP-compliant repository.
  - **Port**. The port where your LDAP repository is listening for secure communications; this is usually port 636.
  - SSL configuration for outbound connection. Accept the default value.
  - Alias. An alias name for the retrieved certificate.
- 6. Click Retrieve signer information.
- 7. When the signer information is displayed, click **OK**.
- 8. In the **Messages** box on the Signer certificates page, click the **Save** link in **Save to the master configuration**.

- **9**. On the Signer certificates page, select the LDAP repository certificate that you just retrieved and click **Extract**.
- 10. On the Extract signer certificate page, enter values for the following fields:
  - File name. The file name for this certificate. For example, LDAPSSLCert. This file is saved in the C:\*Tivoli Integrated Portal install directory*\profiles\TIPProfile\etc\ directory on the Windows platform. In the AIX, Linux, and UNIX platforms, this file is saved in the /*Tivoli Integrated Portal install directory*/profiles/TIPProfile/etc/ directory. *Tivoli Integrated Portal install directory* is the directory where Tivoli Integrated Portal is installed.
  - Data type. Accept the default value.
- 11. Click **OK**. A message is displayed on the Signer certificates page stating that the file was successfully extracted.
- 12. In the Tivoli Integrated Portal navigation tree, click Security → Secure administration, applications, and infrastructure.
- **13**. On the Secure administration, applications, and infrastructure page, make sure that **Federated Repositories** is selected in the **Available Realm Definitions** list.
- 14. Click Configure. The Federated repositories page is displayed.
- 15. Under Related Items, click Manage repositories.
- **16.** On the Manage repositories page, click the identifier for the repository for which you want to enable the SSL protocol.
- 17. On the configuration page for the repository, configure the following items:
  - a. In the Port field, enter 636
  - b. Select the Require SSL communications check box.
- 18. Click OK.
- In the Messages box on the Manage repositories page, click the Save link in Save to the master configuration.
- 20. Log off of Tivoli Integrated Portal.
- 21. From the command line, stop the Tivoli Integrated Portal server, the Tivoli Storage Productivity Center for Replication, and the Tivoli Storage Productivity Center Device and Data servers. For information regarding starting and stopping a server, go to the Tivoli Storage Productivity Center Information Center and search for *starting and stopping services*.
- **22**. Use the following commands to import the LDAP repository certificate into the Tivoli Storage Productivity Center Device server keystore:

## Windows

cd C:\Tivoli Storage Productivity Center install directory\jre\bin\

keytool -import -keystore C:\Tivoli Storage Productivity Center install directory \device\apps\was\profiles\deviceServer\config\cells\DefaultNode\nodes\DefaultNode\ trust.pl2 -storetype pkcs12 -storepass WebAS -file C:\Tivoli Integrated Portal install directory\profiles\TIPProfile\etc\ LDAP repository certificate file name

where *Tivoli Storage Productivity Center install directory* is the is the directory where Tivoli Storage Productivity Center is installed, *Tivoli Integrated Portal install directory* is the directory where Tivoli Integrated Portal is installed, and *LDAP repository certificate file name* is the file name that you assigned to the LDAP repository certificate in Step 11.

Type yes when you are asked if you want to trust this certificate.

## AIX, Linux, and UNIX

cd Tivoli Storage Productivity Center install directory/jre/bin/

./keytool -import -keystore /Tivoli Storage Productivity Center install directory/device/apps/was/profiles/deviceServer/config/ cells/DefaultNode/nodes/DefaultNode/trust.pl2 -storetype pkcsl2 -storepass WebAS -file /Tivoli Storage Productivity Center install directory/profiles/TIPProfile/etc/ LDAP repository certificate file name

where *Tivoli Storage Productivity Center install directory* is the is the directory where Tivoli Storage Productivity Center is installed, *Tivoli Integrated Portal install directory* is the directory where Tivoli Integrated Portal is installed, and *LDAP repository certificate file name* is the file name that you assigned to the LDAP repository certificate in Step 11.

Type yes when you are asked if you want to trust this certificate.

**23.** Use the following commands to import the LDAP repository certificate into the Tivoli Storage Productivity Center for Replication server keystore:

#### Windows

keytool -import -keystore C:\Tivoli Storage Productivity Center install directory\eWAS\profiles\CSM\config\cells\DefaultNode\nodes\DefaultNode \trust.pl2 -storetype pkcs12 -storepass WebAS -file <C:\Tivoli Storage Productivity Center install directory\profiles\TIPProfile\ etc\LDAP repository certificate file name

where *Tivoli Storage Productivity Center for Replication* install directory is the directory where Tivoli Storage Productivity Center for Replication is installed.

Type yes when you are asked if you want to trust this certificate.

#### AIX, Linux, and UNIX

./keytool -import -keystore /Tivoli Storage Productivity Center install directory/eWAS/profiles/CSM/config/cells/DefaultNode/nodes/DefaultNode /trust.pl2 -storetype pkcs12 -storepass WebAS -file /Tivoli Storage Productivity Center install directory/profiles/TIPProfile/etc/ LDAP repository certificate file name

where *Tivoli Storage Productivity Center for Replication* install directory is the directory where Tivoli Storage Productivity Center for Replication is installed.

Type yes when you are asked if you want to trust this certificate.

24. From the command line, start the Tivoli Integrated Portal server, the Tivoli Storage Productivity Center for Replication, and the Tivoli Storage Productivity Center Device and Data servers.

**Important:** All of the group-to-role mappings in Tivoli Storage Productivity Center for Replication are deleted as a result of securing communications between LDAP and the Tivoli Storage Productivity Center system. You must manually re-create the Tivoli Storage Productivity Center for Replication group-to-role mappings following this procedure. The Tivoli Storage Productivity Center and Tivoli Integrated Portal group-to-role mappings are preserved during this procedure and require no adjustment.

# Disabling secure communication between Tivoli Storage Productivity Center and the LDAP repository:

You can disable the Secure Socket Layer (SSL) protocol between the LDAP repository and the IBM Tivoli Storage Productivity Center system at any time.

To disable the use of SSL, you must complete the following steps in IBM Tivoli Integrated Portal:

 Start an Internet Explorer or Firefox Web browser, and type the following information in the address bar: http://hostname:port Where *hostname* defines the server that is running Tivoli Integrated Portal such as the server name or IP address and *port* defines the port number for Tivoli Integrated Portal. If the default port was accepted during the installation of Tivoli Integrated Portal, the port number is 16310. Contact your Tivoli Storage Productivity Center administrator if you need to verify the host name and port number.

- 2. On the Tivoli Integrated Portal logon page, log on using the appropriate user ID and password. Your user ID must have administrator permissions.
- 3. In the Tivoli Integrated Portal navigation tree, click Security → Secure administration, applications, and infrastructure.
- 4. On the Secure administration, applications, and infrastructure page, make sure that **Federated Repositories** is selected in the **Available Realm Definitions** list.
- 5. Click **Configure**. The Federated repositories page is displayed.
- 6. Under Related Items, click Manage repositories.
- 7. On the Manage repositories page, click the identifier for the repository for which you want to disable the SSL protocol.
- On the configuration page for the repository, configure the following items:
   a. In the Port field, enter 389.
  - b. Clear the Require SSL communications check box.
- 9. Click OK.
- 10. In the **Messages** box on the Manage repositories page, click the **Save** link in **Save to the master configuration**.
- 11. Log off of Tivoli Integrated Portal.
- **12.** From the command line, stop and then start the Tivoli Integrated Portal server, the Tivoli Storage Productivity Center for Replication, and the Tivoli Storage Productivity Center Device and Data servers. For information regarding starting and stopping a server, go to the Tivoli Storage Productivity Center Information Center and search for *starting and stopping services*.

**Important:** All of the group-to-role mappings in Tivoli Storage Productivity Center for Replication are deleted as a result of disabling the secure communications between LDAP and the Tivoli Storage Productivity Center system. You must manually re-create the Tivoli Storage Productivity Center for Replication group-to-role mappings following this procedure. The Tivoli Storage Productivity Center and Tivoli Integrated Portal group-to-role mappings are preserved during this procedure and require no adjustment.

# Changing the authentication method from LDAP to local operating system

You can configure IBM Tivoli Storage Productivity Center to authenticate against the local operating system. To change the authentication method from LDAP to local operating system, you must use Tivoli Integrated Portal.

If you use operating system authentication, the use of the single sign-on feature is limited. Operating system authentication does not support single sign-on if Tivoli Storage Productivity Center and Tivoli Integrated Portal are on separate computers. Operating system authentication also does not support single sign-on for element managers regardless of the location of the element manager application.

To change the user authentication method from LDAP to local operating system, complete the following steps:

1. Start an Internet Explorer or Firefox Web browser, and type the following information in the address bar:

http://hostname:port

Where *hostname* defines the server that is running Tivoli Integrated Portal such as the server name or IP address and *port* defines the port number for Tivoli Integrated Portal. If the default port was accepted during the installation of Tivoli Integrated Portal, the port number is 16310. Contact your Tivoli Storage Productivity Center administrator if you need to verify the host name and port number.

- 2. On the Tivoli Integrated Portal logon page, log on using the appropriate user ID and password. Your user ID must have administrator permissions.
- 3. In the Tivoli Integrated Portal navigation tree, click Security → Secure administration, applications, and infrastructure.
- 4. On the Secure administration, applications, and infrastructure page, select **Local operating system** from the **Available Realm Definitions** list.
- 5. On the Local operating system page, configure the following items:
  - a. In the **Primary administrative user name** field, enter the name of a user that is defined in your local operating system. This user will be granted administrative privileges in the Tivoli Integrated Portal server, the Tivoli Storage Productivity Center Device server, and the IBM Tivoli Storage Productivity Center for Replication server.
  - b. Click Server identity that is stored in the repository.
  - c. In the **Server user ID or administrative user on a Version 6.0.x node** field, enter the same ID that you entered in the **Primary administrative user name** field and enter the password for the user ID in the **Password** field.
  - d. Click OK.
  - e. In the **Messages** box on the Secure administration, applications, and infrastructure page, click the **Save** link in **Save to the master configuration**.
- **6**. Configure the following items on the Secure administration, applications, and infrastructure page:
  - a. In the **Available realm definitions** list, select **Local operating system** and then click **Set as current**.
  - b. Click **Apply** and then click the **Save** link in **Save to the master configuration**
- 7. Stop and restart the Tivoli Integrated Portal, IBM Tivoli Storage Productivity Center for Replication servers and the IBM Tivoli Storage Productivity Center Data and Device servers. For information regarding stopping and starting a server, go to the Tivoli Storage Productivity Center Information Center and search for *starting and stopping services*.

# Changing the LTPA token expiration for single-sign on

A single sign-on environment requires a centralized authentication repository that is accessed by all applications within the environment. The user's authentication information is passed between applications using Lightweight Third-Party Authentication (LTPA) tokens. You can change the expiration time for the LTPA tokens using IBM Tivoli Integrated Portal.

To change the expiration time for the LTPA tokens, complete the following steps.

1. Start an Internet Explorer or Firefox Web browser, and type the following information in the address bar:

http://hostname:port

Where *hostname* defines the server that is running Tivoli Integrated Portal such as server name or IP address and *port* defines the port number for Tivoli Integrated Portal. If the default port was accepted during the installation of Tivoli Integrated Portal, the port number is 16310. Contact your Tivoli Storage Productivity Center administrator if you need to verify the host name and port number.

- 2. On the Tivoli Integrated Portal logon page, log on using the appropriate user ID and password. Your user ID must have administrator permissions.
  - If you are using Tivoli Integrated Portal that was installed with Tivoli Storage Productivity Center, type your Tivoli Storage Productivity Center ID and password in the **User ID** and **Password** fields and click **Log in**. Your Tivoli Storage Productivity Center user ID must be a member of the Tivoli Storage Productivity Center Superuser role.
  - If you are using a stand-alone Tivoli Integrated Portal system, type your Tivoli Integrated Portal user ID and password. Your Tivoli Integrated Portal user ID must be a member of the Administrator role.
- 3. In the Tivoli Integrated Portal navigation tree, click Security → Secure administration, applications, and infrastructure.
- 4. Under Authentication, click Authentication mechanisms and expiration.
- 5. On the Configuration tab under Authentication expiration, type the expiration time in minutes in the Timeout value for forwarded credentials between servers field. The expiration time must be greater than the authentication cache timeout value that is shown above the Timeout value for forwarded credentials between servers field. The default expiration time is 1440 minutes (24 hours).
- 6. Click Apply.
- 7. In the Messages box, click **Save directly to the master configuration**.

# Managing Agent Manager

This topic provides information about working with Agent Manager. After you make changes to the Agent Manager, you must stop and then restart the Agent Manager server before it can use the new settings.

# **Getting started**

This section contains information on how to get started using Agent Manager.

# **Tivoli Common Agent Services**

IBM Tivoli Storage Productivity Center uses Tivoli Common Agent Services for software distribution and desired state management. An *agent* is a program that automatically performs some service, such as data collection. To take advantage of some Tivoli Storage Productivity Center software management features, the Common agent must be installed on all managed endpoints.

The Common agent environment consists of the following:

## Common agent

The Common agent is a common container for all the subagents to run within. It enables multiple management applications to share resources when managing a system. The Common agent is installed on each endpoint.

## Agent Manager

The Agent Manager is the server component of the Common agent that

provides functions that allow clients to get information about agents and resource managers. It enables secure connections between managed endpoints, maintains the database information about the endpoints and the software running on those endpoints, and processes queries against that database from resource managers. It also includes a registry and an agent recovery service.

## **Resource manager**

A resource manager is the server component of a management application product that manages the agents. Examples of resource managers are Tivoli Storage Productivity Center (server component) and IBM Tivoli Storage Productivity Center for Data for Data (server component).

## The Agent Manager:

The Agent Manager is a network service that serves as a certificate and registration authority to provide authentication and authorization using X.509 certificates and the Secure Sockets Layer (SSL) protocol. It also processes queries against its registry of configuration information about the agents and resource managers. The Agent Manager service is a WebSphere servlet.

*The registry:* The registry is a database that contains the current configurations of all known agents and resource managers. Resource managers and agents must register with the Agent Manager before they can use its services to communicate with each other. Registration is password protected, with separate passwords for the registration of agents and resource managers.

The registry contains the identity, certificates, and communication information for each resource manager, and the following information about agents:

- The identity of every known agent and its computer system
- The certificate issued to each agent
- Basic configuration information about each agent, including information about the type and version of the hardware and operating system
- The configuration of each agent (updated by the agent at a configurable interval)
- The errors reported by each agent (updated by the agent at a configurable interval)
- Current communication parameters for the agent, including the IP address, the port or ports for which the agent is configured, and the supported protocol
- The agents on which each bundle is installed

The information in the registry is updated by asynchronous events, such as the registration of agents and resource managers, and by updates from the agent. The agent provides a configuration update when it starts, when a bundle is installed or uninstalled, and at a configurable interval (by default, daily). By default, the registry contains only the most recent configuration update and error information about each agent. However, the retention period for these records is configurable. For all other information, the registry contains the complete history of your agents and resource managers.

The registry can be placed in the DB2 database or Oracle9i Database.

*The agent recovery service:* The Agent Manager also provides an agent recovery service that is a network service for error logging for agents that cannot communicate with other Agent Manager services. Agents use an unsecured HTTP connection to communicate with the agent recovery service. Because the connection

is unsecured, an agent can always communicate with the agent recovery service, even if the agent is incorrectly configured or has expired or revoked certificates. The agent recovery service is a WebSphere servlet container that runs on the Agent Manager server.

Agents locate the agent recovery service using the unqualified host name TivoliAgentRecovery. Your Domain Name System (DNS) server must map the host name TivoliAgentRecovery to the computer system where you installed the Agent Manager. The normal DNS lookup mechanism iterates through the domain search list for the agent, appends each domain in the list to the unqualified host name, and then performs a DNS lookup to attempt to resolve the name. The agent recovery service listens for recovery requests on two ports: port 80 and a configurable port (by default, 9513).

## The Common agent:

The Common agent is a common infrastructure in which product-specific agent code can be deployed and run. Examples of product-specific agents are Fabric Manager agent and Data Manager agent. A product-specific subagent consists of one or more *OSGi bundles*. A bundle is an application that is packaged in a format defined by the Open Services Gateway Initiative (OSGi) Service Platform specification, which is implemented in a lightweight infrastructure based on WebSphere Everywhere Deployment technology. The Common agent code will only be installed once on a managed host. For example, if you have two management applications on the same managed host (application A and application B), the Common agent code will only be installed once. However, there will be two product-specific agents: one for application A and one for application B. The term *agent* or *Common agent* is used to refer to both the Common agent and product-specific agent unless specifically stated otherwise.

The Common agent provides these services:

- · Deployment and life cycle management of product agent bundles
- · Agent registration and security certificate management
- Agent Manager queries
- Common agent health monitoring and configuration monitoring services

The Common agent provides configuration information to the Agent Manager. Updates are initiated by the Common agent or product agent bundle events. There are times when management applications might require periodic updates of the configuration of product agents. The Common agent allows any product agent to participate and provide application specific status. The Common agent provides a registration interface that allows resource managers to receive agent configuration updates. The Agent Manager distributes the configuration monitoring reports to all interested parties.

The monitoring service has a "heartbeat" function that allows for periodic updates of status reports. This function will force the monitoring service to send a status report after a period of time since the last status report delivery was attempted. The frequency of this update can be configured or completely disabled (the default frequency is 24 hours). You can change this frequency by editing the **status.heartbeat.frequency** property in the **endpoint.properties** file. To disable this function, set the status.heartbeat.frequency property to zero. The **endpoint.properties** file is located in the config directory where you installed the agent.

The Common agent contacts the registration server and reports its status and any configuration changes at these times:

- After initial registration
- When a Common agent starts or stops
- After a configurable period of time
- Any time a bundle is installed, upgraded, or removed

# Starting the Agent Manager

This topic describes how to start the Agent Manager.

1. Determine the name of the server on which Agent Manager is installed. From a command prompt, type the following text and press **Enter**.

Table 32. Getting the Agent Manager server name for Version 1.2

On Linux or UNIX	<agent_manager_install_directory>/embedded/bin/ serverStatus.sh -all</agent_manager_install_directory>
On Windows	<agent_manager_install_directory>\embedded\bin\ serverStatus.bat</agent_manager_install_directory>

Table 33. Getting the Agent Manager server name for Version 1.3

On Linux or UNIX	<agent_manager_install_directory>/AppServer/ agentmanager/bin/serverStatus.sh -all</agent_manager_install_directory>
On Windows	<agent_manager_install_directory>\AppServer\ agentmanager\bin\serverStatus.bat</agent_manager_install_directory>

where <Agent\_Manager\_install\_directory> is the directory where Agent Manager is installed. The default directory for Windows is C:\Program Files\IBM\AgentManager. The default directory for UNIX or Linux is /<usr or opt>/IBM/AgentManager.

2. To start the Agent Manager server, type the following command and press **Enter**.

Table 34. Starting the Agent Manager server for Version 1.2

On Linux or	<agent_manager_install_directory>/embedded/bin/</agent_manager_install_directory>	
UNIX	startServer.sh <app_server_name></app_server_name>	
On Windows (as	Open the Windows service window and start the Agent Manager server:	
a service)	IBM WebSphere Application Server V6 - Tivoli Agent Manager	
On Windows (not as a service)	<agent_manager_install_directory>\embedded\bin\ startServer.bat <app_server_name></app_server_name></agent_manager_install_directory>	

Table 35. Starting the Agent Manager server for Version 1.3

On Linux or UNIX	<pre><agent_manager_install_directory>/AppServer/ agentmanager/bin/startServer.sh <app_server_name></app_server_name></agent_manager_install_directory></pre>	
On Windows (as	Open the Windows service window and start the Agent Manager server:	
a service)	IBM WebSphere Application Server V6 - Tivoli Agent Manager	
On Windows (not	<agent_manager_install_directory>\AppServer\</agent_manager_install_directory>	
as a service)	agentmanager\bin\startServer.bat <app_server_name></app_server_name>	

where <app\_server\_name> is the case-sensitive name of the server where Agent Manager is installed. By default, this is **AgentManager**.

When the Agent Manager starts, the following message is displayed:

ADMU3000I: Server <server> open for e-business; process id is 3600

# **Stopping the Agent Manager**

This topic describes how to stop the Agent Manager.

1. Determine the name of the server on which Agent Manager is installed. From a command prompt, type the following text and press **Enter**:

Table 36. Getting the Agent Manager server name for Version 1.2

On Linux or UNIX	<agent_manager_install_directory>/embedded/bin/ serverStatus.sh -all</agent_manager_install_directory>
On Windows	<agent_manager_install_directory>\embedded\bin\ serverStatus.bat</agent_manager_install_directory>

Table 37. Getting the Agent Manager server name for Version 1.3

On Linux or UNIX	<agent_manager_install_directory>/AppServer/ agentmanager/bin/serverStatus.sh -all</agent_manager_install_directory>
On Windows	<agent_manager_install_directory>\AppServer\ agentmanager\bin\serverStatus.bat</agent_manager_install_directory>

where <Agent\_Manager\_install\_directory> is the directory where Agent Manager is installed.

2. To stop the Agent Manager server, type the following command and press **Enter**.

Table 38. Stopping the Agent Manager server for Version 1.2

On Linux or	<agent_manager_install_directory>/embedded/bin/</agent_manager_install_directory>
UNIX	stopServer.sh <app_server_name></app_server_name>
On Windows (as	Open the Windows service window and stop the Agent Manager server:
a service)	IBM WebSphere Application Server V6 - Tivoli Agent Manager
On Windows (not	<agent_manager_install_directory>\embedded\bin\</agent_manager_install_directory>
as a service)	stopServer.bat <app_server_name></app_server_name>

Table 39. Stopping the Agent Manager server for Version 1.3

On Linux or UNIX	<pre><agent_manager_install_directory>/AppServer/ agentmanager/bin/stopServer.sh <app_server_name></app_server_name></agent_manager_install_directory></pre>	
On Windows (as a service)	Open the Windows service window and stop the Agent Manager server: IBM WebSphere Application Server V6 - Tivoli Agent Manager	
On Windows (not as a service)	<pre><agent_manager_install_directory>\AppServer\ agentmanager\bin\stopServer.bat <app_server_name></app_server_name></agent_manager_install_directory></pre>	

where <app\_server\_name> is the case-sensitive name of the server where Agent Manager is installed. By default, this is **AgentManager**.

When the Agent Manager server is stopped, the following message is displayed:

ADMU4000I: Server <app\_server\_name> stop completed.

# Configuring Agent Manager to use different ports

This topic describes how to change the ports that IBM Tivoli Storage Productivity Center uses to communicate with Agent Manager. By default, these are ports 9511, 9512, and 9513.

To change the ports used by Tivoli Storage Productivity Center to communicate with Agent Manager, complete the following steps:

1. Determine which ports are currently in use. You can use the **netstat -an** command to list the active ports on a system, or you can examine one of the following files to review the port definitions:

On Windows	<pre>%SYSTEMROOT%\System32\drivers\etc\services</pre>
------------	-------------------------------------------------------

The list includes ports that can be used by services on the system, even if the port is not currently in use. The file does not include ports that are opened dynamically by applications.

- 2. Using a text editor, modify the virtualhosts.xml file. This file is at <directory>\config\cells\<cell\_name>, where <directory> is the directory where Agent Manager is installed, and <cell\_name> is the cell name for the Agent Manager.
- Modify the server.xml file. This file is at <directory>\embedded\config\cells\ DefaultNode\nodes\DefaultNode\servers\<AgentManager>, where <directory> is the directory where Agent Manager is installed, and <Agent Manager> is the application server name.
- 4. Modify the **AgentManager.properties** file. This file is located at <directory>\embedded\installedApps\DefaultNode\AgentManager.ear\ AgentManager.war\WEB-INF\classes\resources
- To stop Agent Manager, run the following command: stopServer AgentManager
- 6. To start Agent Manager, run the following command: startServer AgentManager

# How to change port 80

Using port 80 for the Agent Manager recovery service makes the request more likely to pass through a firewall between the agent and the agent recovery service. However, if the Agent Manager is on the same system as the HTTP server, port 80 is not available. The configurable second port provides an alternate communication port, in case you need to disable the use of port 80 by the agent recovery service.

If you need to change port 80, you must change the following jacl scripts:

# EPMHostAliasAdmin.jacl

This script file changes the WebSphere host alias port configuration.

# EPMTransportAdmin.jacl

This script file changes the WebSphere HTTP transport port.

These files are found in the following directories:

C:\Program Files\IBM\AgentManager\install\jacl (for Windows) /opt/IBM/AgentManager/install/jacl (for UNIX or Linux)

To change the port number, follow these steps:

- 1. Change the EPMHostAliasAdmin.jacl script. This file changes the WebSphere host alias port configuration. Use this file when you run the WebSphere **wsadmin** command.
  - The following parameters are **required** by the **wsadmin** command. For information about the **wsadmin** command, see the WebSphere documentation.

-f Full path of the EPMSSLAdmin.jacl script.

## -conntype

Choices are NONE, RMI, or SOAP. Select SOAP.

### -wsadmin\_classpath

List of fully-qualified jar files needed to run this script (**JLog.jar** and **install.jar**).

The following parameters are required by the EPMHostAliasAdmin.jacl script:

### -action

Create or remove.

## -propfile

Fully-qualified Java Properties file (AMInstall.properties).

## -logDir

Directory to store log files.

• The following keys **must** be set in the Java properties file:

Cell WebSphere cell name.

## VirtualHostName

Name of the virtual host.

## PortCount

Number of ports that are to be configured (1 through n) which is appended to the following keys. For example, if **PortCount** is set to

- 2, then the following keys are also checked: - SSLEnabled1, HostName1, PortNumber1
- SSLEnabled2, HostName2, PortNumber2

## SSLEnabled(n)

Indicates if SSL is enabled for this port. The setting is either true or false.

## HostName(n)

Host name.

## PortNumber(n)

Port number.

The **AMInstall.properties** file has the necessary keys and values. It is recommended that you copy the **AMInstall.properties** file and make changes to that file.

- 2. Change the EPMTransportAdmin.jacl script. This file is provided to change the WebSphere HTTP Transport port configuration. This file can be used when you run the WebSphere **wsadmin** command.
  - The following parameters are **required** by the **wsadmin** command. For information about the **wsadmin** command, see the WebSphere documentation.
    - -f Full path of the EPMSSLAdmin.jacl script.

## -conntype

Choices are NONE, RMI, or SOAP. Select SOAP.

## -wsadmin\_classpath

List of fully-qualified jar files needed to run this script (**JLog.jar** and **install.jar**).

• The following parameters are required by the EPMTransportAdmin.jacl script:

-action

Create or remove.

-propfile

Fully-qualified Java properties file (AMInstall.properties).

## -logDir

Directory to store log files.

• The following keys **must** be set in the Java properties file:

Cell WebSphere cell name.

## VirtualHostName

Name of the virtual host.

## PortCount

Number of ports that are to be configured (1 through n) which is appended to the following keys. For example, if **PortCount** is set to 2, then the following keys are also checked:

- SSLEnabled1, HostName1, PortNumber1(,SSLProfileName1)
- SSLEnabled2, HostName2, PortNumber2(,SSLProfileName2)

## SSLEnabled(n)

Indicates if SSL is enabled for this port. The setting is either true or false.

## SSLProfileName(n)

Name of the SSL profile (required only when SSLEnabled(n) is true).

## HostName(n)

Host name.

# PortNumber(n)

Port number.

The **AMInstall.properties** file in the Agent Manager directory has all the keys and values except for **KeyFilePassword** and **TrustFilePassword**. It is recommended that you use the copy of the **AMInstall.properties** file for your changes.

- **3**. Change the virtual host aliases.
  - Remove the host alias with port 80 using AMHostAliasAdmin.jacl with the **action=remove** parameter. This is a properties file example:

```
Cell=namtp4
Node=namtp4
VirtualHostName=AgentManagerHost
ApplicationServerName=AgentManager
##
PortCount=1
##
HostName1=*
PortNumber1=80
SSLEnabled1=false
##
```

• Create the host alias with the desired port number using the AMHostAliasAdmin.jacl with the action=create parameter. This is a properties file example:

```
Cell=namtp4
Node=namtp4
VirtualHostName=AgentManagerHost
ApplicationServerName=AgentManager
##
PortCount=1
##
HostName1=*
PortNumber1=1080
SSLEnabled1=false
##
```

4. Change the HTTP Transport:

• Remove the http transport with port 80 using the AMTransportAdmin.jacl with the **action=remove** parameter. This is a properties file example:

```
Cell=namtp4
Node=namtp4
VirtualHostName=AgentManagerHost
ApplicationServerName=AgentManager
##
PortCount=1
##
HostName1=*
PortNumber1=80
SSLEnabled1=false
##
```

• Create the http transport with the desired port number using the AMTransportAdmin.jacl script with the **action=create** parameter. This is a properties file example:

```
Cell=namtp4
Node=namtp4
VirtualHostName=AgentManagerHost
ApplicationServerName=AgentManager
##
PortCount=1
##
HostName1=*
PortNumber1=1080
SSLEnabled1=false
##
```

Here is a batch example for removal:

```
set am path=C:/MyPrograms/IBMAgentManager
set am_install_path=%am_path%/install
set wsadmin classpath=
 %am_install_path%/lib/install.jar
set prop path=%am install path%/AMInstallTest.properties
set action=remove
set jacl_path=%am_install_path%/jacl/EPMHostAliasAdmin.jacl
set log_path=%am_path%/logs/jacl/hostAliasAdmin
wsadmin -f %jacl path% -conntype SOAP -wsadmin classpath
 %wsadmin classpath% -action %action% -propfile %prop path%
  -logDir %log_path%
set jacl path=%am install path%/jacl/EPMTransportAdmin.jacl
set log path=%am path%/logs/jacl/transportAdmin
wsadmin -f %jacl path% -conntype SOAP -wsadmin classpath
  %wsadmin classpath% -action %action% -propfile %prop path%
  -logDir %log_path%
```

To use the same example for creation, set the following action variable: set action=create

# Packaging the Agent Manager log files

You can use the **LogCollector** tool to collect logs and other information needed to debug problems with the Agent Manager. If you contact IBM Customer Support, you will need to provide this package.

If you encounter a problem that you cannot resolve immediately, you can use the **LogCollector** tool to package the Agent Manager log files. This preserves the information that you need to perform detailed problem determination and prevents you from having to scan back through messages and trace events that

were recorded after the problem occurred. For more information about the **LogCollector** tool, see the readme file in the <Agent\_Manager\_install\_directory>/ toolkit directory, where <Agent\_Manager\_install\_directory> is the directory where Agent Manager is installed. The readme file provides information on how to run this tool and what parameters you can specify.

1. Change to the following directory:

<Agent\_Manager\_install\_directory>/toolkit/bin

where <Agent\_Manager\_install\_directory> is the directory where Agent Manager is installed.

2. Run one of the following commands:

On Linux or UNIX	LogCollector.sh	
On Windows	LogCollector.bat	

The LogCollector.zip file is created.

# Determining the version of Agent Manager

You can run the **GetAMInfo** command to determine which version of Agent Manager is installed.

To display the version of the Agent Manager, complete the following steps:

1. Change to one of the following directories:

For AIX, Linux, and UNIX	<agent_manager_install_directory>/bin</agent_manager_install_directory>
For Windows	<agent_manager_install_directory>\bin</agent_manager_install_directory>

where <Agent\_Manager\_install\_directory> is the directory where Agent Manager is installed.

2. To display the version for the Agent Manager, run the following command:

For AIX, Linux, and UNIX	GetAMInfo.sh AgentManager
For Windows	GetAMInfo.bat AgentManager

3. To get the version for the Agent Recovery Service, run the following command:

For AIX, Linux, and UNIX	GetAMInfo.sh AgentRecoveryService
For Windows	GetAMInfo.bat AgentRecoveryService

# **Backup and recovery**

This section provides procedures for backup and recovery tasks.

**Backing up the original certificates on the Agent Manager server** Optionally, you can back up the original certificates before you change them. This allows you to restore the original environment if you have trouble generating new certificates.

To back up the original certificates, make a copy of the <Agent\_Manager\_install\_dir>/certs directory on the Agent Manager server. Set the file and directory permissions so that unauthorized users cannot access the copy.

It is not necessary to back up the certificates on each resource manager or agent. If you need to restore the original certificates, restore the directory on the Agent Manager server, and then redistribute the Agent Manager signer certificate (the **agentTrust.jks** file) to each system. This enables them to reregister with the Agent Manager, at which time they will receive a new certificate to use to authenticate themselves.

# Backing up and restoring agents and resource managers

This section provides information on backing up and restoring agents and resource managers.

You do not need to specifically back up your agent and resource manager systems, aside from your standard backup procedures.

If the Agent Manager server must be restored, no special action is required on the agent or resource manager systems.

If the agent or resource manager itself fails, follow your standard procedures to reinstall it. The reinstall will have one of the following results:

- If the globally unique identifier (GUID) on the system was preserved across the failure, then the existing GUID is reused when the agent or resource manager is reinstalled. This allows the agent or resource manager to assume the identity it had before its failure.
- If the GUID is lost, such as when a computer is re-imaged, the installation of the agent or resource manager will create a new GUID. When the agent or resource manager registers with the Agent Manager server, it takes on a new identity. The information about the original agent or resource manager remains in the registry.

From a practical point of view, this distinction matters only if you configured the Agent Manager to save more than the most recent agent status update. In that case, you cannot associate the new agent with its previous configuration records.

You must wait a few days after reinstalling the agents, so that they appear inactive in the registry.

Uninstalling the agent or resource manager does not uninstall the GUID.

## **Recovering unregistered agents**

This section provides information on recovering agents that were unable to register.

Periodically, check the Agent Manager log for agents that are unable to communicate with the Agent Manager server. The recovery messages are in the <**Agent\_Manager\_install\_dir>\AgentManager\logs\SystemOut.log** file. Use the information in the log file to determine why the agent could not register and then take corrective action.

# Backing up and restoring your Tivoli Common Agent Services deployment

To protect your Tivoli Common Agent Services deployment against the loss of the Agent Manager server, it is a good idea to make regular complete backups of the systems and databases involved. However, you can get your deployment working again if you back up and restore a smaller set of critical files on the Agent Manager server. You can even restore your deployment without a backup of the registry database, because the Agent Manager server recreates the registry information about each active agent or resource manager the next time it connects to the Agent Manager server.

You can restore your Tivoli Common Agent Services deployment if you back up the following files on the Agent Manager server:

#### os.guid

This file contains the name of the Agent Manager server. Some resource managers use this information to verify that they are communicating with the correct Agent Manager server. When you reinstall the Agent Manager, this name might change. The file is located in the <Agent\_Manager\_install\_dir> directory.

## CARootKeyRing.jks

This file is the private key ring of the certificate authority in the Agent Manager. It contains the private key and the certificate of the public key for the Agent Manager. The file is located in the <Agent Manager install dir>/certs directory.

#### CARootKey.pwd

This file contains the password to decrypt the private key ring file. The file is located in the <Agent\_Manager\_install\_dir>/certs directory.

### agentKeys.jks

This file is the Agent Manager key store.

## agentTrust.jks

This file is the Agent Manager trust store.

**Note:** Keep the copy of these files in a secure location. A malicious user with access to these files can create an imposter Agent Manager server.

Although periodic database backups of the registry are important, you can restore your deployment without restoring the registry. By default, each agent provides a configuration update to the Agent Manager server every 24 hours. Thus, within 24 hours after reinstalling the Agent Manager server, the registry lists all active agents. Resource managers do not provide scheduled updates, but they contact the Agent Manager server frequently.

If you restore your environment without restoring the registry database, the following information is lost:

• Historical information about the agent, if the Agent Manager server was configured to save it.

By default, only the most recent agent update is saved.

• The certificate revocation list.

## Backing up the Agent Manager server

To protect your deployment of common agents and resource managers, make a backup copy of the Agent Manager files that are needed to restore your environment if your Agent Manager server has a serious problem.

Make a copy of the following files on the Agent ManagerAgent Manager:

#### os.guid

This file contains the Tivoli GUID of the Agent Manager, which uniquely identifies the server. Some resource managers use this information to verify that they are communicating with the correct Agent Manager. When you reinstall the Agent Manager, a new GUID is created, which might not match the original GUID. The file is located in the following directory: <Agent\_Manager\_install\_dir>

## Security files

The security files are in the <Agent\_Manager\_install\_dir/certs> directory. You should also ensure that you know the password that unlocks each of these files.

## CARootKeyRing.jks

This file is the private key ring of the certificate authority in the Agent Manager. It contains the private key and the certificate of the public key for the Agent Manager.

### CARootKey.pwd

This file contains the password to decrypt the private key ring file.

#### agentManagerKeys.jks

This file is the Agent Manager key store.

## agentManagerTrust.jks

This file is the Agent Manager trust store.

#### agentTrust.jks

This file contains the signer certificate for the Agent Manager.

**Note:** Keep the copy of these files in a secure location. A malicious user with access to these files can create an imposter Agent Manager server.

## **Restoring the Agent Manager server**

This section provides information about restoring the Agent Manager server after a failure.

If you experience a failure on the Agent Manager server that requires you to replace the computer system, reimage its hard drive, or reinstall its operating system, complete the following steps to restore your Tivoli Common Agent Services deployment:

1. Install the Agent Manager server.

**Note:** If the products you are using support a more recent version of the Agent Manager, you can install that version of the Agent Manager when you restore. The files you backed up are compatible with any version of the Agent Manager.

- Replace <Agent\_Manager\_install\_dir>/os.guid file created during the installation with the backup copy.
- Replace the following files in the <Agent\_Manager\_install\_dir>/certs directory with the backup copy:
  - a. CARootKeyRing.jks
  - b. CARootKey.pwd
  - c. agentManagerKeys.jks
  - d. agentManagerTrust.jks
  - e. agentTrust.jks
- 4. Restart the Agent Manager server.

# Changing agent registration properties

This section provides information for changing agent registration properties.

# **Controlling duplicate registration**

You can control whether the Agent Manager allows an agent that is registering with the registration password to assume the identity of another agent that is currently registered. This situation is referred to as *duplicate registration*. Duplicate registration can happen when an agent reregisters itself or when an agent attempts to maliciously assume the identity of another.

By default, duplicate registration is allowed. When duplicate registration is not allowed, an agent that loses its key cannot reregister until its entry in the registry is reset.

To modify the duplicate registration policy:

1. Edit the **AgentManager.properties** file using a text editor. The properties file is located in the following directory:

<Agent\_Manager\_install\_dir>\embedded\InstalledApps\<cell>\AgentManager.ear\ AgentManager.war\WEB-INF\classes\resource

 Set the Registration.Agent.Reregistration.Policy property to one of the following values:

**Any** Any agent may reregister. This is the default value.

- **OS** An agent cannot reregister, but multiple agents are allowed on a single computer system, as identified by the operating system GUID. There is no restriction on the number of managers on a computer system.
- **None** An agent may not reregister and there can be only one agent per computer system, as defined by the operating system GUID.

Any unrecognized value is treated as None.

- 3. Save the file.
- 4. Restart the Agent Manager.

## Removing old agents from the registry

This section provides information on removing inactive or obsolete agents from the registry.

Agents are not automatically removed from the registry when they become inactive or are uninstalled. To identify and remove obsolete agents from the registry, use the agent registration tools that are available in the toolkit subdirectory of the Agent Manager installation directory (<Agent\_Manager\_install\_dir>). For information about the agent deregistration tools, see the toolkit readme file in the toolkit directory.

# Managing resource manager authorization

The following sections describe how to change resource manager registration properties.

## Creating a user for resource manager registration

When the Agent Manager is installed, a single user named manager has the authority to register any resource manager. You can provide a more granular authorization by restricting the access of the default user and creating users that have authority to register only specified resource managers.

To create a new user for resource manager registration, use the **AuthXMLAddUser** command. This is the syntax for the command:

AuthXMLAddUser <user\_name> <clear\_text\_password> <auth\_type>
[<auth\_type> ...]

Where:

### <user\_name>

Specifies the name of the new user. User names are case-sensitive.

## <clear\_text\_password>

Specifies the password you want to set.

## <auth\_type>

Specifies one or more resource manager authorization types that the user is permitted to register. This value is case-sensitive. To allow the user to register any type of resource manager, specify "\*" (an asterisk symbol enclosed in double quotation marks). If the authorization type contains spaces, enclose the value in double quotation marks (").

For example, to create the user **FabricAdmin** on a Windows system, set the resource manager registration password to the string **myPassword** and grant the authority to register resource managers for type **IBM Tivoli Storage Productivity Center for Fabric**, run the following command:

<Agent\_Manager\_install\_dir>\bin\AuthXMLAddUser FabricAdmin
myPassword "IBM Tivoli Storage Productivity Center for Fabric"

To create the user **DataAdmin** on an AIX, Linux, or Solaris system, with the password **myPassword** and authority to register a resource manager of type **IBM Tivoli Storage Productivity Center for Data**, run the following command:

<Agent\_Manager\_install\_dir>/bin/AuthXMLAddUser.sh DataAdmin myPassword "IBM Tivoli Storage Productivity Center for Data"

To create the user **fred** on an AIX, Linux, or Solaris system, with the password **myPassword** and authority to register resource managers of type **IBM Tivoli Storage Productivity Center for Fabric**, run the following command:

<Agent\_Manager\_install\_dir>/bin/AuthXMLAddUser.sh fred myPassword "IBM Tivoli Storage Productivity Center for Fabric"

To create the user **fred** on an AIX, Linux, or Solaris system, with the password **myPassword** and authority to register resource managers of type **IBM Tivoli Storage Productivity Center for Data**, run the following command:

<Agent\_Manager\_install\_dir>/bin/AuthXMLAddUser.sh fred myPassword "IBM Tivoli Storage Productivity Center for Data"

To create the user **moosa** on an AIX, Linux, or Solaris system, with the password **myPassword** and authority to register any type of resource manager, run the following command:

<Agent\_Manager\_install\_dir>/bin/AuthXMLAddUser.sh moosa myPassword "\*"

## Removing a resource manager user name

This section provides information about the commands used to remove resource manager user names.

To remove a resource manager user, use the **AuthXMLRemoveUser** command. The syntax is as follows:

AuthXMLRemoveUser <user\_name>

Where:

<user\_name>

Specifies the name of the resource manager user. User names are case-sensitive.

For example, to remove the user **FabricAdmin** on a Windows system, run the following command:

<Agent\_Manager\_install\_dir>\bin\AuthXMLRemoveUser FabricAdmin

To remove the user **manager** on AIX, Linux, or Solaris system, run the following command:

<Agent\_Manager\_install\_dir>/bin/AuthXMLRemoveUser.sh manager

### Creating a resource manager authorization type

This topic describes how a new resource manager authorization type is created.

You do not explicitly create resource manager authorization types. A new type is created when you create a user and give them access to an authorization type that does not yet exist.

#### Removing a resource manager authorization type

This section provides information about the commands used to remove resource manager authorization types.

A resource manager authorization type is deleted automatically when the last user is removed from its user list. You can also remove an authorization type explicitly with the **AuthXMLRemoveAuthType** command. The syntax of the command is as follows:

AuthXMLRemoveAuthType <type\_name>

Where:

### <type\_name>

Specifies the name of an authorization type. Authorization type names are case-sensitive.

For example, to remove the **IBM Tivoli Storage Productivity Center for Fabric** authorization type on a Windows system, run the following command:

```
<Agent_Manager_install_dir>\bin\AuthXMLRemoveAuthType
"IBM Tivoli Storage Productivity Center for Fabric"
```

For example, to remove the **IBM Tivoli Storage Productivity Center for Data** authorization type on a Windows system, run the following command:

```
<Agent_Manager_install_dir>\bin\AuthXMLRemoveAuthType
```

```
"IBM Tivoli Storage Productivity Center for Data"
```

To remove the **manager** authorization type on an AIX, Linux, or Solaris system, run the following command:

<Agent\_Manager\_install\_dir>/bin/AuthXMLRemoveAuthType.sh manager

When the Agent Manager is installed, the **Authorization.xml** file contains the following statement, which allows the user **manager** to access all authorization types:

```
<authType name="*" userList="manager"/>
```

To delete the wildcard authorization type, run the following command: AuthXMLRemoveAuthType "\*"

# Configuring unsuccessful login threshold and lockout periods for resource managers

The Agent Manager protects resource manager registration against attacks by limiting the number of unsuccessful login attempts that may be made by a user in a fixed time period. This makes it impractical for an attacker to try a large number of user ID and password combinations. Unsuccessful login attempts are logged. You should monitor the log. A large number of failed login attempts may indicate an attack.

To change the threshold for unsuccessful attempts to register using a resource manager user or the amount of time that the user is locked out, follow these steps:

1. Edit the **AgentManager.properties file** using a text editor. The properties file is located in the following directory:

<Agent\_Manager\_install\_dir>\embedded\InstalledApps\<cell>\AgentManager.ear\ AgentManager.war\WEB-INF\classes\resources

2. Change the Registration.Manager.Authorization.Strikes,

Registration.Manager.Authorization.ResetIntrvl, and

Registration.Manager.Authorization.ResetScanIntrvl properties as follows:

# Registration.Manager.Authorization.Strikes

Specifies the threshold. Set this to the number of times a resource manager user can unsuccessfully attempt to register before the user is locked out. To disable tracking of unsuccessful attempts, set the value to zero or a negative integer.

# Registration.Manager.Authorization.ResetIntrvl

Specifies both the lockout duration and the reset interval. Set this to the number of seconds that the user is locked out, which is also the amount of time before the strike count is reset (set to zero) when no additional unsuccessful attempts are logged.

# Registration.Manager.Authorization.ResetScanIntrvl

Specifies the reset scan interval. Specify how often, in seconds, the Agent Manager should scan for users that are eligible to be unlocked or whose strike count can be reset because no additional unsuccessful attempts are logged.

For example, if the reset interval is 10 minutes (600 seconds) and there is one failed attempt every 11 minutes, then the user will never be locked out because the strike count is reset every 10 minutes. However, if there is one failed attempt every 9 minutes, then the strike count accumulates until the threshold is reached. When the threshold is reached, the user is locked out for 10 minutes plus between zero and reset scan interval additional seconds. When the ID is reset, the strike count is set to zero.

- 3. Save the file.
- 4. Restart the Agent Manager.

# Configuring how long agent configuration information is saved

By default, the registry contains only the most recent operational state and the associated error state record for each agent. You can configure the Agent Manager to save additional information.

To change the retention period for configuration information, perform the following steps:

- Edit the AgentManager.properties file using a text editor. The properties file is located in the following directory: <Agent\_Manager\_install\_dir>\embedded\InstalledApps\<cell>\AgentManager.ear\ AgentManager.war\WEB-INF\classes\resources
- 2. Set the Status.timeToLive property to one of the following values:
  - **0** Only the most recent record is kept for each agent. This is the default value.
  - *n* Keeps agent configuration records for *n* hours, where *n* is a positive integer.
  - -1 Keeps all agent configuration records. This setting will greatly increase the size of your registry database.
- **3**. Save the file.
- 4. Restart the Agent Manager.

# Changing the maximum heap size for Agent Manager

This topic describes how to change the maximum heap size for the Agent Manager.

When you install the Agent Manager, it has a default maximum heap size of 100 MB for the server. If you have a lot of common agents and request a list of agents from the Agent Manager, the Agent Manager will produce a core dump. For example, 800-900 agents is considered a lot of agents.

The following example assumes that you have installed Agent Manager using the default directory. To correct this problem on Windows, complete the following steps:

- Go to the following directory: C:\Program Files\IBM\AgentManager\embedded\bin
- Enter the following command: stopserver AgentManager

Wait until the Agent Manager has successfully stopped.

**3**. Go to the following directory:

C:\Program Files\IBM\AgentManager\embedded\config\cells\ DefaultNode\nodes\DefaultNode\servers\AgentManager

 Edit the server.xml file and search for the following: genericJvmArguments=""

Change this to: genericJvmArguments="-Xmx512m"

Save the file.

- Go to this directory: C:\Program Files\IBM\AgentManager\embedded\bin
- 6. Enter the following command: startserver AgentManager

Wait until the Agent Manager successfully starts.

# Multiple Agent Managers in your enterprise

You need to have only one Agent Manager in your production environment. This topic provides information if you want to use more than one Agent Manager in your enterprise.

If the Agent Manager is already installed, you can reuse it for additional products. When you install subsequent products that use the Agent Manager, the product installation requires you to provide information needed to connect to the existing Agent Manager. For more information, see

You can have multiple installations of the Agent Manager in your environment, but there is no communication between them. That is, the Agent Manager, agents, and resource managers from one installation cannot interact with the Agent Manager, agents, and resource managers in another installation.

If you plan to have a separate production environment and a test environment, specify a different name for the certificate authority when you install the Agent Manager for each environment.

# **Reusing an existing Agent Manager**

Multiple management applications can use the services of a single Agent Manager. When you install a management application or product that will reuse an existing Agent Manager, this topic provides information on that procedure.

When you install a management application or product that will reuse an existing Agent Manager, the installation requires you to provide the following information, which is needed to connect to the existing Agent Manager:

- The host name where the Agent Manager is installed
- The TCP/IP port used to connect to the Agent Manager

The information is in the AgentManager.properties file, which is located in the following directory:

<Agent\_Manager\_install\_dir>\embedded\InstalledApps\<cell>\AgentManager.ear\ AgentManager.war\WEB-INF\classes\resources

Use the values in the following properties:

## ARS.host

This property specifies the host name of the Agent Manager server. Use the exact value of this property, which is typically an IP address or a fully qualified host name.

# ARS.port.base

This property specifies the port that is used for secure SSL communication. The default value is 9511.

## **ARS.port.secure**

This property specifies the port that is used for secure SSL communication with client authentication. The default value is 9512.

## ARS.port.public

This property specifies the port that is used for unsecured, public communication. This port is used when initially contacting the Agent Manager and for agent recovery requests. The default value is 9513.

# Administering data sources

Use the following topics for information about how to administer CIMOM agents, Data agents, Storage Resource agents, Inband Fabric agents, Out of Band Fabric agents, IBM Tivoli Storage Productivity Center servers, and VMware VI data sources.

# Checking the health of your agents

This topic provides information about checking the health of your agents.

Expand **Administrative Services → Data Sources** and left-click on the following nodes:

- CIMOM Agents
- Data/Storage Resource Agents
- Inband Fabric Agents
- Out of Band Fabric Agents

A list of agents is displayed in the right pane. If these agents are up and running, there is a green health status icon in the State column. For the CIMOM, a green health status icon is displayed in the Connection Status column.

# Manually changing the Windows service logon for the agent

This topic describes how to change the Windows service logon for the Common agent.

To change the Windows service logon for the Common agent, complete the following steps:

- 1. In Windows, open the Services panel: Start → Settings → Control Panel → Administrative Tools → Services.
- 2. On the Services panel, right-click **IBM Tivoli Common agent 'C:\Program Files\IBM\TPC\ca'**. Select **Properties**.
- 3. Select the Log On tab. Change This account field with your changed logon ID. If your Tivoli Storage Productivity Center server is part of a Windows domain, change this logon to <domain>\<account>. For example, mydomain\myaccount. Enter the password if you have changed the password. Click Enable and then OK. The Common agent requires that the domain account have local administrator privileges as well as "Log on as a service" and "Act as part of the operating system" user rights.

# **CIM** agents

CIM agents provide a CIM interface for management applications. These include IBM Tivoli Storage Enterprise Storage Server (Tivoli Storage Enterprise Storage Server), SAN Volume Controller, DS4000, DS6000, and DS8000, any SMI-S certified CIMOM, and tape and switch CIMOMs.

# Adding a CIM agent manually

CIM agents provide a Common Information Model (CIM) interface for management applications. This topic discusses how to manually add a CIM agent.

To add a CIM agent to the CIMOM node, follow this procedure:

- 1. In the Navigation Tree pane, expand Administrative Services → Data Sources and click CIMOM Agents.
- 2. In the right pane, click Add CIMOM. The Add CIMOM window opens.

- 3. Specify information about the CIM agent:
  - **Host** The hostname of the machine on which the CIMOM is installed. You can enter a host name, IPv4, or IPv6 address depending on what is supported within your environment:
    - Enter an IPv4 address in the following format: ###.###.###. For example: 192.168.1.65

You can enter an IPv6 address for a CIMOM if the machine where IBM Tivoli Storage Productivity Center is installed is IPv6 or dual stack (IPv4 and IPv6) enabled.

**Port** The port on which the CIMOM is listening. By default this is 5989 for a secure connection and 5988 for an unsecure connection. See the documentation for the appropriate SMI-S CIM Provider for more information about available ports.

## Username

The user ID used for authentication, if required by the CIMOM.

## Password and Password Confirm

The password, if required by the CIMOM.

## Interoperability Namespace

This namespace within the CIMOM allows for accessing the CIM Interop Schema (including the class instances of the Server Profile) and determines how IBM Tivoli Storage Productivity Center interacts with the CIMOM when retrieving information. The following are the default namespaces for CIMOM agents for switches:

- IBM: /root/ibm
- Brocade: /interop
- NetApp: /interop
- Cisco: /root/cimv2
  - For version 3.2.1 or later: /root/pg\_interop
- Engenio: /interop
- EMC: /root/emc
- HDS: For HiCommand 5.6 or higher, use /root/smis/current For a HiCommand version that supports SMI-S 1.2, use following namespace to traverse the model as SMI-S 1.1: /root/smis/smis11
   For HiCommand versions lower than HiCommand 5.6, use: /root/hitachi/dmxx, where xx is represents the level of HiCommand.
- HP: /root
- McData: /interop
- SUN (storage subsystem): /root/sun3510 or /interop
- XYRATEX: /root/PG\_interop

To view a list of default namespaces for CIMOM agents for storage subsystems that is included with Tivoli Storage Productivity Center, open the following file in a text editor: *install\_directory*/data/ config/namespace.config, where *install\_directory* represents the directory where the product is installed.

Check the documentation of the appropriate SMI-S CIM Provider or contact the storage system vendor to ensure you use the most current namespaces.

## Protocol

The version of the cim-xml protocol. Can be http or https.

# **Truststore Location**

The location (path on this computer) of a certificate file for certificate based authentication in the https protocol. This field applies only to certain non-IBM devices. See the documentation for the appropriate SMI-S CIM Provider for more information about the truststore location.

## **Truststore Passphrase**

The passphrase for the truststore for the CIMOM.

## **Display Name**

The name of the CIMOM, as specified by the CIMOM provider, that will appear in the Tivoli Storage Productivity Center interface.

## Description

The optional description.

## Test CIMOM connectivity before adding

Check box. Check this box to have Tivoli Storage Productivity Center ensure that communication to the CIMOM is working properly before adding information about that CIMOM.

4. Click Save.

**Note:** This procedure does not physically add a CIMOM, but adds the information you have given about the CIMOM to Tivoli Storage Productivity Center so that Tivoli Storage Productivity Center can communicate with the CIMOM.

# Discover CIM agents automatically

This topic discusses how to discover storage subsystem CIMOMs that are visible to the Device server using Service Location Protocol (SLP).

In many cases CIM agents can be automatically discovered using SLP. The criteria is that the CIM agent must be visible to the Device server.

To automatically discover all CIM agents that are visible to the Device server, complete the following steps:

- 1. In the navigation tree pane, expand **Administrative Services** → **Discovery** and click **CIMOM**.
  - a. Click the **Options** tab.
  - b. Enter the IP address or host name for the SLP directory agents for CIMOM discovery. Or select the **Scan local subnet** check box.
  - c. Click **File** → **Save** on the menu bar to save the information.
- 2. Right-click CIMOM and click Run Now.

- **3**. After you submit a CIMOM discovery job, a message window is displayed with the text **CIMOM Discovery Job submitted**. Click **OK**. The job name is located below **CIMOM**. While it is running, the CIMOM job has a blue circle outline to the left of the job name.
- 4. To determine if the job has completed, right-click **CIMOM** and click **Update Job Status**. If the job has completed successfully, a green square is shown in front of the job name. If the job has completed but failed, a red circle is shown.

**Note:** The job returns as failed if one or more sub-jobs failed. Some CIMOMs might still have been discovered.

- After the job completes, the discovered CIM agents are listed in the CIMOM Agents table. Expand Administrative Services → Data Sources and click CIMOM Agents.
- 6. For each CIM agent that you want to use, highlight the CIM agent and click the magnifying glass at the left of the listing. You must select the CIM agents one at a time. The **CIMOM Agents** window is opened.
- 7. Enter additional information for the CIM agent, such as the user name and password, and select the **Test CIMOM connectivity before updating** check box.
- 8. Click **File** → **Save** on the menu bar to save the information and perform a connectivity check.

**Note:** This procedure does not physically add the CIM agent to your environment, but provides IBM Tivoli Storage Productivity Center with the information it needs to communicate with that CIM agent. This includes information that you have defined and CIM agents discovered using SLP.

# Viewing information about a CIM agent

Use panels and reports in IBM Tivoli Storage Productivity Center to view detailed information about a CIM agent.

Use the following reports to view information about a CIM agent:

- In the Navigation Tree pane, expand IBM Tivoli Storage Productivity Center → Reporting → Data Source Reports → CIMOM Agents and click By CIMOM Agent or By Managed Device.
- In the Navigation Tree pane, expand Administrative Services → Data Sources and click CIMOM Agents. A list of CIM agents appears in the content pane. Click the magnifying glass next to a CIM agent to view the following information about that agent:

# Service URL

The service URL of the CIMOM containing the IP address of the CIMOM, the port on which the CIMOM is listening, and the protocol used for communication. This URL has a protocol [http | https], an IP or Hostname, and a port number. This field displays IPv4 and IPv6 addresses as appropriate.

## **Display Name**

The name of the CIMOM as specified by the CIMOM provider that will appear in the IBM Tivoli Storage Productivity Center interface.

## Description

The optional description that was entered on the Add CIMOM window.

## Username

The CIMOM user ID used for authentication.

## Password and Password Confirm

The password for the CIMOM.

## Interoperability Namespace

Enter the interoperability namespace of the CIMOM. This namespace within the CIMOM allows for accessing the CIM Interop Schema (including the class instances of the Server Profile) and determines how Tivoli Storage Productivity Center interacts with the CIMOM when retrieving information.

## **Truststore Location**

The location (path on this computer) of a certificate file for certificate based authentication in the https protocol.

# **User Interface Description**

The name of the Human Interface Service (if any) supported by this CIMOM.

## Software Level

The software version level of the CIMOM agent.

## **Protocol Version**

The version of the cim-xml protocol.

## Authentication Mechanism

The authentication mechanism supported by the CIMOM. This field can contain the following values: Unknown, None, Other, Basic, Digest.

Alias The alias of the CIMOM.

# Service ID

The service ID for the CIMOM.

## Protocol

The communication protocol used for the CIMOM. Possible values are http and https.

## **SLP** Attributes

The standard set of attributes for this CIMOM. The attributes are retrieved via SLP.

## **Connection Status**

The status of this CIMOM with respect to Tivoli Storage Productivity Center. Possible values are: SUCCESS, UNCONFIGURED, UNKNOWN, INVALID\_NAMESPACE, TIMEOUT, REFUSED, LOGIN\_FAILED, SSL\_HANDSHAKE\_ERROR, SSL\_REGISTRATION\_INVALID, CIMCLIENT\_ERROR

## Status Timestamp

The date/time when the Connection Status information was last collected.

# Test CIMOM connectivity before updating

If this box is checked Tivoli Storage Productivity Center ensures that communication to the CIMOM is working properly before making any changes.

# Updating CIM agent user identification

After a CIM agent has been added to the **CIMOM** node, you can update the user ID, password, and other information.

To update the CIM agent user identification, follow this procedure:

- 1. In the Navigation Tree window, expand Administrative Services → Data Sources. Left-click CIMOM.
- 2. In the right pane, click on the icon to the left of the agent for which you want to change information.
- **3**. Information about the CIM agent is displayed in the Information window. The fields which can be updated are:

# **Display Name**

The name of the CIM agent, as specified by the CIMOM provider, that will appear in the IBM Tivoli Storage Productivity Center interface.

# Description

The name of the CIM agent, as specified by the CIMOM provider, that will appear in the Tivoli Storage Productivity Center interface.

# Username

The user ID used for authentication, if required by the CIM agent.

# Password and Confirm Password

The password for the CIM agent, if required by the CIM agent.

# Interoperability Namespace

This namespace within the CIM agent allows for accessing the CIM Interop Schema (including the class instances of the Server Profile) and determines how Tivoli Storage Productivity Center interacts with the CIM agent when retrieving information.

# Test CIMOM connectivity before updating

Check box. Check this box to have Tivoli Storage Productivity Center ensure that communication to the CIM agent is working properly before updating information about that CIM agent.

- 4. Save your changes by clicking the Save icon.
  - If you have selected **Test CIMOM connectivity before updating**, the CIMOM connectivity check will be run when you save the changes.
  - If **Test CIMOM connectivity before updating** is not selected, a discovery will be started immediately after you save the changes.

# Testing a CIM agent connection

Manually check to make sure that communication to the CIM agent is working properly.

To test a CIM agent connection, follow this procedure:

- 1. In the Navigation Tree, expand Administrative Services → Data Sources. Left-click CIMOM.
- 2. In the right pane, select a CIM agent. Click **Test CIMOM Connection**. a confirmation dialog appears: "Testing CIMOM connectivity can take up to several minutes in case of an incorrectly entered port number, network problems or an unpassed firewall. Would you like to continue anyway?" Select **yes** to perform the CIMOM connection test.
- 3. To close the Test CIMOM Connection window, click OK.

# **Removing a CIM agent**

You can remove a CIM agent from the navigation tree and the repository database. Data discovered by the CIM agent is not removed from the repository.

To remove a CIM agent, follow this procedure:

- 1. In the Navigation Tree pane, expand **Administrative Services** → **Data Sources**. Left-click **CIMOM Agents**.
- 2. In the right pane, select a CIM agent. Click Remove CIMOM.
- **3**. The Remove CIMOM confirmation window opens. Click **Yes**. The CIM agent is immediately deleted from the list.

# Show managed devices for a CIM agent

You can display the managed devices for a CIM agent.

To show the managed devices for a CIM agent, follow these steps:

- 1. In the Navigation Tree pane, expand Administrative Services → Data Sources. Left-click CIMOM Agents.
- 2. In the right pane, select a CIM agent. Click Show Managed Devices.
- **3**. The CIMOM Managed Devices window opens displaying the managed devices. Click **OK** to close the window.

# Collecting CIM agent logs

You can collect logs for certain IBM CIM agents using the command line interface.

1. Change to the directory where the CIM agent is installed.

DS3000, DS4000, DS6000, DS8000	On Linux	/opt/IBM/cimagent/cimom
	On Windows	C:\Program Files\IBM\cimagent\ cimom
SAN Volume Controller	On Linux	<usr opt="" or="">/IBM/svcconsole/ support</usr>
	On Windows	C:\Program Files\IBM\svcconsole\ support

2. Run one of the following commands:

On Linux	collectLogs.sh
On Windows	collectLogs.bat

A **collectedLogs.zip** file is created.

Attention: this file is overwritten if you run the script again.

## Collecting XIV CIM agent logs

The log files for the XIV Storage System CIM agent are bundled with the XIV Storage System system logs.

The log files for the XIV Storage System CIM agent are collected using the XIV Storage System XCLI commands. These commands are available on any host that has the XIV Storage System GUI installed or on the system where Tivoli Storage Productivity Center Element Manager starts the XIV Storage System GUI. You use the XCLI commands to bundle the log files into compressed tar files on the XIV Storage System device and then you use a web browser to retrieve those tar files using HTTP.

The XCLI command utility is included with the XIV Storage System GUI and is located by default at the following location: C:/Program Files/XIV/GUI10.

The following command prints the help text for the XCLI command utility: xcli -h

To collect the log files, perform the following steps:

- Enter the following command to list the known XIV Storage System configurations that were set up using the XIV Storage System GUI: xcli -L
- 2. Using the information gathered in Step 1, note the IP address of the XIV Storage System for which you want to collect the logs.
- **3**. Enter the following command to collect the XIV Storage System system logs for the XIV Storage System identified in Step 2:

xcli -u <admin\_user> -p <admin\_password> -m <ip\_of\_the\_XIV\_system> system\_logs\_collect
where:

- *admin\_user* is the administrator user name.
- *admin\_password* is the administrator password.
- *ip\_of\_the\_XIV\_system* is the IP address of the XIV Storage System to use for collecting the log files.

For example, the following command collects system logs from the IP address 129.42.58.216:

xcli -u admin -p abcabc -m 129.42.58.216 system\_logs\_collect

4. Since log collection may take some time, enter the following command to monitor the log collection process:

xcli -u <admin\_user> -p <admin\_password> -m <ip\_of\_the\_XIV\_system> system\_logs\_get\_status Log collection is complete when you see status message: system logs are available over HTTP.

- 5. To access the logs, start a web browser and go to the following URL: http://<ip\_of\_the\_XIV\_system>.
- When prompted, download the tar files and make a note of the download directory. The tar file will have a name like system\_xray\_2810A14unknown\_2009-02-03-2319[1].tar.bz2.
- 7. Locate the tar file and use an archive manager utility such as WinRAR to extract the log files from the tar archive.
- 8. Locate the XIV Storage System CIMOM log files by navigating to the following path within the archive: xray\7\FS\local\cim\log.

## Verifying that a CIM agent is running

You can verify that a CIM agent is running from the command line interface.

To verify that a CIM agent is up and running, run the following command: telnet <IP> <port>

Where <IP> is the IP address of the system where the CIM agent is installed, and <port> is the port number. By default, this is 5989 for a secure connection and 5988 for an unsecure connection.

# Data agents and Storage Resource agents

This topic provides information about administering, configuring, and viewing information about Data agents and Storage Resource agents.

See "Using Data agents or Storage Resource agents" on page 300 for information about the differences between Data agents and Storage Resource agents.

# Viewing information about an agent

From the IBM Tivoli Storage Productivity Center GUI, you can view detailed information about a Data agent or Storage Resource agent.

To view information about a Data agent or Storage Resource agent, complete the following steps:

- In the navigation tree, click Administrative Services > Data Sources. Left-click Data/Storage Resource Agents.
- 2. In the right pane, click the magnifying glass icon to the left of a Data agent or Storage Resource agent under the list of agents. In the right pane, a notebook window opens. On the General page, the following information is displayed:
  - Agent Displays the name of an agent and indicates whether the agent is enabled or disabled.
  - **Port** Displays the port number on which the agent is listening for requests.

### **Host Address**

Displays the host address of the computer on which an agent is running.

#### Last update

Displays the date and time when an agent was last updated.

### Timezone

Displays the current time zone for an agent.

# **Connection Errors**

Displays any connection errors that occurred for an agent.

## **Consecutive Errors**

Displays how many errors occurred consecutively.

**3**. Click the **Details** tab to view more detailed information. The following information is displayed:

Agent Displays the name of the agent.

**Host** Displays the host name of the system on which the agent is running.

#### Host ID

Displays the identifier of the host computer in hexadecimal format. Tivoli Storage Productivity Center only collects Host ID information for Solaris systems. All other platforms will display GUID information in the Host ID column.

## Start Time

Displays the date and time that the agent was started.

#### **Elapsed** Time

Displays the time elapsed since the agent was last updated.

## VM Size

Displays the size (in MB) of the disk space that is allotted to virtual memory for the agent.

## Manufacturer

Displays the manufacturer of the system.

### OS Type

Displays the operating system that is running on the system.

#### **CPU** Architecture

Displays the architecture of the system.

## Job Count

Displays the number of jobs scheduled to run against the agent.

4. Click the **Jobs** tab to view information about the jobs scheduled to run on the managed system.

# Viewing an agent log file

The log file for a Data agent or Storage Resource agent contains informational, warning, and error messages for the previous sessions of the agent. You can use the log file to troubleshoot errors that might occur when starting an agent, processing, or shutting down the agent.

The log file is located in the agent installation directory:

#### **Storage Resource agents**

For Windows default: C:\Program Files\IBM\TPC\agent\log\
<computer\_name>\agent.log.

For Linux or AIX (default): /opt/IBM/TPC/agent/log/ <computer\_name>agent.log.

#### Data agents

For Windows (default): C:\Program Files\IBM\TPC\ca\subagents\TPC\ Data\log\<computer\_name>.

For Linux or AIX (default): /opt/IBM/TPC/ca/subagents/TPC/Data/log/ <computer\_name>.

For Data agents, by default, information from the last five sessions of the agent appears in the log window. A session starts when the agent is started and ends when the agent stops. You can increase or decrease how many sessions are kept in the history file by changing the value for the **logFilesKept** parameter in the agent.config file. The default location for the agent.config file is:

#### Windows

C:\Program Files\IBM\TPC\ca\subagents\TPC\Data\config\

#### Linux or UNIX

/opt/IBM/TPC/ca/subagents/TPC/Data/config

To view the log for a Data agent or Storage Resource agent, complete the following steps:

- In the navigation tree, click Administrative Services > Data Sources. Left-click Data/Storage Resource Agents.
- 2. In the right pane, select a Data agent or Storage Resource agent and click View Log.

# Configuring a Data agent

You can change the configuration of a Data agent by modifying the values that are specified in the **agent.config** file. The configuration parameters that are set in the **agent.config** file include the host name of the system on which the Data server is installed, the port on which the Data agent listens, and log file options.

To modify the configuration parameters for a Data agent, complete the following steps:

1. Using a text editor, modify the **agent.config** file. This file is located in one of the following directories:

On AIX	/opt/IBM/TPC/ca/subagents/TPC/Data/config

On Linux	/opt/IBM/TPC/ca/subagents/TPC/Data/config
On Windows	<pre><directory>\TPC\ca\subagents\TPC\Data\config</directory></pre>

where <directory> is the directory where the Data agent is installed.

- 2. Save the modified **agent.config** file.
- From the IBM Tivoli Storage Productivity Center GUI, in the navigation tree, click Administrative Services > Data Sources. Left-click Data/Storage Resource Agents.
- 4. In the right pane, select a Data agent. Click **Read Config**. The Data server reads the **agent.config** file that you modified in step 1 and applies the changes.

# Configuring tracing for an agent

You can configure and enable tracing for a Data agent or Storage Resource agent. This provides extensive logging of exception and trace messages; it can provide useful information for the IBM Support center.

You must have administrator authority to perform this procedure.

To configure tracing for a Data agent or a Storage Resource agent, complete the following steps:

- In the navigation tree, click Administrative Services > Data Sources . Left-click Data/Storage Resource Agents.
- 2. In the right pane, select a Data agent or Storage Resource agent. Click **Configure Tracing**. The Tracing Configuration window opens.
- 3. Select the **Enable Trace** check box.
- 4. Specify the tracing options:
  - a. In the Level field, select one of the following options:

# DEBUG\_MIN

Minimum level of debugging

# DEBUG\_MID

Medium level of debugging

# DEBUG\_MAX

Maximum level of debugging

- b. In the **Maximum Number of Files** field, specify the maximum number of trace files that are created. When this number is reached, the oldest file is overwritten. By default, this is set to five.
- **c**. In the **Maximum File Size (kilobytes)** field, specify the maximum size of each trace file.
- 5. Click OK. The settings are saved to the AgentTraceLog.config file

# **Disabling an agent**

You can disable a Data agent or a Storage Resource agent. Disabling the agent signifies that the Data agent or Storage Resource agent is unavailable and the Data server should not contact that agent for any job processing.

You might want to disable a Data agent or Storage Resource agent in the following situations:

• The agent computer is undergoing maintenance and will be unavailable. This prevents the server from flagging the agent as "down" if it cannot reach the agent. The amount of times that the server tries to contact the agent is defined by the **agentErrorLimit** parameter in the server.config file.
• The agent computer is busy with resource-intensive processing and you do not want to add any jobs to that processing load.

While disabled, the agent name in the user interface is outlined with a red circle with a line through it. The server does not attempt to contact the agent.

To disable a Data agent or Storage Resource agent, complete the following steps:

- In the navigation tree, click Administrative Services > Data Sources > . Left-click Data/Storage Resource Agents.
- 2. In the right pane, select a Data agent or Storage Resource agent and click **Disable**.

## Enabling an agent

You can enable an agent that is currently disabled. After it is enabled, the Data server resumes communication with that agent. This action is available for disabled agents only.

If the server cannot contact an agent, the server automatically flags the agent as "down". Click **Enable** to reestablish communication between the agent and server. The number of times the server tries to contact the agent is specified in the **agentErrorLimit** parameter in the server.config file. The default is 3.

The default directory for the server.config file is:

#### Windows

C:\Program Files\IBM\TPC\Data\config

#### Linux or UNIX

/opt/IBM/TPC/Data/config

Tip: Clicking **Check** also enables an agent that is disabled.

To enable an agent, complete the following steps:

- In the navigation tree, click Administrative Services > Data Sources. Left-click Data/Storage Resource Agents.
- 2. In the right pane, select an agent and click Enable.

### Shutting down an agent

You can shut down Data agents and Storage Resource agents (run as daemon processes) from the graphical user interface.

To shut down an agent, complete the following steps:

- In the navigation tree, click Administrative Services > Data Sources. Left-click Data/Storage Resource Agents.
- 2. In the right pane, select a Data agent or Storage Resource agent and click **Shutdown**. This button is not available for Storage Resource agents that are installed as non-daemons.
- **3**. Select how you want an agent to shut down. You can select from the following options:

#### Normal

Shut down the agent software and let all running processes complete. The agent will continue to accept new jobs that are submitted and will not shut down until:

• All running processes are complete.

• There are no new jobs submitted.

### Immediate

Shut down the agent software when the currently running processes complete. No new jobs will be accepted by the agent and shutdown will occur immediately after the last job completes.

**Abort** Shut down the agent software and stop whatever processes are currently running.

You cannot start a Data agent from the Data/Storage Resource agent panel in the IBM Tivoli Storage Productivity Center user interface. To start a Data agent, you must access the computer on which the agent is installed and start it manually.

For Storage Resource agents that are run as daemon processes, you can use the **Start** button on the Data/Storage Resource agent panel to start those agents. See "Starting a Storage Resource agent" for more information about how to start Storage Resource agents.

## Starting a Storage Resource agent

You can start a Storage Resource agent if the daemon process for that Storage Resource agent is down.

You can only perform this task for Storage Resource agents running as a daemon service.

To start a Storage Resource agent, complete the following steps:

- In the navigation tree, click Administrative Services > Data Sources. Left-click Data/Storage Resource Agents.
- 2. In the right pane, select a Storage Resource agent and click Start.

## Checking whether an agent can communicate with the Data Server

You can check whether an agent can communicate with the Data server.

You can only perform this task for Storage Resource agents running as a daemon service.

To start a Storage Resource agent, complete the following steps:

- In the navigation tree, click Administrative Services > Data Sources. Left-click Data/Storage Resource Agents.
- 2. In the right pane, select an agent and click Check.

If a Data agent is selected, this operation verifies that the Data server can communicate with the selected agent.

If a Storage Resource agent is selected, this operation verifies that the Data server can communicate with the host system where the Storage Resource agent is installed with the appropriate authentication information. After verifying that the Data server can communicate with the selected agent, the process checks for the existence of the Storage Resource agent's runtime files.

## Changing authentication for a Storage Resource agent

There are times when you might need to change the user ID, password, and certificate location for a Storage Resource agent.

To change the authentication for a Storage Resource agent, follow these steps:

- 1. In the navigation tree, expand **Administrative Services > Data Sources**. Left-click **Data/Storage Resource Agents**.
- 2. In the right pane, select one or more Storage Resource agents for which you want to change authentication information.
- 3. Click Change Authentication.
- 4. In the Change Authentication window, enter the following information:
  - **User** Enter the user ID that IBM Tivoli Storage Productivity Center should use when logging on to the computer on which the Storage Resource agent is installed.

**Requirement:** This ID must have administrative or root privileges when installing a Storage Resource agent on a computer.

### Password

Enter the password.

## Re-type

Reenter the password.

## **Certificate Location**

Enter the fully qualified path of the certificate on the computer where the Data server is located. This file is used for certificate-based authentication. If you do not enter a value in this field the default location is used. When deploying Storage Resource agents, Tivoli Storage Productivity Center uses the Secure Shell (SSH) protocol to communicate with the target computer.

## Passphrase

Enter the passphrase for the certificate file. The passphrase was created when the certificate was generated.

Click Save.

## **Related Tasks:**

For information about certificates used after deployment, see "Planning for Storage Resource agents" on page 32.

## Adding Storage Resource agents

You can add Storage Resource agents to your system by scheduling a job or by adding an agent immediately.

To add a Storage Resource agent, complete the following steps:

- 1. In the navigation tree, you have two methods of adding a Storage Resource agent:
  - Click Administrative Services > Data Sources. Left-click Data/Storage Resource Agents. In the right pane, click Add Storage Resource agents.
  - Click Administrative Services > Configuration. Right-click Storage Resource Agent Deployments. On the menu, click Create Storage Resource Agent Deployments.
- **2**. The Create Storage Resource agent Deployments window opens displaying the Computers tab. Enter the following information:

## Header fields

Creator

Predefined creator name.

Name Predefined name.

### **Description (optional)**

Enter a user-defined description name for the job.

#### Enabled

Check this box to enable Storage Resource agent deployments.

## Add Host List

Click this button to manually enter names and logon credentials for the computers on which you want to deploy Storage Resource agents.

If you click this button, the Login Information window opens. You can enter information in the following ways:

- Click Add Agents from MS Directory to install Storage Resource agents on one or more Windows computers that are members of a Windows domain. Enter the domain controller name and login information on the displayed window. On the next window, select the domain and click Get List of Domain Computers. The host names of computers that you add using this method are displayed in the Remote Agent Machines section of the window. In that section, you must also enter an installation location for each computer and indicate whether you are reinstalling a Storage Resource agent on a computer.
- Click **Get Agent List From file** to retrieve a list of computer names from a flat text file. The computers that are listed in the file are automatically added to the deployment job and displayed in the **Remote Agent Machines** section of this window. In that section, you must also enter an installation location for each computer and indicate whether you are reinstalling a Storage Resource agent on a computer.

The file that you retrieve must contain one host name or IP address per line. For example:

systemxyz.storage.usa.ibm.com
9.79.179.179
systemzyx.storage.usa.ibm.com
9.89.189.189

If Tivoli Storage Productivity Center discovers any syntax problems in the file, none of the host entries in the file are added to the deployment job.

- Enter the computer names or IP addresses in the Remote Agent Machines table. Enter the installation locations. If you do not enter a value in this field the default location is used. The default installation directories are:
  - For Windows: C:\Program Files\IBM\TPC\agent
  - For Linux and UNIX: /opt/IBM/TPC/agent

• Select Force under the following circumstances:

- If an earlier Storage Resource agent installation failed and there are damaged agent files on the computer that cause further installations to fail. If you select this option, Tivoli Storage Productivity Center attempts to overwrite the previous failed deployment on the computer with a new Storage Resource agent.
- If you want an existing Storage Resource agent to communicate with an additional Tivoli Storage Productivity Center server. To do this, you must create the deployment job from the additional

Tivoli Storage Productivity Center server to which you want the Storage Resource agent to communicate.

#### Note:

- You cannot change the communication type for a Storage Resource agent (daemon or non-daemon) when you select the Force option. Make sure to select the same communication type as the existing Storage Resource agent when you create a deployment job.
- If a Storage Resource agent exists on a target computer and you do not select Force, an error occurs during validation and the Storage Resource agent is not installed.

## Enter the following information:

**User** Enter the user ID that Tivoli Storage Productivity Center should use when logging in to the host computer to install a Storage Resource agent. The value in the field is applied to all the computers that appear in the **Remote Agent Machines** table.

**Requirement:** This ID must have administrative or root privileges on the target computer.

#### Password

Enter the password for the user ID.

#### **Re-type**

Reenter the password for the agent machine.

#### **Certificate Location**

Enter the fully-qualified path of the certificate on the computer where the Data server is located. This file is used for certificate-based authentication. If you do not enter a value in this field the default location is used.

#### Passphrase

Enter the passphrase for the certificate file. The passphrase was created when the certificate was generated.

**Port** Enter the port number on which a Storage Resource agent listens for requests. The default is 9510.

**Tip:** This value is required if you run the Storage Resource agent as a daemon service.

#### Use Daemon Service for Runtime Operation

Select this option to run a Storage Resource agent on the monitored computer as a daemon service.

**Restriction:** Do not select this option to run the Storage Resource agent as a stand-alone executable file on the monitored computer.

## Validate before Save

Check this box to indicate that Tivoli Storage Productivity Center should attempt to communicate with the computers that are added to the deployment job when you click the **Save** button on this page. If the validation fails for a computer, the agent is not installed on that computer.

#### **Edit Selected Entries**

Click this button to edit settings for the selected Storage Resource

agents. This information includes user ID, password, certificate location, passphrase, and port. You must submit the deployment job for the changes to take effect.

#### Remove

Click this button to remove a Storage Resource agent from the deployment job.

**Tip:** This button does not remove the agent from Tivoli Storage Productivity Center if it is already installed; it only removes it from the deployment job.

3. Click the When to run tab to enter the following information:

#### How often to run

- Specify a time to run:
- Run now
- Run once at (specify a date and time to run)

#### How to handle time zones

Specify a time zone to use:

- Use the time zone that the server runs in
- Use this time zone (select a time zone)
- 4. Click the **Alert** tab to specify the following information:

#### **Triggering-Condition**

The triggering condition you can specify is: Storage Resource agent Deployment Failed

## **Triggered-Actions**

Choose from the following check boxes:

- SNMP Trap
- TEC Event
- Login Notification
- Windows Event Log
- Run Script
- Email

Depending on what action you select, you might have other choices to make. For example, if you select the **Windows Event Log** check box, the **Event Type** field becomes active so that you can specify a severity for the event in the Windows event log.

5. Click File > Save.

## **Related Tasks:**

Check the TPCD\_#####.log file in the Tivoli Storage Productivity Center installation directory to view the error messages related to failed validations. The following are the default locations for this log file:

- Windows: C:\Program Files\IBM\TPC\data\log
- UNIX/Linux: /opt/IBM/TPC/data/log

## Help command for Storage Resource agent

The **help** command for the Storage Resource agent provides information about the parameters for installing, uninstalling, and upgrading Storage Resource agents.

For information about the Storage Resource agent commands, run the **help** command. Follow these steps:

- Go to the installation location for the Storage Resource agent: cd <CD installation location>
- Run the following command: bin/Agent -help
- 3. The output from the **help** command is as follows:

```
Usage:

Agent -INSTALL

[-COMMTYPE DAEMON -AGENTPORT portnumber]

[-FORCE]

-INSTALLLOC pathname

-SERVERIP address[,address,...]

-SERVERPORT portnumber

[-USERID username -PASSWORD password -CERT file -PASSPHRASE phrase]

Agent -UNINSTALL

[-FORCE]

-SERVERNAME servername

Agent -UPGRADE

-INSTALLLOC pathname
```

For information about how to install the Storage Resource agent using commands, see "Installing the Storage Resource agents locally" on page 242.

For information about how to uninstall the Storage Resource agent using commands, see "Uninstalling the Storage Resource agent manually" on page 390.

For information about how to upgrade the Storage Resource agent using commands, see "Upgrading Storage Resource agents manually" on page 369.

## Deleting or uninstalling an agent using the GUI

You can delete or uninstall a Data agent or Storage Resource agent and all the data that is collected by that agent from the database repository. The information that is collected by the agent will no longer be available within IBM Tivoli Storage Productivity Center reports. When you delete an agent, the agent is uninstalled and you can no longer activate the agent.

To delete or uninstall a Data agent or Storage Resource agent, complete the following steps:

- In the navigation tree, click Administrative Services > Data Sources. Left-click Data/Storage Resource Agents.
- 2. In the right pane, select an agent and click **Delete**.

## Enabling or disabling automatic upgrade for agents

This topic provides information for enabling or disabling the automatic upgrade function for a Data agent or Storage Resource agent.

For Data agents, the agent will automatically be upgraded to the same version as the Data server. The upgrade occurs when the Data agent registers with the Data server and IBM Tivoli Storage Productivity Center determines that the Data agent is running an older version from the Data server. For Storage Resource agents, the agent is automatically upgraded to the same version as the Data server. The upgrade occurs when a probe is run against the Storage Resource agent and Tivoli Storage Productivity Center determines that the agent is running an older version from the Data server.

To enable the program so that a Data agent or Storage Resource agent can be automatically upgraded, follow these steps:

- 1. In the navigation tree, expand Administrative Services > Data Sources. Left-click Data/Storage Resource Agents.
- 2. In the right pane, select one or more agents for which you want an automatic upgrade performed.
- **3.** Click **Enable Auto Upgrade**. Note that if you click this button it shows **Disable Auto Upgrade**.

To disable the automatic upgrade function for agents, select the agents for which you want the automatic upgrade discontinued. Click **Disable Auto Upgrade**. Note that if you click this button, it shows **Enable Auto Upgrade**.

## Exporting a Storage Resource agent list

You can export a Storage Resource agent list to a formatted flat file. This list is used to manage user authentication through a script file. This list contains the host name, installation location, user ID, encrypted password, and fully qualified certificate file for the selected Storage Resource agents. The password is in the encrypted format with @ENC@ appended to the encrypted password. You can change the user authentication data such as user ID, password, and fully qualified certificate location.

This option is enabled for Storage Resource agents that use non-daemon based communication only. Information about Storage Resource agents that run as daemon processes on monitored computers is not exported to a file.

Storage Resource agents can either be run as a daemon service or non-daemon service (on-demand service). If the agent is run as a non-daemon service, there is no agent process running on the managed host. Programs on the host system are run as needed.

To export a Storage Resource agent list, complete the following steps:

- In the navigation tree, click Administrative Services > Data Sources. Left-click Data/Storage Resource Agents.
- 2. In the right pane, click Export Storage Resource Agent List.

## Updating a Storage Resource agent list

The Storage Resource agent list file is used to manage user authentication through a script file. This list contains the host name, installation location, user ID, encrypted password, and fully qualified certificate file for the selected Storage Resource agents. The password is in encrypted format with @ENC@ appended to the encrypted password. You can change the user authentication data such as user ID, password, and fully-qualified certificate location.

To update a Storage Resource agent list, complete the following steps:

- In the navigation tree, click Administrative Services > Data Sources. Left-click Data/Storage Resource Agents.
- 2. In the right pane, select the Storage Resource agents you want to update.

- **3.** Click **Export Storage Resource agent List** to export information about those agents to a file.
- 4. Edit the information in that file to match the changes that you want to make for the Storage Resource agents.
- 5. Click **Update Storage Resource agent List** and select the file to apply your changes. You can update the logon credentials for the Storage Resource agents that are listed with the information in a file that you specify. The file must use the following format for the host names you want to update:

host name installation location user ID password

If the Data server cannot find any Storage Resource agent with a host name and location that you specify in the file, that entry is ignored and the error is logged.

Keep in mind the following considerations when including a password in the update file:

For non-encrypted passwords: If you use "|" in the line for an agent, you
must provide an "escape" character before it. The escape character is "\". For
example, if the password you want to include in an update file is
"native|agent", use native\|agent in the update file.

If you use "\" in the line for an agent, you must provide an additional "\" as an escape character. For example, if the password is "native\agent", use native\\agent in the update file.

- For encrypted passwords:
  - To encrypt a password, start IBM Tivoli Storage Productivity Center's command-line tool (tpctool) from the \cli directory where Tivoli Storage Productivity Center is installed and run the following command: tpctool encrypt [password], where [password] represents the password you want to encrypt. This command will generate a text string that represents the encrypted version of the password. For example, output might appear like the following: iDroqToC070ubh5i4mxMHQ==. Copy this encrypted password to the correct location in the update file.
  - To include an encrypted password in an update file, you must add the following after the encrypted text: @ENC@. For example, an encrypted password in an update file might appear like this: iDroqToC070ubh5i4mxMHQ==@ENC@

## Note:

- Do not include @ENC@ at the end of non-encrypted passwords.
- See the *IBM Tivoli Storage Productivity Center Command-Line Interface Reference* for more information about **tpctool**.

## Registering the Data agent with a different server

This topic provides information on how to register the Data agent with a different server.

Use the PROBE\_ME file to get an existing Data agent to register with a different IBM Tivoli Storage Productivity Center Data server from the one that it currently uses. This file is also useful to reestablish the connection between the Data server and Data agent (for example, in the case of a Data server reinstallation). To change the registration of the Data agent with a different server, complete the following steps:

1. Change the name of the server in the agent.config file by performing the following steps:

- a. In the <TPC\_install>/ca/subagents/TPC/Data/config directory, open the agent.config file.
- b. Change the serverHost property to the IP address of the new Tivoli Storage Productivity Center server.
- Create a blank text file called PROBE\_ME (all in uppercase letters with no txt extension) in the root of the agent's Data agent directory (<TPC\_install\_dir>/ ca/subagents/TPC/Data/).
- **3**. Restart the agent.

This will initiate a probe job to run and the agent to register with the server specified in the agent.config file. If you put any text in the PROBE\_ME file, a default scan will also be run.

## **In-band Fabric agents**

In-band Fabric agents are agents that are used by Fabric Manager for in-band SAN operations.

## Displaying information about an in-band Fabric agent

You can view information about an in-band Fabric agent including the status, IP address, host name, operating system, and Host Bus Adapter data.

To display information about an in-band Fabric agent, follow this procedure:

- 1. In the Navigation tree pane, expand Administrative Services → Data Sources. Left-click Inband Fabric.
- 2. In the right pane, click on the icon to the left of the Fabric agent for which you want information for. In the right pane, a notebook window opens. On the General page, the following information is displayed:

**Status** The status of the agent.

#### **IP** Address

The IP address of the agent.

Host name

The host name of the agent.

#### **Operating System and Version**

The operating system and version of the agent (for example, Windows 9.1: Service Pack 2).

### HBA Data

The Host Bus Adapter data for the agent.

## Checking the in-band agent connection

You can check if an in-band Fabric agent is running and whether the version of the agent is up to date. A check also enables an agent that is disabled.

To check an in-band Fabric agent connection, follow this procedure:

- 1. In the Navigation Tree pane, expand Administrative Services → Data Sources. Left-click Inband Fabric.
- 2. In the right pane, select an agent and click **Check**.

**Note:** The Fabric agent status is taken from the database. Because the agent does not send indications when it is shut down, the status may not be current. The setup.properties file for the Fabric agent has the following default parameter set: monitorInterval=10. This indicates that the monitor will be

refreshed every 10 minutes. You can change the monitor setting for a different refresh time.

The status of the agent is displayed in the Agent Status window. If updates are required, they are automatically installed.

## Viewing an agent log

Use the content of the log file to troubleshoot any errors that might occur during startup, processing or shutdown. Service alerts, if any, are displayed in red.

To display the log of an in-band Fabric agent, follow this procedure:

- 1. In the Navigation Tree pane, expand Administrative Services → Data Sources. Left-click Inband Fabric.
- 2. In the right pane, select an agent and select **View Log**. In the right pane, the agent log is displayed.

## Deleting an in-band Fabric agent

You can delete an in-band Fabric agent from the navigation tree and the database. Data discovered by the agent is removed from the database repository. This action is available for inactive agents only. You must first stop the agent before deleting the information for the agent. The agent is not uninstalled from IBM Tivoli Storage Productivity Center.

To remove information for an in-band Fabric agent, follow this procedure:

- 1. In the navigation tree pane, expand Administrative Services → Data Sources. Left-click Inband Fabric Agents.
- 2. In the right pane, select the agent and click Delete.

## **Out-of-band Fabric agents**

Out-of-band agents are used by Fabric Manager for out-of-band SAN operations.

For information about the supported agent types for switch performance management and fabric zone configuration, see "Collecting data with the Fabric Manager" on page 77.

## Displaying information about an out-of-band agent

You can view information about an out-of-band agent including the IP address, status and SNMP community. If the agent is a Brocade switch, the admin users ID is also displayed if it has been previously entered.

To display information about an out-of-band agent, follow this procedure:

- 1. In the navigation tree pane, expand Administrative Services > Data Sources. Left-click Out of Band Fabric Agents.
- 2. In the right pane, click on the icon to the left of the agent for which you want information for. In the right pane, a notebook window opens. On the General Information page, the following information is displayed:

**Status** The status of the agent.

### Host Name

The host name of the system on which the agent is installed.

#### **IP** Address

The IP address of the system on which the agent is installed. This column displays IPv4 and IPv6 addresses as appropriate.

## **SNMP** Community Read

The name of the SNMP community that the agent belongs to. The SNMP community name acts as a password that is shared by one or more SNMP hosts. The community name is used to authenticate messages being received by this SNMP host. This field is optional and might be blank if the SNMP community has not been set. This default for this field is set for public.

**Note:** the default SNMP community is public. If this is not the correct community name for your environment, the out-of-band agent might not be able to properly perform scans.

## **SNMP** Community Write

The default for this field is set for private.

## **Brocade Advanced Properties**

The admin user name and password and whether advanced Brocade discovery has been enabled. These properties are optional and might be blank if an admin user name and password has not been set. These properties apply only if the agent is a Brocade switch.

## Updating out-of-band agent information

After an out-of-band agent has been added, you can update the SNMP community name and, if the switch is a Brocade switch, the user ID and password and enable advanced Brocade discovery.

**Note:** You should not add the Brocade user ID and password to all switches; for more information see "Zone configuration" on page 615.

To update information for an out-of-band agent, follow this procedure:

- 1. In the Navigation Tree pane, expand Administrative Services > Data Sources. Left-click Out of Band Fabric Agents.
- 2. In the right pane, click on the icon to the left of the agent.
- **3**. In the right pane, a notebook window opens. On the General page, update the following information:

### **SNMP** Community

The SNMP community the agent belongs to. This field is optional.

## **Brocade Advanced Properties**

The admin user name and password. Select the Enable Advanced Brocade discovery to enable advanced Brocade discovery. These properties are optional and apply only if the agent is a Brocade switch.

The Brocade API is supported on IPv4 systems only. IPv6 systems are not supported.

## Checking the out-of-band agent connection

You can check to determine if an out-of-band agent is running.

To check the agent connection, follow this procedure:

- 1. In the Navigation Tree pane, expand Administrative Services > Data Sources. Left-click Out of Band Fabric Agents.
- 2. In the right pane, select an agent and click **Check**. The status of the agent is displayed in the Agent Status window. If updates are required, they are automatically installed.

## Adding an out-of-band agent

This topic provides information about adding an out-of-band agent.

To add an out-of-band agent, follow this procedure:

- 1. In the Navigation Tree pane, expand Administrative Services > Data Sources. Left-click Out of Band Fabric Agents.
- 2. In the right pane, click Add.
- **3**. In the Add Out of Band Fabric Agent window, enter host name, SNMP community (optional) and, if the agent switch is a Brocade switch, enter a user ID and password (optional). Select the Enable Advanced Brocade Discovery check box to enable advanced Brocade discovery. Click **OK**.

Note: The Brocade API can be used with IPv4 only. IPv6 is not supported.

## Deleting an out-of-band agent

You can remove an out-of-band agent from the navigation tree and the database. Data discovered by the agent is not removed from the database repository.

To remove an out-of-band agent, follow this procedure:

- 1. In the Navigation Tree pane, expand Administrative Services > Data Sources. Left-click Out of Band Fabric.
- 2. In the right pane, select an agent and click Delete.

## Removing out-of-band Fabric agent data

If you have a McDATA Intrepid 10000 director and have out-of-band Fabric agents as well as in-band or SMI-S agents, and you have run an out-of-band fabric discovery job, you must delete the data collected from the out-of-band Fabric agent because that data is invalid. This topic provides information on how to delete the out-of-band agent data.

To remove out-of-band Fabric agent data, complete the following steps:

- 1. Open the IBM Tivoli Storage Productivity Center GUI.
- 2. Expand Administrative Services → Data Sources. Left-click Out of Band Fabric.
- 3. In the right pane, select the out-of-band agent and click Delete.
- 4. On the agent machine where you installed the in-band agent, stop the Common agent service.
- 5. On the server machine, open the Tivoli Storage Productivity Center GUI and display the topology viewer. Wait for the topology viewer to display a status of "missing" for the machine where the in-band agent is installed. This can take approximately 5 minutes or more.
- 6. On the agent machine where you installed the in-band agent, start the Common agent service. This will start the data collection.

## **IBM Tivoli Storage Productivity Center Servers**

Use the Administrative Services > Data Sources > IBM Tivoli Storage Productivity Center Servers function to manage the relationships between a *master* IBM Tivoli Storage Productivity Center server and its *subordinate* Tivoli Storage Productivity Center servers.

Creating master and subordinate relationships between Tivoli Storage Productivity Center servers enables you to use a single interface to generate reports based on data and metrics collected by multiple servers in a storage environment:

- A **master** server is a server that performs normal monitoring and reporting of storage resources like a standard server, but also gathers the storage information (using Tivoli Storage Productivity Center server probes) that has been collected by subordinate servers.
- A **subordinate** server is a server that monitors and reports on storage resources like a standard server, but also communicates with the master server during Tivoli Storage Productivity Center server probes. During these probes, the master server collects the storage information gathered by a subordinate server's agents and stores that information in its own database repository.



Figure 88. Master and subordinate server architecture

The rollup reports that reflect the storage information collected by the master server from subordinate servers are available in the **Tivoli Storage Productivity Center** > **Rollup Reports** node of the master server's navigation tree.

If the master server is located on an IPv6–only server, it can communicate with existing subordinate servers under the following conditions:

- The subordinate servers are upgraded to Tivoli Storage Productivity Center V4.1 or higher and
- The IPv6 protocol is enabled on the machines where they are located.

Before you can configure and manage subordinate servers, keep in mind the following:

- The master server must be up and running.
- You must be logged in to the user interface as an Tivoli Storage Productivity Center administrator or superuser
- We recommend that the master server should monitor no more than 500 unique data sources. This number includes subordinate servers, Data agents, Fabric agents (Inband and Out of Band), CIMOM agents, and VM servers (VMWare).
- We recommend that each subordinate server monitors no more than 1200 unique data sources. This number includes Data agents, Fabric agents (Inband and Out of Band), CIMOM agents, and VM servers (VMWare). Once this threshold has been met for a server, a new server should be deployed and all new agents pointed to it.
- After upgrading to Tivoli Storage Productivity Center V4.1 or later from a previous version of the application, you must run probes against a master server's monitored storage assets to have information about those assets appear in **Tivoli Storage Productivity Center > Reporting > Rollup Reports**.

## Adding an IBM Tivoli Storage Productivity Center Server

Learn how to add an Tivoli Storage Productivity Center server as a subordinate sever.

Keep in mind the following when adding a Tivoli Storage Productivity Center server as a subordinate server:

- How subordinate servers are configured to monitor storage entities within your environment can determine if fragmentation occurs within rollup reports. See Rollup reports Fragmentation for more information.
- Tivoli Storage Productivity Center servers must be at version 3.3 or greater to be added as a subordinate server.
- We recommend that the master server should monitor no more than 500 unique data sources. This number includes subordinate servers, Data agents, Fabric agents (Inband and Out of Band), CIMOM agents, and VM servers (VMWare).
- We recommend that each subordinate server monitors no more than 1200 unique data sources. This number includes Data agents, Fabric agents (Inband and Out of Band), CIMOM agents, and VM servers (VMWare). Once this threshold has been met for a server, a new server should be deployed and all new agents pointed to it.
- If the master server is located on an IPv6–only server, it can communicate with existing subordinate servers under the following conditions:
  - The subordinate servers are upgraded to Tivoli Storage Productivity Center V4.1 or higher and
  - The IPv6 protocol is enabled on the machines where they are located.

To add a server as a subordinate server, follow this procedure:

- 1. In the Navigation Tree pane, expand Administrative Services → Data Sources → Tivoli Storage Productivity Center Servers.
- 2. In the right pane, click Add Tivoli Storage Productivity Center Server.
- **3**. In the Add Tivoli Storage Productivity Center Server window, enter the following information:

### Host Name

Enter the host name of the machine on which the subordinate server is installed.

### Host Device server Port

Enter the port with which the subordinate server's Device server is listening for requests. The default port for Tivoli Storage Productivity Center servers is 9550.

### Host Authentication Password

Enter the password for the subordinate Tivoli Storage Productivity Center server. This host authentication password is entered when installing Tivoli Storage Productivity Center. Contact your system administrator or the person who installed Tivoli Storage Productivity Center to determine this password.

### **Display Name (optional)**

Enter a name for the subordinate server.

## **Description (optional)**

Enter a description for the subordinate server.

Test Tivoli Storage Productivity Center Server Connectivity before adding Select this check box to have the master server connect and log into the subordinate server using the information provided on this window. This test is performed when you click **Save**.

- 4. Click Save to add the server as a subordinate server.
  - If you selected **Test Tivoli Storage Productivity Center Server Connectivity before adding**, IBM Tivoli Storage Productivity Center attempts to connect to the subordinate server using the information provided on this window.
  - If you did not select Test Tivoli Storage Productivity Center Server Connectivity before adding, the subordinate server is automatically added as a subordinate server but has a connection status of Unknown on the Administrative Services → Data Sources → Tivoli Storage Productivity Center Servers window.

**Note:** If the login information for a subordinate server is incorrect, an error occurs and an associated error message dialog box is displayed.

## Viewing subordinate server details

Learn how to view information about the subordinate servers that have been associated with a master server.

After you add a subordinate server to a master server, basic information about that server appears on the **Administrative Services**  $\rightarrow$  **Data Sources**  $\rightarrow$  **TPC Servers** window. To view additional information about a subordinate server on the TPC Servers window, follow this procedure:

- 1. In the Navigation Tree pane, expand Administrative Services → Data Sources → TPC Servers.
- In the right pane, double-click a server row or click the icon next to a server for more detailed information about that server. Information about a subordinate server will appear on the Administrative Services → Data Sources → TPC Servers → TPC Server Details window.

## Testing the connection to subordinate servers

Learn how to test the connection from a master server to its associated subordinate servers.

After you add a subordinate server to a master server, basic information about that server appears on the **Administrative Services**  $\rightarrow$  **Data Sources**  $\rightarrow$  **TPC Servers** window. To verify that the master server can use the information provided to connect to subordinate server, follow this procedure:

- 1. In the Navigation Tree pane, expand Administrative Services → Data Sources → TPC Servers.
- 2. In the right pane, highlight the row for a subordinate server and click Test TPC Server Connection to test its connection to the master server. A message window will appear with the results of the tested connection. The information that appears in the Connection Status field will be updated to reflect its status.

## **Removing subordinate servers**

Learn how to remove a subordinate server from its association with a master server.

Use the **Administrative Services** → **Data Sources** → **TPC Servers** window to remove a subordinate server from a master server. Removing a subordinate server will:

- · Remove its information from master server's database repository
- Remove its information from all rollup reports

 Remove it from the TPC Servers list on the Administrative Services → Data Sources → TPC Servers window

To remove a subordinate server, follow this procedure:

- 1. In the Navigation Tree pane, expand Administrative Services → Data Sources → TPC Servers.
- 2. In the right pane, highlight the row of a subordinate server and click **Remove TPC Server**. A confirmation window appears.
- 3. Click Yes to confirm the removal of the subordinate server.

## Modifying subordinate server information

Learn how to modify information about the subordinate servers that have been associated with a master server.

After you add a subordinate server to a master server, basic information about that server appears on the **Administrative Services**  $\rightarrow$  **Data Sources**  $\rightarrow$  **TPC Servers** window. You can edit the information for a subordinate server by modifying its Display Name, Description, and Host Authentication Password. To view modify information about a subordinate server on the TPC Servers window, follow this procedure:

- 1. In the Navigation Tree pane, expand Administrative Services → Data Sources → TPC Servers.
- In the right pane, double-click a server row or click the icon next to a server to edit information about that server. Information about a subordinate server will appear on Administrative Services → Data Sources → TPC Servers → TPC Server Details.
- **3**. Edit the information in the following fields:

## Host Authentication Password

Enter the password for the subordinate IBM Tivoli Storage Productivity Center server.

### **Display Name (optional)**

Enter a name for the subordinate server.

### **Description (optional)**

Enter a description for the subordinate server.

## Test TPC Server Connectivity before adding

Select this check box to have the master server connect and log into the subordinate server using the information provided on this window. This test is performed when you click **Save**.

 Select File → Save . If successful, the TPC Servers window appears and any new values for Display Name and Description are shown for a subordinate server.

## **Rollup reports - fragmentation**

Fragmentation occurs when related storage entities are being monitored by different subordinate IBM Tivoli Storage Productivity Center servers.

The following example shows when fragmentation can occur using subordinate servers and rollup reports:

• **Example:** Host A is assigned a volume from storage subsystem 1. Host A is being monitored only by one Tivoli Storage Productivity Center subordinate server (Server 1) and storage subsystem 1 is being monitored by another subordinate server (Server 2). Server 1 and Server 2 are subordinate servers to the master server (Server 3).

**Reason for fragmentation:** In this example, the host and subsystem are fragmented because they are not being monitored by the same Tivoli Storage Productivity Center server. This will cause the **Correlated Volume Space** value in the rollup reports for storage subsystems and volumes to be incorrect.

To prevent fragmentation when using master and subordinate server relationships to generate rollup reports, we recommend the following:

- Do not monitor a storage subsystem and the hosts to which its volumes are assigned with different subordinate servers that are associated with the same master server.
- Do not monitor a fabric and its related switches with different subordinate servers that are associated with the same master server.
- If an agent machine is using storage from a subsystem, then both the agent and subsystem should be monitored by the same subordinate server.
- Configure all the subordinate servers to discover all the storage subsystems within your environment. Note that if a subordinate server is monitoring a subsystem with an agent other than the agent that is using storage on that subsystem, the value for the **Correlated Volume Space** column in rollup reports will be incorrect. For example:
  - Host A has storage from Subsystem 1
  - Subordinate server B is Monitoring Host A and Subsystem 1
  - Subordinate server C is Monitoring Subsystem 1 and probed the subsystem more recently than server B.
  - The master server is monitoring subordinate servers B and server C.

The master server will report the storage subsystem data from server C. Because the master server does not know about Host A, the value for the **Correlated Volume Space** column will be incorrect.

## VMware data source

VMware Virtual Infrastructure data sources are used by IBM Tivoli Storage Productivity Center to collect information from the hypervisors and virtual machines within them.

When you add a VMware data source in IBM Tivoli Storage Productivity Center, you need a user ID that has permission to browse through the data stores on VMware. IBM Tivoli Storage Productivity Center needs to browse through the data stores to collect information from the ESX Servers. However the "Read Only" role as defined by VMware does not allow IBM Tivoli Storage Productivity Center to browse the data stores. You can use the "Virtual Machine Power User" role as a choice if you do not want to use the Administrator role, or you can create a custom role with the required permissions.

To check what user role you have for VMware, follow these steps:

- 1. Connect a VI client to the ESX Server or VirtualCenter (whichever is used as the data source). Click on the ESX Server and go to the **Summary** tab. Select a data source, right-click on the data source and select **Browse**, to confirm that the browse permission is working correctly.
- 2. Connect the VI client to the data source with the admin role, go to the **Permission** tab and determine if the role name is used for the user.
- **3**. Open the **Permissions** view, select that role, then right-click and select the **Edit** role. See what permissions are checked. Expand the check groups to find the specific ones.

For more information about VMware user roles, see http://www.vmware.com/pdf/vi3\_vc\_roles.pdf.

## Adding a VMware VI Data Source

This topic provides information about adding a VMware Virtual Infrastructure data source.

To add a VMware VI data source, follow this procedure:

- 1. In the Navigation Tree pane, expand Administrative Services → Data Sources → VMware VI Data Source.
- 2. In the right pane, click Add VMware VI Data Source.
- 3. In the Add VMware VI Data Source window, enter the following information:

### Host Name

The host name for the VMware data source (ESX Server or VirtualCenter).

## Protocol

This is http or https. If you use https, you must have first imported the SSL certificate into IBM Tivoli Storage Productivity Center. For information about how to import the SSL certificate, see "Importing SSL certificates for VMware" on page 489. The protocol must match the same protocol that is set for the ESX Server or VirtualCenter.

**Port** The port used by the VMware data source.

## Username

The user name for the VMware data source.

## Password

The password for the VMware data source.

## **Password Confirm**

The password is confirmed for the VMware data source.

## **Display** Name

The name displayed in reports for the VMware data source.

### Description

The description for the VMware data source.

## Test VMware VI Data Source connectivity before adding

Check this box to check the connectivity for the VMware data source.

4. Click Save.

## Updating VMware data source information

After a VMware data source has been added, you can update the administrator name or password for the VMware data source.

To update information for a VMware data source, follow this procedure:

- 1. In the Navigation Tree pane, expand Administrative Services → Data Sources → VMware VI Data Source.
- 2. In the right pane, click on the icon to the left of the VMware data source you wish to change.
- 3. In the right pane, a notebook window opens. Make the appropriate changes.

## Displaying information about a VMware data source

You can view information about a VMware data source including its host name, protocol, port, and type.

To display information about an out-of-band agent, follow this procedure:

- 1. In the Navigation Tree pane, expand Administrative Services → Data Sources → VMware VI Data Source.
- 2. In the right pane, click on the icon to the left of the VMware data source for which you want information for. In the right pane, a notebook window opens. The following information is displayed:

#### Host Name

The IP address of the data source.

#### Protocol

This is http or https.

**Port** The port used by the VMware data source.

Type Virtual Center.

#### Administrator Name

The name of the administrator for the VMware data source.

#### Password

The password for the VMware data source.

#### Password Confirm

Confirm the password for the VMware data source.

#### Display Name

The name displayed for the VMware data source.

#### Description

Description for the VMware data source.

#### Software Level

The software level for the VMware data source.

### ConnectionStatus

The connection status to the VMware data source.

#### **Status Timestamp**

## Test VMware VI Data Source connectivity before updating Check this box to check the connectivity to the VMware data source.

#### Show managed devices for VMware

You can view information about the managed devices for VMware.

To show the managed devices for VMware, follow this procedure:

- 1. In the Navigation Tree pane, expand Administrative Services → Data Sources → VMware VI Data Source.
- 2. In the right pane, click Show Managed Devices.
- **3.** A pop-up window displays the VMware managed devices. Click **OK** to close the window.

## Deleting a VMware VI Data Source

This topic provides information about deleting a VMware Virtual Infrastructure data source.

To delete a VMware VI data source, follow this procedure:

- 1. In the Navigation Tree pane, expand Administrative Services → Data Sources → VMware VI Data Source.
- 2. In the right pane, click Remove VMware VI Data Source.

3. In the confirmation dialog window to remove a VMware data source, click OK.

## Administering agents on the Virtual I/O Server

Use the **startsvc** and **stopsvc** commands to start and stop the agents on the Virtual I/O Server. Use the **lssvc** command to list the agents installed on the Virtual I/O Server.

## Listing agents on Virtual I/O Server

Use the **lssvc** command to list the IBM Tivoli Storage Productivity Center agents on a Virtual I/O Server.

You must log into the Virtual I/O Server as the **padmin** user ID to use this command.

The syntax for the lssvc command is:

► — 1 ssvc — TPC —-

The **lssvc** command lists all the available agents that are managed by the Virtual I/O Server. If an agent name is passed to the **lssvc** command, then a listing of the attributes with their configured values are displayed.

### Examples

To list all the agents installed, enter the following command: lssvc TPC

## Starting IBM Tivoli Storage Productivity Center agents

Use the **startsvc** command to start Tivoli Storage Productivity Center agents on a Virtual I/O Server.

You must log into a Virtual I/O Server as the **padmin** user ID to use the **startsvc** command.

The parameters for the command are:

►►—startsvc—agent\_name—

The **startsvc** command starts the specified agent. The agent name is case sensitive. For repeated execution, you typically receive a message that the agent has already been started.

The *agent\_name* can be:

TPC\_data

Starts the Data agent.

**TPC\_fabric** Starts the Fabric agent.

**Note:** The agent name is case sensitive.

Examples

To start the Data agent, enter the following command: startsvc TPC\_data

To start the Fabric agent, enter the following command: startsvc TPC\_fabric

## Stopping IBM Tivoli Storage Productivity Center agents

Use the **stopsvc** command to stop Tivoli Storage Productivity Center agents on the Virtual I/O Server.

You must log into a Virtual I/O Server as the **padmin** user ID to use this command.

The parameters for the **stopsvc** command are:

►►—stopsvc—agent\_name—

The *agent\_name* can be:

TPC\_data

Stops the Data agent.

TPC\_fabric

Stops the Fabric agent.

Note: The agent name is case sensitive.

Examples

To stop the Data agent, enter the following command: stopsvc TPC\_data

To stop the Fabric agent, enter the following command: stopsvc TPC fabric

# Adding a IBM Tivoli Storage Productivity Center user group name to IBM Tivoli Storage Productivity Center for Replication

To access IBM Tivoli Storage Productivity Center for Replication using a user ID from the IBM Tivoli Storage Productivity Center user group name, you must add the user group name to the IBM Tivoli Storage Productivity Center for Replication administrative role. If you installed IBM Tivoli Storage Productivity Center with LDAP authentication, you do not have to perform these steps.

Follow these steps:

- 1. Log in to IBM Tivoli Storage Productivity Center as the Superuser.
- Expand Administrative Services > Configuration. Left-click Role-to-Group Mappings. Locate the user group name that has the user ID you want for logging in to IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication.
- 3. Add the user group name to IBM Tivoli Storage Productivity Center for Replication Administrator role by using the Add Access wizard. Open IBM Tivoli Storage Productivity Center for Replication using a IBM Tivoli Storage Productivity Center for Replication Administrator user ID.

- 4. Click Add Access on the Administration page.
- **5**. Add the user group name to IBM Tivoli Storage Productivity Center for Replication and complete the wizard.

# Accessing the IBM Tivoli Storage Productivity Center for Replication GUI

After IBM Tivoli Storage Productivity Center for Replication has been installed, you can access the IBM Tivoli Storage Productivity Center for Replication GUI.

If you are running IBM Tivoli Storage Productivity Center for Replication on AIX, Linux, or Windows, be sure you use IBM Tivoli Storage Productivity Center Standard Edition Version 4.1 to install IBM Tivoli Integrated Portal and IBM Tivoli Storage Productivity Center for Replication Version 4.1.

Go to the following URL to access the IBM Tivoli Storage Productivity Center for Replication GUI (the Web address is case-sensitive): https://<HostName>:<port>/CSM

## Note:

- The default port is 3443 for open systems and 9443 for z/OS<sup>®</sup>. For information about z/OS, see *IBM Tivoli Storage Productivity Center for Replication for System z<sup>®</sup> v4.1 Installation and Configuration Guide.*
- **2.** If you modified the default port settings during the installation, replace *3443* with the port number you selected for the https port.
- **3.** If you are using IBM System Services Runtime Environment for z/OS, the default port is 32200.
- 4. If you are using IBM Tivoli Storage Productivity Center for Replication version 3.3 or earlier, the default port for open system is 9443.

Use the CLI user ID and password that you entered during the installation of IBM Tivoli Storage Productivity Center for Replication to log in. This ID and password are the same as the Administrator ID and password that you entered in you installed the product.

# Backing up and recovering IBM Tivoli Storage Productivity Center for Replication

There are two backup methods for IBM Tivoli Storage Productivity Center for Replication. This section provides information about these methods.

The backup methods are:

- The first backup option is to use IBM Tivoli Storage Productivity Center for Replication's import and export function to save the configuration of each IBM Tivoli Storage Productivity Center for Replication session. You would export a IBM Tivoli Storage Productivity Center for Replication session to a CSV file. The CSV file can then be used to recover a IBM Tivoli Storage Productivity Center for Replication session.
- The second backup option is to use IBM Tivoli Storage Productivity Center for Replication's high availability function. This option allows IBM Tivoli Storage Productivity Center for Replication to have a real time backup server that can take over in the event of a disaster.

For information about the high availability function and configuring sessions and copy sets, go to the Information Center at http://publib.boulder.ibm.com/ infocenter/tivihelp/v4r1/index.jsp.

## Starting and stopping the IBM Tivoli Storage Productivity Center services

This section provides information on how to start and stop the IBM Tivoli Storage Productivity Center services.

## Stopping the IBM Tivoli Storage Productivity Center services

This topic describes how to stop the IBM Tivoli Storage Productivity Center services.

To stop the services on Windows, go to **Start > Control Panel > Administrative Tools > Services**. Stop the following services:

```
IBM WebSphere Application Server V6.1 - DeviceServer
IBM Tivoli Storage Productivity Center - Data Server
IBM Tivoli Common Agent <directory>
  (Directory is where the common agent is installed.
    The default is: c:\Program Files\IBM\TPC\ca.)
IBM Storage Resource Agent - <directory>
  (<directory> is where the Storage Resource agent is installed.
    The default is: c:\Program Files\IBM\TPC\agent.)
IBM WebSphere Application Server V6.1 - CSM
Tivoli Integrated Portal - TIPProfile_Port_<xxxxx>
  (<xxxxx> indicates the port specified during installation
    The default port is 16310.)
IBM ADE Service (Tivoli Integrated Portal registry)
```

**Note:** Tivoli Common Agent Services stops the Common agent and any Data agent or Fabric agent running under it.

To stop the services on Linux:

```
Data server:
   /<TPC_install_directory>/data/server/tpcdsrv1 stop
Device server:
  /<TPC install directory>/device/bin/linux/stopTPCF.sh
Common agent:
   /<common agent install directory>/ca/endpoint.sh stop
Storage Resource agent:
  /<SRA install directory>/agent/bin/agent.sh stop
IBM WebSphere Application Server V6.1 - CSM:
   /<usr or opt>/IBM/replication/eWAS/profiles/CSM/bin/stopServer.sh server1
    -username <username> -password <passsword>
       (where <username> represents the ID of the TPC superuser and
       <password> represents the password for that user)
Tivoli Integrated Portal:
   <install directory>\tip\profiles\TIPProfile\bin\stopServer server1
   -username <tipadmin> -password <mypassword>
      (where <tipadmin> is the administrator user ID and <password> is the
      administrator password.)
IBM ADE Service:
  Source the environment:
      . /var/ibm/common/acsi/setenv.sh
   Run this command:
      /usr/ibm/common/acsi/bin/acsisrv.sh stop
         (wait for operation to complete)
```

**Note:** The <TPC\_install\_directory>, <common\_agent\_install\_directory>, and <SRA\_install\_directory> default directory is: /opt/IBM/TPC.

```
To stop the services on AIX:
Data server:
  stopsrc -s TSRMsrv1
Device server:
  /<TPC install directory>/device/bin/aix/stopTPCF.sh
Common agent:
   /<common agent install directory>/ca/endpoint.sh stop
Storage Resource agent:
   /<SRA_install_directory>/agent/bin/agent.sh stop
IBM WebSphere Application Server V6.1 - CSM:
   /<usr or opt>/IBM/replication/eWAS/profiles/CSM/bin/stopServer.sh server1
   -username <username> -password <passsword>
      (where <username> represents the ID of the TPC superuser and
     <password> represents the password for that user)
Tivoli Integrated Portal:
   <install directory>\tip\profiles\TIPProfile\bin\stopServer server1
   -username <tipadmin> -password <mypassword>
      (where <tipadmin> is the administrator user ID and <password> is the
     administrator password)
IBM ADE Service:
  Source the environment:
     . /var/ibm/common/acsi/setenv.sh
   Run this command:
     /usr/ibm/common/acsi/bin/acsisrv.sh stop
         (wait for operation to complete)
```

**Note:** The <TPC\_install\_directory>, <common\_agent\_install\_directory>, and <SRA\_install\_directory> default directory is: /opt/IBM/TPC.

## Starting the IBM Tivoli Storage Productivity Center services

This topic describes how to start the IBM Tivoli Storage Productivity Center services.

To start the services on Windows, go to **Start > Control Panel > Administrative Tools > Services**. Start the following services:

```
IBM WebSphere Application Server V6.1 - DeviceServer
IBM Tivoli Storage Productivity Center - Data Server
IBM Tivoli Common Agent - <directory>
    (<directory> is where the common agent is installed.
    The default is: c:\Program Files\IBM\TPC\ca.)
IBM Storage Resource Agent - <directory>
    (<directory> is where the Storage Resource agent is installed.
    The default is: c:\Program Files\IBM\TPC\agent.)
IBM WebSphere Application Server V6.1 - CSM
Tivoli Integrated Portal - TIPProfile_Port_<xxxxx>
    (<xxxxx> indicates the port specified during installation
    The default port is 16310.)
IBM ADE Service (Tivoli Integrated Portal registry)
```

**Note:** Tivoli Common Agent Services starts the Common agent and any Data agent or Fabric agent running under it.

To start the services on Linux:

```
Data server:
    /<TPC_install_directory>/data/server/tpcdsrv1 start
Device server:
    /<TPC_install_directory>/device/bin/linux/startTPCF.sh
Common agent:
    /<common_agent_install_directory>/ca/endpoint.sh start
Storage Resource agent:
    /<SRA_install_directory>/agent/bin/agent.sh start
IBM WebSphere Application Server V6.1 - CSM:
```

```
/<usr or opt>/IBM/replication/eWAS/profiles/CSM/bin/startServer.sh server1
-username <username> -password <passsword>
  (where <username> represents the ID of the TPC superuser and
  <password> represents the password for that user)
Tivoli Integrated Portal:
  <install_directory>\tip\profiles\TIPProfile\bin\startServer server1
-username <tipadmin> -password <mypassword>
  (where <tipadmin> is the administrator user ID and <password> is the
  administrator password.)
IBM ADE Service:
  Source the environment:
    . /var/ibm/common/acsi/setenv.sh
  Run this command:
    /usr/ibm/common/acsi/bin/acsisrv.sh start
```

**Note:** The <TPC\_install\_directory>, <common\_agent\_install\_directory>, and <SRA\_install\_directory> default directory is: /opt/IBM/TPC.

To start the services on AIX: Data server: startsrc -s TSRMsrv1 Device server: /<TPC\_install\_directory>/device/bin/aix/startTPCF.sh Common agent: /<common agent install directory>/ca/endpoint.sh start Storage Resource agent: /<SRA\_install\_directory>/agent/bin/agent.sh start IBM WebSphere Application Server V6.1 - CSM: /<usr or opt>/IBM/replication/eWAS/profiles/CSM/bin/startServer.sh server1 -username <username> -password <passsword> (where <username> represents the ID of the TPC superuser and <password> represents the password for that user) Tivoli Integrated Portal: <install directory>\tip\profiles\TIPProfile\bin\startServer server1 -username <tipadmin> -password <mypassword> (where <tipadmin> is the administrator user ID and <password> is the administrator password.) IBM ADE Service: Source the environment: . /var/ibm/common/acsi/setenv.sh Run this command: /usr/ibm/common/acsi/bin/acsisrv.sh start

**Note:** The <TPC\_install\_directory>, <common\_agent\_install\_directory>, and <SRA\_install\_directory> default directory is: /opt/IBM/TPC.

## Starting and stopping the IBM Tivoli Integrated Portal server

The IBM Tivoli Integrated Portal server starts automatically after it has been installed and whenever the computer is started. You can manually stop the server before beginning certain configuration tasks or as needed.

Perform the following steps at the command prompt:

- 1. Change to the <install\_dir>\tip\profiles\TIPProfile\bin\ directory.
- 2. To stop the server, enter the following command:

```
stopServer server1 -username <tipadmin>
-password <mypassword>
```

Where *<tipadmin>* is the administrator user ID and *<mypassword>* is the administrator password. Wait for the server to complete the operation.

 To start the server, enter the following command: startServer server1 -username <tipadmin> -password <mypassword>

Where *<tipadmin>* is the administrator user ID and *<mypassword>* is the administrator password. Wait for the server to complete the operation.

## Starting and stopping the Tivoli Storage Productivity Center GUI

This topic describes how to start and stop the IBM Tivoli Storage Productivity Center graphical user interface (GUI).

## Starting the Tivoli Storage Productivity Center GUI

Learn how to start the IBM Tivoli Storage Productivity Center graphical user interface (GUI) from one of the following locations: the Microsoft Windows Start menu, IBM Tivoli Integrated Portal, the Productivity Center icon on your desktop (Windows), or the command line (AIX, UNIX, or Linux).

## Starting the Tivoli Storage Productivity Center GUI from Tivoli Integrated Portal

This section describes how to start the Tivoli Storage Productivity Center graphical user interface (GUI) from Tivoli Integrated Portal. With the new single sign-on feature, you can log on to the Tivoli Storage Productivity Center GUI without having to explicitly enter your username and password.

Before you start Tivoli Integrated Portal and Tivoli Storage Productivity Center, ensure that you are using one of the following Web browsers:

- AIX: Firefox 2.0
- Linux and UNIX: Firefox 2.0
- Windows: Internet Explorer 7, Firefox 2.0, Firefox 3.0

Ensure that a fully qualified domain name is defined for the Tivoli Storage Productivity Center server. To verify the Tivoli Storage Productivity Center server name and modify the name if required, see "Data server and Device server are inaccessible from Tivoli Integrated Portal" on page 590. Contact your Tivoli Storage Productivity Center administrator before you modify the file.

To start Tivoli Storage Productivity Center from Tivoli Integrated Portal, complete the following steps.

1. Start an Internet Explorer or Firefox Web browser, and type the following information in the address bar:

http://hostname:port

Where *hostname* defines the server that is running Tivoli Integrated Portal such as the server name or IP address and *port* defines the port number for Tivoli Integrated Portal. If the default port was accepted during the installation of Tivoli Integrated Portal, the port number is 16310. Contact your Tivoli Storage Productivity Center administrator if you need to verify the host name and port number.

- 2. On the Tivoli Integrated Portal logon page, log on using the appropriate user ID and password. Your user ID must have administrator permissions.
- 3. In the Tivoli Integrated Portal navigation tree, click **Tivoli Storage Productivity Center**.

- 4. On the Tivoli Storage Productivity Center portlets page, click **Start Storage Productivity Center**. One of the following actions occur:
  - If single sign-on is successful, Tivoli Storage Productivity Center starts without displaying the logon window.
  - If single sign-on is not successful, an error message and the Tivoli Storage Productivity Center logon window are displayed.
  - If the Tivoli Storage Productivity Center Data server or Device server is not accessible, an error message is displayed. The status of both the Data server and the Device server also display.
  - If the status of the Device server and Data server is inaccessible and you started Tivoli Integrated Portal from a remote computer, it is possible that a fully qualified domain name was not defined for the Tivoli Storage Productivity Center server during installation. To check the Tivoli Storage Productivity Center server name and modify the name if required, see the Tivoli Storage Productivity Center troubleshooting documentation.
  - If you are using a Lightweight Directory Access Protocol (LDAP) compliant directory for Tivoli Storage Productivity Center user authentication and the directory is not available, an error message is displayed.

Once you have logged on to Tivoli Integrated Portal, a Lightweight Third-Party Authentication (LTPA) token is created. This token is passed to other applications that you start from Tivoli Integrated Portal for single sign-on authentication purposes.

During the period between when you log on to Tivoli Integrated Portal and when you start another application such as Tivoli Storage Productivity Center from Tivoli Integrated Portal, the following conditions might occur:

- The user password that was used to log on to Tivoli Integrated Portal is changed in the user repository.
- The user ID that was used to access Tivoli Integrated Portal is changed in the repository or removed from the user repository.
- The user repository is not accessible.

Under the first condition, the original user credentials that were used to access Tivoli Integrated Portal are used to access other applications until the timeout period for the LTPA token that is used for single sign-on expires. When the LTPA token expires, you are prompted to re-enter your user ID and password when you attempt to start another application using single sign-on.

Under the second and third conditions, the single sign-on feature does not work. You are always prompted to re-enter your user ID and password when you attempt to start another application.

## Starting the Tivoli Storage Productivity Center GUI as a stand-alone application

This section describes how to start the IBM Tivoli Storage Productivity Center from the Microsoft Windows Start menu, or the Productivity Center icon on your desktop (Windows), or from the command line (AIX, UNIX, or Linux).

To start the Tivoli Storage Productivity Center graphical user interface (GUI) on Windows, click **Start** → **Programs** → **IBM Tivoli Storage Productivity Center** → **Productivity Center**. You can also double-click the IBM Tivoli Storage Productivity Center icon if it is installed on your desktop. To start the Tivoli Storage Productivity Center GUI on UNIX or Linux, type the following path and command at the command line: /opt/IBM/TPC/gui/TPCD.sh

To start the Tivoli Storage Productivity Center GUI on AIX, type the following path and command at the command line: /opt/IBM/TPC/gui/TPCD.sh

## Logging on to Tivoli Storage Productivity Center

Use the logon window to specify the user ID and password that you want to use to log on to a IBM Tivoli Storage Productivity Center server.

Define logon information for Tivoli Storage Productivity Center in the following fields:

## User ID

Enter the user ID that you want to use to log on to Tivoli Storage Productivity Center. The roles that are assigned to that user ID determine what nodes in the navigation tree you can see and act upon.

## Password

Enter the password that is associated with the User ID.

**Server** Enter the IP address or Domain Name System (DNS) name of the computer on which the Tivoli Storage Productivity Center server is installed.

When you enter an IP address, you can use either an IPv4 or IPv6 address format depending on the protocol enabled on the computer. For example, enter an IPv6 address for an IPv6-only computer. Enter an IPv4 or IPv6 address for a computer with dual stacks (both IPv4 and IPv6 enabled).

- To enter an IPv4 address, use the dotted decimal format: *nnn.nnn.nnn*. For example: 127.0.0.1.
- When entering an IPv6 address you must include brackets [] to separate those addresses from their port numbers when you enter a value in this field. For example: [2001:DB8::1234:0000:0000:5678:ABCD]:9550. Use one of the following methods to enter an IPv6 address:
  - The preferred IPv6 address representation is written as eight groups of four hexadecimal digits: xxx:xxx:xxx:xxx:xxx:xxx:xxxx:xxxx; where each x is a hexadecimal digit representing 4 bits. For example: 2001:DB8:0000:1234:0000:0000:5678:ABCD
  - You can specify an IPv6 address using a shortened format that omits leading zeros: (2001:DB8:0:1234:0:0:5678:ABCD)
  - You can use double colons in place of a series of zeros: (2001:DB8:0000:1234::5678:ABCD)

## Setting up a user role and collecting system statistics

If you are logging on to the Tivoli Storage Productivity Center graphical user interface (GUI) for the first time after installing the product, note the following information:

• If you did not set up a Tivoli Storage Productivity Center user role, you might not be able to log on. To set up a Tivoli Storage Productivity Center user role, log on as the superuser and create the roles as described in "Planning for IBM Tivoli Storage Productivity Center authorization" on page 18. • After you log on, you will see a panel that prompts you to collect system statistics. Click **Yes**.

## Single sign-on

Tivoli Storage Productivity Center can use the single sign-on feature, which enables you to start Tivoli Storage Productivity Center from either the Tivoli Integrated Portal V1.1.1.0 instance that is installed with Tivoli Storage Productivity Center or from an existing Tivoli Integrated Portal V1.1.1.0 instance. If you have a single sign-on environment configured and Tivoli Integrated Portal user authentication is successful, the Tivoli Storage Productivity Center logon window does not open when you start the Tivoli Storage Productivity Center GUI from Tivoli Integrated Portal.

### User credential considerations for single sign-on

When you log on to either Tivoli Integrated Portal or Tivoli Storage Productivity Center, a Lightweight Third-Party Authentication (LTPA) token is created and used for single sign-on authentication when you start other applications from within the Tivoli Storage Productivity Center GUI.

During the period between when you log on to Tivoli Storage Productivity Center and when you start other applications, such as element managers, from the Tivoli Storage Productivity Center GUI, the following conditions might occur:

The user password that was used to log on to Tivoli Integrated Portal or Tivoli Storage Productivity Center is changed in the user repository.	Under this condition, the original user credentials that were used to log into Tivoli Integrated Portal or Tivoli Storage Productivity Center are used to access other applications until the timeout period for the LTPA token that is used for single sign-on expires. When the LTPA token expires, you are prompted to reenter your user ID and password when you attempt to start another application using single sign-on.
The user ID that was used to access Tivoli Integrated Portal is changed in the repository or removed from the user repository. The user repository is not accessible.	Under the second and third conditions, the single sign-on feature does not work. You are always prompted to reenter your user ID and password when you attempt to start another application through single sign-on.

## Stopping the Tivoli Storage Productivity Center GUI

This section describes how to stop the IBM Tivoli Storage Productivity Center graphical user interface (GUI).

To stop the Tivoli Storage Productivity Center user interface, click File → Exit.

## Checking IBM Tivoli Storage Productivity Center status

This section provides information on checking the status of Tivoli Storage Productivity Center.

## **Related tasks**

"Checking the health of your agents" on page 430 This topic provides information about checking the health of your agents.

## Checking the IBM Tivoli Storage Productivity Center version

This section describes how to check the version of IBM Tivoli Storage Productivity Center that is installed on your system.

To check the version of Tivoli Storage Productivity Center you have installed, go to the following directory:

Windows: C:\Program Files\IBM\TPC UNIX or Linux: <usr or opt>/IBM/TPC

This directory contains the version.txt file which displays the version of Tivoli Storage Productivity Center you have installed.

This is an example of the information in version.txt: TPC V3.3.2 Build TPC\_3.3.2.56 20080403

## Checking the status of the Data Server

This topic describes how to check the status of the Data server.

To check the status of the Data Server, complete the following steps:

- 1. Open the IBM Tivoli Storage Productivity Center graphical user interface (GUI).
- 2. In the left pane, click Administrative Services → Services → Data Server. A status icon is displayed to the left of each service.

## Checking the status of the Device server

This topic describes how to check the status of the Device server.

To check the status of the Device server, complete the following steps:

- 1. Open the IBM Tivoli Storage Productivity Center graphical user interface (GUI).
- 2. In the left pane, click **Administrative Services** → **Services** → **Device server**. A status icon is displayed to the left of each service.

## Checking the status of agents

This topic describes how to check the status of the agents.

In the Navigation Tree on the left, go to **Administrative Services**  $\rightarrow$  **Data Sources**. Click on one of the following nodes:

- CIMOM Agents
- Data/Storage Resource Agents
- Inband Fabric Agents
- Out of Band Fabric Agents

In the right pane, a list of agents is displayed. If the agents are up and running, there will be a green health status icon in the State column. For CIMOM Agents, there will be a green health status icon in the Connection Status column.

If the status icon is red, you can view the log by selecting an agent and click **View Log** for Data, Native, and Inband Fabric. This will display the log in the right pane. If the reason that an agent is down is a connectivity problem, you might not

be able to get the log files. A given discovered CIMOM will appear as a red (critical) icon status until you enter valid credentials.

## Increasing memory allocation

If you run out of memory for the Data server, Device server, or agent, you might want to increase the memory allocated for these components. This section describes how to increase the memory allocated for these components on systems running AIX, Linux, and Windows.

## Increasing the memory allocation for the Data server

If you run out of memory for the Data server, you might want to increase the memory allocated for the Data server. This section describes how to increase the memory allocated for the Data server on systems running AIX, Linux, and Windows.

## Increasing the memory allocation for the Data server running on AIX

This section describes how to increase the memory allocation for the Data server running on AIX.

To increase the memory allocated for the Data server running on AIX, complete the following steps:

- 1. Log in as a user with root authority.
- To stop the Data server, run the following command: /opt/IBM/TPC/data/server/stopsrc -s TSRMsrv1
- **3**. Run the following command:

odmget -qsubsysname=TSRMsrv1 SRCsubsys

Output similar to the following is returned:

```
SRCsubsys:
        subsysname = "TSRMsrv2"
        synonym = ""
        cmdargs = "-Xmx256m CLASSPATH=/usr/ibm/TPC/Data/
           cloudscape/db2j.jar:
           /usr/ibm/TPC/Data/cloudscape/db2jtools.jar LC_ALL=en_US"
        path = "/usr/ibm/TPC/Data/server/bin/aix power/TSRMssys"
        uid = 0
        auditid = 0
        standin = "/dev/console"
        standout = "/dev/console"
        standerr = "/dev/console"
        action = 2
        multi = 0
        contact = 3
        svrkey = 0
        svrmtype = 0
        priority = 20
        signorm = 0
        sigforce = 0
        display = 1
        waittime = 20
        grpname = ""
```

- 4. Copy the entire string (excluding the quotation marks) that follows the **cmdargs** parameter.
- 5. Run the following command:

```
chssys -s TSRMsrv2 -a '<modified cmdargs>'
```

where <modified\_cmdargs> is a modification of the string that you copied in step 4 on page 472. For example, to increase the memory from 256 to 512 MB, change -Xmx256m to -Xmx512m.

- 6. Save the modified file.
- 7. Restart the Data server.

## Increasing the memory allocation for the Data server running on UNIX or Linux

This section describes how to increase the memory allocation for the Data server running on Linux.

To increase the memory allocated for the Data server running on HP-UX, Linux, or Sun Solaris, complete the following steps:

- 1. Log in as a user with root authority.
- 2. To stop the Data Server, from the command prompt, run the following command:

/opt/IBM/TPC/data/server/tpcdsrv1 stop

- 3. Using a text editor, open the **tpcdsrv1** file.
- 4. Locate the following line:

```
exec $JAVAEXE -Xrs -Xmx<XXXm> -cp $CLASSPATH com.tivoli.itsrm.server.Server &
```

where  $\langle XXXm \rangle$  is the memory allocated for the Data server. By default, this is 256m (256 MB).

- 5. Increase the memory allocated for the Data server. For example, to increase the memory to 512 MB, change the line to read as follows:
- exec \$JAVAEXE -Xrs -Xmx512m -cp \$CLASSPATH com.tivoli.itsrm.server.Server &
- 6. Save the modified **tpcdsrv1** file.
- To restart the Data server, run the following command: /opt/IBM/TPC/data/server/tpcdsrv1 start

## Increasing memory allocation for Data server running on Windows

This section describes how to increase the memory allocation for the Data server running on Windows.

To increase the amount of memory available to the server, complete the following steps:

- 1. Select **Start**  $\rightarrow$  **Run**. The Run window is displayed.
- 2. Type **regedit** in the Open: field and click **OK**. The Registry Editor window is displayed.
- 3. Expand the HKEY\_LOCAL\_MACHINE → SOFTWARE → IBM → TSRM folder on the left side of the Registry Editor window.
- 4. Right-click the 1 folder and select **New** → **String Value** from the pop-up menu.
- 5. Type **SRVJPARMS** as the name of the string.
- 6. Right-click the name of the string and select Modify from the pop-up menu.
- 7. Enter -Xmx<###>m in the Value data field, where ### represents the number of megabytes for the server's maximum heap size. The default size is 256. Click OK. The largest possible value for the maximum heap size is 1536 megabytes. If the value is set to something larger than 1536, that value will be ignored and 1536 megabytes will be used as the maximum heap size.

- **8**. Stop and restart the server to have the changes take effect. To stop the server, complete the following steps:
  - a. Go to **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Services**. The Services window is displayed.
  - b. Right-click on **IBM Tivoli Storage Productivity Center Data Server** service and click **Stop** from the pop-up menu. To restart the server, complete the following steps:
    - Go to Start → Settings → Control Panel → Administrative Tools → Services. The Services window is displayed.
    - 2) Right-click on **Tivoli Storage Productivity Center Data Server** service and click **Start** from the pop-up menu.

## Increasing the memory allocation for the Device server

This topic describes how to increase the memory allocated for the Device server.

- 1. Stop the Device server.
- 2. Open the server.xml file in a text editor. This file is located at <directory>\device\apps\was\profiles\deviceServer\config\cells\ DefaultNode\nodes\DefaultNode\servers\server1, where <directory> is the directory where IBM Tivoli Storage Productivity Center is installed.
- 3. Search for JVMArguments, and change the value of the -Xmx512m parameter.
- 4. Save the modified server.xml file.
- 5. Restart the Device server.

## Increasing the memory allocation for an agent

This topic describes how to increase the memory allocated for a Data agent or an in-band Fabric agent.

To increase the memory allocated for an agent, complete the following steps:

- 1. Stop the agent.
- Using a text editor, open the nonstop.properties file. This file is at <directory>/config/nonstop.properties

where <directory> is the directory where the agent is installed.

3. Prepend the following text to the beginning of the **parameter** property: -Xmx512m

The property should read as follows:

```
parameter="-Xmx512m -cp :lib/smf.jar:lib/SMFCoreMsg_en.jar:lib/
ep_system.jar -Dcom.tivoli.agent.nonstop.launcher=true
-Dcom.ibm.osg.smf.bundledir=installedBundles -Djlog.noLogCmd=true
com.tivoli.agent.system.SMFLauncher"
```

- 4. Save the modified **nonstop.properties** file.
- 5. Restart the agent.

## Displaying information about a Device server service

You can view service information including start time, version, and status.

To display information about a service, follow this procedure:

1. In the Navigation Tree pane, expand **Administrative Services** → **Services** → **Device server**.

2. Click the name of the service.

## Viewing a Device server log

You can use the content of the log file to troubleshoot any errors that might occur during startup, processing or shut down. Service alerts, if any, are displayed in red.

To display the log of a service, follow this procedure:

- 1. In the Navigation Tree pane, expand Administrative Services → Services → Device server.
- 2. Right-click the name of the service and select View Log.

## Changing passwords

This section provides information about changing passwords.

If you installed IBM Tivoli Storage Productivity Center using the typical installation and used the same DB2 user ID and password for the items IBM Tivoli Storage Productivity Center requires, then when you change the DB2 password, you must also change the passwords for the items that the DB2 password applies to. For example, the DB2 administrative password might also apply to the following items:

- Database administration user ID and password (for the Data Server or Device server to connect to the database)
- Database user ID and password to create the database schema
- Host authentication password (for the Fabric agents to communicate with the Device server)
- Common agent service login user ID and password (for Windows only, if this user ID does not exist)
- WebSphere administration user ID and password (for the Device server to communicate with embedded WebSphere if the user ID does not exist). This is the case only if you select OS authentication during the IBM Tivoli Storage Productivity Center installation. If you chose LDAP authentication, then the WebSphere administration user ID and password are set to the LDAP TPC Administrator username and password.

## Changing the DB2 user password for the Device server

This section provides information about changing the DB2 user password for the Device server.

If you change the DB2 user password, follow these steps to change it for the Device server:

 Go the <TPC\_install\_dir>\cli directory and run the following command: tpctool encrypt <password>

This encrypts the password.

 Copy the encrypted password to the following file: <TPC\_install\_dir>\device\conf\tsnmdbparms.properties

Replace this password:

tivoli.sanmgmt.jdbc.dbPassword=<encrypted\_password>

**3**. Restart the Device server.

4. If you performed a typical installation and selected OS authentication, then this DB2 user ID is also the WebSphere administrative user ID. You must also change the WebSphere administrative user password. See "Changing the WebSphere administrative user password for the Device server."

# Changing the WebSphere administrative user password for the Device server

This topic describes how to change the WebSphere administrative user password for the Device server.

**Note:** If you selected LDAP authentication during IBM Tivoli Storage Productivity Center installation, then the WebSphere administrative ID and password are set to the LDAP TPC Administrator username and password. Therefore, you must also change the LDAP TPC Administrator password in your LDAP-compliant directory when you change the WebSphere administrative user password for the Device server.

To change the WebSphere administrative user password for the Device server, follow these steps:

- 1. Stop the Device server.
- 2. Go to the <TPC\_install\_dir> directory. For example:

```
C:\Program Files\IBM\TPC\device\bin\W32-ix86 (Windows)
/<usr or opt>/IBM/TPC/device/bin/aix (AIX)
/<usr or opt>/IBM/TPC/device/bin/linux (Linux)
```

3. Run the ChangeWASAdminPass script:

ChangeWASAdminPass.<bat or sh> <user\_ID> <password> <install\_dir>

Where <user\_ID> is the WebSphere user ID, <password> is the password, and <install\_dir> is the directory where the Device server is installed.

4. Restart the Device server.

## Changing the DB2 password for the Data Server

This section provides information about changing the DB2 password for the Data Server.

To change the DB2 password, complete the following steps:

1. From a command prompt, change to the directory where the file repository.config resides in the IBM Tivoli Storage Productivity Center installation path. For example:

c:\Program Files\IBM\TPC\data\config\ (Windows)
/<usr or opt>/IBM/TPC/data/config/ (AIX or Linux)

 Run the following command for the Data server. This assumes that the Tivoli Storage Productivity Center directory is in C:\Program Files\IBM\TPC for Windows.

```
"C:\Program Files\IBM\TPC\data\config>\"program files"\
ibm\tpc\jre\bin\java -classpath "\program files\ibm\tpc\data\server\lib\
TSRMsrv.zip" com.tivoli.itsrm.repository.Transform
-p <new password> repository.config
```

- 3. Stop and then restart the Data Server.
- 4. Start the Tivoli Storage Productivity Center GUI.
# Changing the DB2 password for the Agent Manager on Windows

This topic describes how to change the DB2 password for the Agent Manager on Windows.

To change the DB2 password for the Agent Manager on Windows, complete the following steps:

- Go to the bin directory. This is the default directory: <Agent\_Manager\_install\_dir>\AgentManager\AppServer\ agentmanager\bin
- 2. Run the WebSphere wsadmin command using the following parameters:
  - a. The following parameters are required by the wsadmin command:
    - -f Full path of the EPMDBUserAdmin.jacl script. For example: <Agent\_Manager\_install\_dir>\AgentManager\install\jacl\ EPMDBUserAdmin.jacl

-lang jacl

Required.

#### -conntype

Specify SOAP.

#### -wsadmin\_classpath

List of fully-qualified jar files needed to run this script.

Here is an example:

```
<Agent Manager install dir>\AgentManager\AppServer\
agentmanager\bin>
>wsadmin -f
"<Agent Manager install dir>\AgentManager\install\jacl\
EPMDBUserAdmin.jacl"
-lang jacl
-conntype SOAP -port 8881 -wsadmin classpath
"<Agent_Manager_install_dir>\AgentManager\install\lib\
jlog.jar;
<Agent Manager install dir>\AgentManager\install\lib\install.jar"
-propfile
"<Agent_Manager_install_dir>\\AgentManager\\install\\
AMInstall.properties"
-logDir
"<Agent Manager_install_dir>\AgentManager\logs"
-DBUserID <user_ID> -DBPassword <password>
```

Note: The double back slashes in the AMInstall.properties line is correct.

If successful, you will see this series of messages:

WASX7209I: Connected to process "AgentManager" on node AgentManagerNode using SOAP connector; The type of process is: UnManagedProcess

WASX7303I: The following options are passed to the scripting environment and are available as arguments that are stored in the argv variable: "[-propfile, C:\\ Program Files\\IBM\\AgentManager\\install\\ AMInstall.properties, -logDir, C:\Prog ram Files\IBM\AgentManager\logs, -DBUserID, db2admin, -DBPassword, tpc8test]"

CTGEM2100I The WebSphere configuration script EPMDBUserAdmin.jacl started. The action taken is update.

CTGEM2108I The object with ID (cells/AgentManagerCell| security.xml#JAASAuthData\_ 1212654377031) and attribute name password was modified.

CTGEM2101I The WebSphere configuration script EPMDBUserAdmin.jacl completed successfully.

b. The following parameters are required by the EPMDBUserAdmin.jacl script:

#### -propfile

Fully-qualified Java Properties file (AMInstall.properties). Note that on Windows, this path requires a double set of back slashes for each directory separator. Here is an example:

C:\\Program Files\\IBM\\AgentManager\\install\\ AMInstall.properties

#### -logDir

Directory to store log files. Note that on Windows, this path requires a double set of back slashes for each directory separator. Here is an example:

C:\\Program Files\\IBM\\AgentManager\\install\\jacl

**-port** The port number for WebSphere. To get the port number, look in the following file:

<WAS\_install\_dir>\config\cells\node\_name\nodes\node\_name\ serverindex.html

Look for a tag containing the property: serverType="APPLICATION SERVER"

Look for an entry within that tag with the following property: endPointName="SOAP CONNECTOR ADDRESS"

Look for a port property within that tag. This is the port for WebSphere.

#### -DBUserID

Use the DB2 user ID (for example, db2admin).

#### -DBPassword

The password for the DB2 user ID.

- c. The following keys in AMInstall.Properties file must have these values set:
  - **Cell** This is your WebSphere Cell Name. Embedded WebSphere hard codes the value "DefaultNode" for both its Cell Name and Node Name. There is no need to change this value.
  - **Type** This is the type of database that the Agent Manager uses. Choices are DB2, Cloudscape, and Oracle. The key and value pair looks like this example: Type=db2.

#### AuthDataAlias

The J2C Authentication Data. The key and value pair looks like this example: AuthDataAlias=AgentRegistryDBAuth.

d. Run the **wsadmin** command. Here is an example of the command:

wsadmin -f c:\<Agent\_Manager\_install\_dir>\EPMDBUserAdmin.jacl -conntype SOAP -port 8881

-wsadmin\_classpath <Agent\_Manager\_install\_dir>\install\lib\JLog.jar;C:\
 <Agent\_Manager\_install\_dir>\install\lib\install.jar

- -propfile C:\\<Agent\_Manager\_install\_dir>\\AMInstall.properties
- -logDir c:\\amjacl
- -DBUserID <user\_ID>
- -DBPassword <password>
- **e**. You should see messages similar to this when you run the command successfully:

WASX7209I: Connected to process "server1" on node <node\_name> using SOAP connector; The type of process is: UnManagedProcess CTGEM2100I The WebSphere configuration script EPMDBUserAdmin.jacl started. The action taken is update. CTGEM2108I The object with ID (cells/<cell\_name>: security.xml#JAASAuthData\_1125249833946) and attribute name password was modified. CTGEM2101I The WebSphere configuration script EPMDBUserAdmin.jacl completed successfully.

- **3**. Stop and restart the Agent Manager. Verify that the Agent Manager can access its database. Check the activity.log file under the Agent Manager directory.
- 4. Run the **HealthCheck.bat** command with the agent registration password. For example:

HealthCheck.bat -registrationPw changeMe
(changeMe is the common agent registration password)

# Changing the DB2 password for the Agent Manager on UNIX or Linux

This topic describes how to change the DB2 password for the Agent Manager on UNIX or Linux.

To change the DB2 password for the Agent Manager on UNIX or Linux, complete the following steps:

- Go to the bin directory. This is the default directory: <Agent\_Manager\_install\_dir>/AgentManager/AppServer/ agentmanager/bin
- 2. Run the WebSphere wsadmin command using the following parameters:
  - **a**. The following parameters are **required** by the **wsadmin** command:

#### -conntype

Choices are NONE, RMI, or SOAP. Select SOAP.

#### -wsadmin\_classpath

List of fully-qualified jar files needed to run this script (jlLog.jar and install.jar), separated by a colon. This is an example: <Agent\_Manager\_install\_dir>\install\lib\jlog.jar:

<Agent\_Manager\_install\_dir>\install\lib\install.jar

b. The following parameters are required by the EPMDBUserAdmin.jacl script:

#### -propfile

Fully-qualified Java Properties file (AMInstall.properties). Here is an example:

<Agent\_Manager\_install\_dir>/install/AMinstall.properties

#### -logDir

Directory to store log files. Here is an example:

<Agent Manager install dir>/scriptlogs/

-port The port number for WebSphere. To get the port number, look in the following file:

<WAS\_install\_dir>/config/cells/node\_name/nodes/node\_name\ serverindex.html

Look for a tag containing the property: serverType="APPLICATION\_SERVER"

Look for an entry within that tag with the following property: endPointName="SOAP CONNECTOR ADDRESS"

Look for a port property within that tag. This is the port for WebSphere.

#### -DBUserID

Use the DB2 user ID (for example, db2inst1).

#### -DBPassword

The password for the DB2 user ID.

- c. The following keys in AMInstall. Properties file must have these values set:
  - **Cell** This is your WebSphere Cell Name. Embedded WebSphere uses the value "DefaultNode" for both its Cell Name and Node Name. There is no need to change this value.
  - **Type** This is the type of database that the Agent Manager uses. Choices are DB2, Cloudscape, and Oracle. The key and value pair looks like this example: Type=db2.

#### AuthDataAlias

The J2C Authentication Data. The key and value pair looks like this example: AuthDataAlias=AgentRegistryDBAuth.

d. Run the **wsadmin** command. Here is an example:

**e**. You should see messages similar to this when you run the command successfully:

WASX7209I: Connected to process "server1" on node <node\_name> using SOAP connector; The type of process is: UnManagedProcess CTGEM2100I The WebSphere configuration script EPMDBUserAdmin.jacl started. The action taken is update. CTGEM2108I The object with ID (cells/<cell\_name>: security.xml#JAASAuthData\_1125249833946) and attribute name password was modified. CTGEM210II The WebSphere configuration script EPMDBUserAdmin.jacl completed successfully.

**3**. Source the db2profile. (This step must be done if the Agent Manager is manually started. Otherwise, if autostart is used, then this step is done automatically.)

- 4. Stop and restart the Agent Manager. Verify that the Agent Manager can access its database. Check the activity.log file under the Agent Manager installation directory.
- 5. Issue the **HealthCheck.sh** command with the agent registration password. For example:

./HealthCheck.sh -registrationPW changeMe
(changeMe is the agent registration password)

# Changing the host authentication password for the Device server

This topic describes how to change the host authentication password for the Device server. If you change this password for the Device server, you must also change the host authentication password for the Fabric agent.

To change the host authentication password for the Device server, complete the following steps:

- 1. Open the IBM Tivoli Storage Productivity Center GUI.
- 2. Expand Administrative Services → Services → Device server.
- 3. Right-click Device server and select Change password from the pop-up menu.
- 4. Enter the new password and click OK.
- 5. Make sure you change the host authentication password for the Fabric agent. See "Changing the host authentication password for the Fabric agent."

# Changing the host authentication password for the Fabric agent

If you change the host authentication password for the Device server, you must also change the password for the Fabric agent. This topic describes how to change the host authentication password for the Fabric agent.

To change the host authentication password for the Fabric agent, complete the following steps:

1. For Windows, go to the following directory and run these commands:

```
cd <TPC_install_dir>\device\bin\w32-ix86
setenv
srmcp -u <user_ID> -p <password> ConfigService
setAuthenticationPW <new_host_password>
```

2. For UNIX or Linux, go to the following directory and run these commands:

<usr or opt>/tivoli/ep/subagents/TPC/fabric/bin/

```
<aix or linux or solaris2>
```

./setenv.sh (note there is a space between the two dots)

- ./srmcp.sh -u <user\_ID> -p <password> ConfigService
  - setAuthenticationPw <new\_host\_password>

# Changing the agent registration password

This section provides information about the agent registration password and how to change it.

The agent registration password serves two purposes:

- · Validates the registration of agents
- Locks the agentTrust.jks truststore file

Therefore, when you change the password, you must update the Agent Manager properties, change the password in the truststore file, and redistribute the truststore file to unregistered agents.

To change the password used by agents when they register:

 Change the value of the Registration.Agent.Access.Password property in the Agent Manager configuration file, AgentManager.properties by running the following command:

EncryptAMProps <new\_password>

Where <new\_password> is the new agent registration password. This command updates the **AgentManager.properties** file.

- Log on to the Agent Manager server as the user that runs the WebSphere Application Server processes. This is the Administrator on Windows systems. On UNIX and Linux systems, this is typically root but can be changed after installing the Agent Manager.
- **3**. Update the **agentTrust.jks** truststore file by encrypting it with the new password. The password used to encrypt the **agentTrust.jks** file must match the password specified in the **AgentManager.properties** file.
  - a. Start the IBM Key Management utility that is provided with WebSphere:
    - 1) Change to the <Agent\_Manager\_install\_dir>\embedded\bin directory.
      - 2) Run one of the following commands:

#### On Windows Systems ikeyman.bat

# On AIX, Linux, and Solaris systems ikeyman.sh

- b. In the IBM Key Management window, click **Key Database File** → **Open**.
- c. In the Open window, specify the truststore file:
  - 1) In the **Key database type** field, select **JKS**.
  - Click Browse to locate the agentTrust.jks truststore file in the <Agent\_Manager\_install\_dir>\certs directory.

If this file is missing or corrupted on the Agent Manager server, you can copy the **agentTrust.jks** from an agent or resource manager in your deployment. However, because the password for the file changes when the agent or resource manager registers, you must use the password that unlocks the file on that system, rather than the agent registration password.

- 3) Click **OK** to open the truststore file.
- d. In the Password Prompt window, type the current agent registration password and then click **OK**. The IBM Key Management window now shows the **agentTrust.jks** file, which contains the signer certificate named **rootcert**.
- e. In the IBM Key Management window, click **Key Database File** → **Change Password**.
- f. In the Change Password window, enter and confirm the new password, and then click OK. The agentTrust.jks file is encrypted with the new password and updated in the <Agent\_Manager\_install\_dir>\certs directory.
- g. Click **Key Database File** → **Exit** to close the IBM Key Management window.
- 4. Restart the Agent Manager server to start using the new properties file.

5. Delete the **pwd** file from the certs directory on the agents and resource managers where you will be distributing the truststore file. Redistribute the truststore file to any agent or resource manager that has not yet registered. Do not distribute the new truststore file to agents or resource manager that are currently registered. If you are using a copy of the agent installation files to rapidly deploy agents, copy the new **agentTrust.jks** truststore file to that location.

# Changing the registration password for a resource manager

This section provides information on changing the password for resource manager registration.

To change the password for resource manager registration, use the **AuthXMLAddUser** command to redefine the user whose password needs to change:

- 1. Edit the **Authorization.xml** file using a text editor. The file is located in the <Agent\_Manager\_install\_dir>\config directory.
- Identify all of the authType elements whose userList attribute contains the user's name. In the following sample Authorization.xml file, the user TPCAdmin (shown in bold face type) is in the userList attribute of the Tivoli Storage Productivity Center authorization type:

```
<authorization>
<user id="TPCAdmin" password="<encrypted_password>" />
<authType name="IBM Tivoli Storage Productivity Center for Fabric"
userList="TPCAdmin"/>
</authorization>
```

For IBM Tivoli Storage Productivity Center for Data, the authorization type would look like this:

```
<authorization>
<user id="TPCAdmin" password="<encrypted_password>" />
<authType name="IBM Tivoli Storage Productivity Center for Data"
userList="TPCAdmin"/>
</authorization>
```

The file might contain a generic authorization file list. The use of the type "\*" in the following example shows that the default user, **manager**, can register all types of resource managers.

3. At a command prompt, change to the <Agent\_Manager\_install\_dir>/bin directory and use the AuthXMLAddUser command to change the password. See "Creating a user for resource manager registration" on page 424 for information on the AuthXMLAddUser command. For example, to change the password for the FabricAdmin user in the first sample Authorization.xml, when the Agent Manager is on an AIX, Linux, or Solaris system, run the following command. Because the IBM Tivoli Storage Productivity Center for Fabric authorization type contains the space character, its name is enclosed in double quotation marks (") on the command line:

cd <Agent\_Manager\_install\_dir>/bin

./AuthXMLAddUser.sh FabricAdmin <mynewpassword>

"IBM Tivoli Storage Productivity Center for Fabric"

Be sure to specify all of the authorization types that are currently listed. If you omit an existing type, the user cannot register that type of resource manager.

For IBM Tivoli Storage Productivity Center for Data, the command would look like this:

```
cd <Agent_Manager_install_dir>/bin
./AuthXMLAddUser.sh FabricAdmin <mynewpassword>
    "IBM Tivoli Storage Productivity Center for Data"
```

4. Restart the Agent Manager.

# Changing the password encryption key

This section provides information on the password encryption key and how to change it.

The passwords in the **AgentManager.properties** and **Authorization.xml** files are encrypted using the HMAC-SHA1 keyed-hashing algorithm and a password that is randomly generated when the Agent Manager is installed.

To change the password encryption key:

- 1. Stop the application server where the Agent Manager application is running.
- 2. Locate and delete the key file, which is pointed to by the ARS.directory and REG.keyPWfile.name properties in the **AgentManager.properties** file. The next time a program that requires this key is run, the Agent Manager randomly generates a new key.
- **3.** Run the **EncryptAMProps** command to update the agent registration password in the **AgentManager.properties** file.
- 4. Run the **AuthXMLAddUser** command to redefine each resource manager user in the **Authorization.xml** file.
- 5. Start the application server.

# Manually encrypting a password

You can manually encrypt a password for use in the **Authorization.xml** or **AgentManager.properties** file, or to verify an encrypted password. You should do this only if you cannot use the commands that replace passwords in those files.

Table 40 lists the preferred commands for updating passwords in the **Authorization.xml** or **AgentManager.properties** file.

To encrypt passwords in this file	Use this command		
Authorization.xml	AuthXMLAddUser		
AgentManager.properties	EncryptAMProps		

Table 40. Commands that encrypt passwords for the Agent Manager

To encrypt a password to manually replace a password:

1. Use the **EncryptPW** command to encrypt the new password. The command takes a single argument, the clear text password you want to encrypt. For example:

EncryptPW <mynewpassword>

The command returns a single output string, the encrypted password.

- Copy the encrypted password from the display and paste it into the password field of the file.
- 3. Save the file.

# Using the password tool

IBM Tivoli Storage Productivity Center provides a password tool for changing the database user ID and DB2 service passwords.

The password tool changes the password for the following components:

- Data server
- Device server
- · Optionally, the DB2 services password on Windows

To change the password, follow these steps:

- 1. Logon to IBM Tivoli Storage Productivity Center using the Administrator user ID.
- 2. Change the user ID password on the system.

#### For Windows

Follow these steps:

- a. From the desktop, click My Computer > Manage.
- b. On the Computer Management window, click Local Users and Groups > Users.
- **c.** In the right pane, right-click on the database user ID that you specified at installation time.
- d. Click **Set Password**. In the Set Password window, enter the new password twice. Click **OK**.

#### For AIX or Linux

Run the **passwd** command logged in as the DB2 user. To change other user credentials, run the **passwd** *<username>* command.

3. On the IBM Tivoli Storage Productivity Center, go to the following directory: C:\Program Files\IBM\TPC\data\server\tools (for Windows) /opt/IBM/TPC/data/server/tools (for Linux or UNIX)

Run the following program:

changepasswords.bat (for Windows)
changepasswords.sh (for Linux or UNIX)

4. The main password tool panel is displayed. Select **Change DB2 user password for Device and Data Server**. Click **OK**.

Change I	DB2 user pa	ssword for	Device an	d Data Server
🔵 Change (	password fo	r the DB2 s	ervices	

Figure 89. Main password tool panel

5. The Change DB2 user password for Device and Data Server panel is displayed. Enter the new password twice and click **OK**. Leave the option for **Restart the Data and Device Server** checked.

Enter password		*******	
Confirm passwo	rd	*****	
Restart the Data	and Device Serve	r 🗹	

Figure 90. Change DB2 user password for Device and Data Server panel

- 6. The progress panel is displayed. When the password change procedure has completed, you will see the message "Finish!" Click **Back to Main**.
- 7. For Windows, you can change the password for the DB2 services. On the main password tool panel, select **Change password for the DB2 services**. Click **OK**.
- 8. The Change DB2 Services password panel is displayed. Enter the password twice and click **OK**.

9. The progress panel is displayed. When the password change procedure has completed, you will see the message "Finish!" Click Exit.

# Checking for a fully qualified host name

IBM Tivoli Storage Productivity Center requires fully qualified host names. Some machines might be configured to return a short host name, such as **ddunham** instead of a fully qualified host name, such as **ddunham.myorg.mycompany.com**. This topic provides information on how to check for a fully qualified host name.

# Checking for a fully qualified host name for Windows systems

This topic provides information on how to verify a fully qualified host name for Windows systems.

To verify a fully qualified host name, complete the following steps:

- 1. On the desktop, right-click My Computer.
- 2. Click Properties.
- 3. The System Properties panel is displayed.
- 4. On the Computer Name tab, click Change.
- 5. The Computer Name Changes panel is displayed. Enter your fully qualified host name in the Computer name filed. Click **More**.
- 6. The DNS Suffix and NetBIOS Computer Name panel is displayed. Verify that the **Primary DNS suffix** field displays a domain name. Click **OK**.
- 7. Click OK on the Computer Name Changes panel.
- 8. Click Apply and close the System Properties panel.

# Checking for a fully qualified host name for AIX systems

This topic provides information on how to verify a fully qualified host name for AIX.

The default domain name search order is as follows:

- 1. Domain Name System (DNS) server
- 2. Network Information Service (NIS)
- 3. Local /etc/hosts file.

If the /etc/resolv.conf file does not exist, the /etc/hosts file is used. If only the /etc/hosts file is used, the fully qualified computer name must be the first one that is listed after the IP address.

Verify that the /etc/resolv.conf file exists and contains the appropriate information, such as:

domain mydivision.mycompany.com nameserver 123.123.123.123

If NIS is installed, the /etc/irs.conf file overrides the system default. It contains the following information:

hosts = bind,local

The /etc/netsvc.conf file, if it exists, overrides the /etc/irs.conf file and the system default. It contains the following information: hosts = bind,local

If the NSORDER environment variable is set, it overrides all of the preceding files. It contains the following information: export NDORDER=bind,local

# Checking for a fully qualified host name for Linux systems

This topic provides information on how to verify a fully qualified host name for Linux.

Linux uses a resolver library to obtain the IP address corresponding to a host name. The /etc/host.conf file specifies how names are resolved. The entries in the /etc/host.conf file tell the resolver library what services to use, and in what order, to resolve names. Edit the host.conf file using the **vi** editor to add the following lines:

# Lookup names through DNS first then fall back to /etc/hosts. order bind,hosts # Machines with multiple IP addresses. multi on # Check for IP address spoofing. nospoof on

The **order** option indicates the order of services. The sample entry specifies that the resolver library should first consult the name server to resolve a name and then check the /etc/hosts file. It is recommended to set the resolver library to first check the name server, bind file, and then the hosts file (hosts) for better performance and security on all your servers. You must have the DNS and BIND software installed for this configuration to work.

The **multi** option determines whether a host in the /etc/hosts file can have multiple IP addresses. Hosts that have more than one IP address are said to be multihomed, because the presence of multiple IP addresses implies that the host has several network interfaces.

The **nospoof** option takes care of not permitting spoofing on this machine. IP-Spoofing is a security exploit that works by tricking computers into a trust relationship that you are someone that you really are not. In this type of attack, a machine is set up to look like a legitimate server and then issue connections and other types of network activities to legitimize end systems, other servers, or large data repository systems. This option must be set ON for all types of servers.

# Checking for a fully qualified host name for Solaris systems

This topic provides information on how to verify a fully qualified host name for Solaris.

Verify that the /etc/resolv.conf file exists and contains the appropriate information, such as:

domain mydivision.mycompany.com nameserver 123.123.123.123

A short name is used if the /etc/nsswitch.conf file contains a line that begins as follows and if the /etc/hosts file contains the short name for the computer: hosts: files

To correct this problem, follow these steps:

 Change the line in the /etc/nsswitch.conf file to the following: hosts: dns nis files

- Enter the following command to stop the inet service: /etc/init.d/inetsvc stop
- Enter the following command to restart the inet service: /etc/init.d/inetsvc start

# Granting local administrative privileges to a domain account

For Windows users, the user account which the Common agent runs under requires local administrative rights. Because these rights are not necessarily guaranteed for domain users in a Windows domain environment, this topic provides information on how to grant local administrative rights for domain users. Using this procedure, you do not have to manually process each machine in the domain.

To use Group Policy to grant local administrative privileges to a domain account, complete the following steps:

- On the domain controller, go to Administrative Tools → Active Directory Users and Computers (you must be running with Domain Administrator privileges).
- 2. Right-click on the Organizational Unit (OU) upon which you want to apply the Group Policy. Click **Properties**.
- **3**. The Group Policy Properties panel is displayed. Select the Group Policy tab and click **New** to create a new Group Policy.
- 4. Designate a name for the new Group Policy. Select the new Group Policy and click **Edit**.
- 5. The Group Policy Object Editor panel is displayed. Go to New Group Policy Object <your\_policy> → Computer Configuration → Windows Settings → Security Settings → Restricted Groups. Right-click on Restricted Groups. Click Add Group.
- 6. For example, name the new group "Administrators." Under "Properties", add the user "Administrator", and the domain accounts or groups upon which you want the Group Policy in effect for. For example, you can add "TPC\tapeadmin", "TPC\tapegroup", and "TPC\TestGroup". Click **OK**.
- 7. Add these user rights to the domain account:
  - Act as part of the operating system
  - Log on as a service

In the Group Policy Object Editor, go to New Group Policy Object <your\_policy> > Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignments. In the right pane, select "Log on as a service" and double-click. Add the domain user for whom you are granting the user right for and click OK. Repeat this step for "Act as part of the operating system."

8. The group policy is now enforced for the Organizational Unit to include the domain accounts and groups specified under the local Administrators group on each computer in the Organizational Unit. In addition, the domain user has been granted the necessary rights. To verify this, log into a domain computer and open the Computer Management console. Select **Groups**, double-click on the Administrators group, and verify the membership of the domain users.

# Importing SSL certificates for VMware

If your VMware uses SSL certificates, you must import the SSL certificates for VMware Virtual Infrastructrue Data Source.

If your VMware uses SSL certificates, you must follow these steps before you can get data from the VMware Virtual Infrastructure. Complete the following steps:

- Open a browser. Point the browser to the following: https://<ESX\_server\_IP\_address>/host
- You will see a list of Configuration files. Right-click on ssl\_cert. Save the file as <ESX\_machine\_name>.crt.

**Note:** Depending on your browser, you would save the file using **Save Target** as (for Internet Explorer) or **Save Link as** (for Firefox). Use this file to import the certificate.

**3**. The VirtualCenter Server uses a self-generated SSL certificate located in the following directory:

```
C:\Documents and Settings\All Users\Applicatin Data\
VMware\VMware VirtualCenter\SSL\rui.crt
```

Install these certificates into a certificate store on the client machine. Copy the certificate file or files from the servers to a directory on the client machine. Enter the **keytool** command:

keytool -import -file <certificate-filename>
-alias <server-name>
-keystore vmware.jks

For example, run this command:

keytool -import -file vc-server1.cer -alias vc-server1
-keystore vmware.jks

Enter a password for the keystore. Enter yes to import the certificate.

The truststore will be located in the Device server configuration directory:

<TPC\_install\_directory>/device/conf

If the truststore was generated in another directory, it must be copied to <TPC\_install\_directory>/device/conf. The truststore is called **vmware.jks**. The truststore will automatically be defined at service startup time as this property in the Device server JVM:

javax.net.ssl.trustStore System

- 4. Add a VMware data source using the URL, user name, and password for the service console.
- 5. Run a discovery job for the VMware data source.
- 6. Run a probe job for the VMware data source.
- 7. You will now be able to display VMware Virtual Infrastructure in reports and the topology viewer.

# **Repository Copy tool**

The Repository Copy tool enables you to export all the tables in the IBM Tivoli Storage Productivity Center repository (Data Manager data) for purposes of debugging problems.

You can send the output to the IBM Support Center to help debug problems.

#### Note:

• You must stop the Device server and Data server before running **repocopy**.

• You cannot import **repocopy** data into the IBM Tivoli Storage Productivity Center database if the migration tool has not been run against the database. When you upgrade the Device server, you must run the migration tool before importing **repocopy** data.

# Exporting repository data

Use the Repository Copy tool to export data from an existing repository into a comma delimited file.

To export repository data, follow these steps:

- 1. Stop the Device server and Data server.
- 2. Go to the following default directory:
  - If on Windows: c:\Program Files\IBM\TPC\data\server\tools
  - If on Linux or UNIX: /opt/IBM/TPC/data/server/tools
- **3**. Run the **repocopy.bat** or **repocopy.sh** command. A window is displayed prompting you for what you would like to do.
- 4. Select **Export data from repository tables**, and then click **Next**. The Options for Import/Export window is displayed.
- 5. In the Options for Import/Export window, enter information in the following fields:

## **Directory for Export**

Enter the directory where the comma delimited file will be saved.

#### Delimiter

Enter a delimiter for the delimited file format (comma is the default).

**Quote** Enter the symbol that will contain string data (double quotes is the default).

IBM Tivoli Storage Productivity Center will export the data into the comma delimited file you specify, and place it in a file named <tablename>.txt. Click Next.

- 6. The Choices for DB2 Export window is displayed. You have the following choices:
  - Export Using DB2 native format
  - Export Using text files

Make a choice and click Next.

- 7. The Table Export Choices windows is displayed. You have the following choices:
  - Export base tables (always)
  - Export Performance Manager tables
  - Export history tables used for IBM Tivoli Storage Productivity Center for Data history reports

Make a choice and click Next.

8. The Connection Properties window is displayed.

In this step, Tivoli Storage Productivity Center reads the server.config file and determines your current repository and the information for accessing the database. The information detected in the server.config file is displayed in the Connection Properties window within the following fields: **Database Types**, **User name**, **Password**, **Driver Class**, **Driver URL**, **Database**, **DB Creator**, **Classpath**.

**Note:** If you want to export data from a different database from the one listed in the server.config file, you can select the database from the **Database Types** list box and manually enter the database information. Click **Finish**.

- **9**. Tivoli Storage Productivity Center will then connect to the database and display the database and connection information. Click **Run** to begin the export process.
- **10.** A window is displayed containing the export progress log. As you progress through the export, messages are written to this progress log, allowing you to keep track of the steps as they happen.

**Note:** When you run the **repocopy** tool on a server that has a remote database, the **repocopy** tool displays a message. When the **repocopy** tool is used with a remote database, the DB2 shared library is not available for loading libTSRMinsudb.so. You can ignore this message. Just click **OK** and continue.

# Importing repository data

Use the Repository Copy tool to import data from a comma delimited file. You must have previously exported data from an existing repository.

To import data into repository tables, follow these steps:

- 1. Stop the Device server and Data server.
- 2. Go to the following directory:
  - If on Windows: c:\Program Files\IBM\TPC\data\server\tools
  - If on Linux or UNIX: /opt/IBM/TPC/data/server/tools
- **3.** Run the **repocopy.bat** or **repocopy.sh** command. A window is displayed prompting you for what you would like to do
- 4. Select **Import data into repository tables**, and then click **Next**. The Options for Import/Export window is displayed.
- 5. In the Options for Import/Export window, enter information in the following fields:

#### **Directory for Import**

Enter the directory where the comma delimited files are stored.

#### Delimiter

Enter a delimiter used for the delimited file format (comma is the default). You must use the same delimiter that was used in the exported file.

**Quote** Enter the symbol used to contain string data (double quotes is the default). You must use the same quote that was used in the exported file.

#### **Delete before inserting**

Check this option if you want to delete any existing data in the repository tables before importing new data.

IBM Tivoli Storage Productivity Center will import the data from the comma delimited file that you specify. Click **Next**.

6. The Connection Properties window is displayed.

- Enter the database and the access information of the database to which you want to import data. The Connection Properties window contains the following fields: Database Types, User name, Password, Driver Class, Driver URL, Database, DB Creator, Classpath. Click Finish.
- 8. Tivoli Storage Productivity Center will then connect to the database and display the database and connection information. Click **Run** to begin the import process.
- **9**. A window is displayed containing the import progress log. As you progress through the import, messages are written to this progress log, allowing you to keep track of the steps as they happen.

**Note:** When you run the **repocopy** tool on a server that has a remote database, the **repocopy** tool displays a message. When the **repocopy** tool is used with a remote database, the DB2 shared library is not available for loading libTSRMinsudb.so. You can ignore this message. Just click **OK** and continue.

# Service tool: collecting information

This section provides information about the information the **Service** tool collects from all installed IBM Tivoli Storage Productivity Center components. This tool detects system configuration, collects the applicable information, and creates a ZIP file that can be sent to the IBM support center.

The **Service** tool collects the following information:

- Host name
- IP address and configuration information
- · Operating system and version
- Java home, version, and classpath
- Java Virtual Machine (JVM) implementation name and version
- Protocol statistics and current TCP/IP network connections, including listening ports
- Diagnostic information regarding the system and its services
- Listing of all library files, for example, server and library, agent and library, and GUI library

When the **Service** tool is run on the system where the Data server or the Device server is installed, it also collects the following information:

- For the Data Server, information on all the GUIs (remote and local) associated with this Data Server
- All e-fixes applied
- Installation logs
- Everything in the log directory, including subdirectories
- Everything in the **conf** directory
- Directory listing of the **lib** directory
- Everything in the WebSphere log directory
- Information in the server.xml file: manager\apps\was\config\cells\DefaultNode\nodes\DefaultNode\ servers\server1\server.xml
- The version of DB2 (output from the db2level command)
- Output from the ipconfig /all command (Windows)
- Output from the **ipconfig -a** command (Linux or UNIX)

• Output from the netstat -an command

When the **Service** tool runs on the Data agent or Fabric agent computer, it collects this information:

- All e-fixes applied
- traceNative.log files from <Agent\_install\_dir>\servlet\bin directory.
- Scanner benchmark files from <Agent\_install\_dir>\agent\bin\<platform> directory.
- Core files on the agent computer (if any).
- Output from scanners run manually from the command line.
- Everything in the log directory (including subdirectories).
- Everything in the conf directory
- Directory listing of the lib directory
- Output from the ipconfig /all command (for Windows).
- Output from the **ifconfig -a** command (for UNIX or Linux).
- Output from the netstat -an command

**Note:** the **Service** tool does not collect service logs or other service information for IBM Tivoli Storage Productivity Center for Replication. If you need to collect the log and trace files for the replication server, see the **Obtaining logs and tracing** topic in the **Troubleshooting** section of the Tivoli Storage Productivity Center for Replication Information Center.

# Running the Service tool for the servers

This topic describes how to run the **Service** tool for the Data Server and the Device server.

To run the tool for the servers, complete the following steps:

- 1. Log onto the system. You must have administrator authority on Windows or root authority on UNIX or Linux.
- 2. If you used the default directory, go to the following directory:
  - For Windows: C:\Program Files\IBM\TPC\service\.
  - For Linux or UNIX: /<usr or opt>/IBM/TPC/service/.
- **3**. Run the following program:
  - For Windows: service.bat.
  - For Linux or UNIX: service.sh.
- 4. One or more zip files are created in the directory where you ran the **Service** tool. If you have a Data agent or Fabric agent installed on the same computer as the Data Server or the Device server, that information is collected when you run the tool for the Data Server or the Device server. The following zip files are created:

TPCDATAservice.zip (for the Data Server) TPCDEVservice.zip (for the Device Server) TPCDATACAservice.zip (for the Data agent) TPCDEVCAservice.zip (for the Fabric agent)

# Running the Service tool for the agents

This topic describes how to run the **Service** tool for the remote agents.

To run the **Service** tool for the remote Data agent or Fabric agent, complete the following steps:

- 1. Log onto the system. You must have administrator authority on Windows or root authority on UNIX or Linux.
- 2. If you used the default directory, go to the following directory:
  - For Windows: C:\Program Files\IBM\TPC\ca\subagents\TPC\service.
  - For Linux or UNIX: /<usr or opt>/IBM/TPC/ca/subagents/TPC/service.
- 3. Run the following program:
  - For Windows: service.bat.
  - For Linux or UNIX: service.sh.
- 4. A zip file is created in the directory where you ran the Service tool. The following zip files are created:

TPCDATACAservice.zip (for the Data agent) TPCDEVCAservice.zip (for the Fabric agent)

# **Chapter 7. Troubleshooting**

This section provides information about troubleshooting IBM Tivoli Storage Productivity Center problems.

For additional troubleshooting topics, check the Tivoli Storage Productivity Center technical support Web site: http://www.ibm.com/servers/storage/support/ software/tpc. Click on a product. Click **Troubleshoot**. Under Problem resolution, click on Version 4 Flashes, Technical notes, and APARs.

Before contacting IBM Support Center about a problem, review the information at http://www-1.ibm.com/support/docview.wss?rs=1133&uid=swg21292441.

# **Configuration files**

This topic provides default file locations for IBM Tivoli Storage Productivity Center configuration files.

The default file locations for the configuration files are shown in the following table.

Tivoli Storage	
Productivity Center For Windows:	
c:\Program Files\IBM\TPC\config	
For UNIX or Linux:	
/opt/IBM/TPC/config	
Data Server	
For Windows:	
c:\Program Files\IBM\TPC\data\config	
For UNIX or Linux:	
/opt/IBM/TPC/data/config	
Device server	
For Windows:	
c:\Program Files\IBM\TPC\device\conf	
For UNIX or Linux:	
/opt/IBM/TPC/device/conf	
Common agent	
For Windows:	
c:\Program Files\IBM\TPC\ca\config	
For UNIX or Linux:	
/opt/IBM/TPC/ca/config	
Data agent	
For Windows:	
c:\Program Files\IBM\TPC\ca\subagents\TPC\Data\config	
For UNIX or Linux:	
<pre>/opt/IBM/TPC/ca/subagents/TPC/Data/config</pre>	

Table 41. Default file locations for Tivoli Storage Productivity Center configuration files

Component	Default file location				
Fabric agent					
	For Windows: c:\Program Files\IBM\TPC\ca\subagents\TPC\Fabric\conf For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC/Fabric/conf				

Table 41. Default file locations for Tivoli Storage Productivity Center configuration files (continued)

# server.config file

This topic lists the parameters that are set in the server.config file. These parameters include Controller, Logging, Repository, and Service.

Table 42. Parameters for server.config file

Parameter	Description				
Controller parameters:					
name	Data Manager Server Name (host computer name)				
port	Port on which the server listens for requests (9549)				
maxConnections	Maximum number of concurrent sockets that the server will open (500)				
routerThreads	Number of threads redirect incoming requests to the appropriate service provider (1)				
serviceThreads	Number of threads to allocate for the Server internal service provider (2)				
agentErrorLimit	Number of consecutive attempts to reach an agent before the agent is displayed as DOWN. When an agent is in this state, no attempts to connect are made until either the agent contacts the Server or the agent status is manually changed to UP (3)				
adminGroup	Name of the group a user must be a member of in order to perform administrative functions from the Graphic User Interface (adm)				
commEncrypted	<ul> <li>Switch that secures communication between the Server/Agent and the Server/GUI by encrypting the data stream.</li> <li>0 = Off. Do not encrypt the data stream.</li> <li>1 = On. Encrypt the data steam.</li> </ul>				
hostAlias	This parameter appears if the HOST_ALIAS is not specific and represents the name of the server. This value for this parameter is used when multiple computers have the same name or the name cannot be determined.				
Logging parameters:					
logsKept	Number of server logs to keep (5)				

Description					
Maximum number of messages in a log, when this number is reached the log is closed and a new log is created. (100,000)					
<ul> <li>Name of the JDBC driver to use, normally:</li> <li>Oracle: oracle.jdbc.driver.OracleDriver</li> <li>MS SQL: com.inet.tds.TdsDriver</li> <li>Sybase: com.sybase.jdbc2.jdbc.SybDriver</li> <li>UDB/DB2: COM.ibm.db2.jdbc.app.DB2Driver</li> <li>Cloudscape: com.ibm.db2j.jdbc.DB2jDriver</li> </ul>					
<pre>The URL used to connect to the database, normally:    Oracle: jdbc:oracle:thin:@<host_name>:<port>:<sid>    MS SQL: jdbc:inetdae:<host_name>    Sybase: jdbc:sybase:Tds:host_name:port    UDR: idbc:database_name</host_name></sid></port></host_name></pre>					
User name that IBM Tivoli Storage Productivity Center uses to connect to the repository					
Number of database connections in a pool of reusable open connections (10)					
<ul> <li>Repeating section that indicates the service providers to start.</li> <li>REQUIRED:</li> <li>TStorm.server.svp.GuiSvp</li> <li>TStorm.server.svp.AgentSvp</li> <li>scheduler.Scheduler</li> </ul>					

Table 42. Parameters for server.config file (continued)

# scheduler.config file

This topic lists the parameters that are set in the scheduler.config file. These parameters include Concurrency parameters and Jobs parameters.

Table 43. Parameters for scheduler.config file

Parameter	Description
Concurrency parameters	5:
maxSubmitThreads	Number of threads to create that handle the submission of jobs (3)
maxCompleteThreads	Maximum Number of threads to create to handle job completions. Initially will create a pool of 1/2 the number that can grow to the maximum (3)
Jobs parameters:	

Table 43. Parameters for scheduler.config file (continued)

Parameter	Description				
minutesAdvanced	Number of minutes in advance of scheduled time to begin the scheduling process. This allows for the overhead time involved in scheduling a job so that the job will actually start close to the scheduled time (1)				

# **TPCD.config file**

This topic lists parameters that are set in the TPCD.config file. These include Server parameters and GUI parameters.

Parameter	Description				
Server parameters:					
threadPoolSize	Number of initial threads to create for handling requests (3)				
abbreviatedProbe	Only Small Computer Systems Interface (SCSI) commands are sent to disk drives for inquiry and disk capacity information (1).				
maxThreads	Maximum number of threads allowed for handling requests (8)				
pingReceiveTimeout	Number of seconds to wait before indicating that a ping has failed (10)				
skipAutoFS=1	Set to 1 for discovery on the Solaris Data agent to skip the automounts process. By default, discovery always processes automounts on the Solaris Data agent.				
GUI parameters:					
threadPoolSize	Number of initial threads to create for handling user interface requests (3)				
maxThreads	Maximum number of threads allowed for handling user interface requests (10)				
reportRowLimit	Maximum number of rows that will be sent at a time to the user interface. If this number is exceeded, a <b>More</b> button will be displayed above the table, along with a warning message (5000)				
keepCachedReport	Number of minutes to retain incomplete reports in the server's <i>tmp</i> directory (120)				

# agent.config file

The **agent.config** file contains configuration parameters for the Data agent. These parameters are set when the Data agent is installed; they can also be changed manually by modifying the file.

The following table contains the parameters for the agent.config file. If the Data agent is installed in the default location, this file is located at either /opt/IBM/TPC/ca/subagents/TPC/Data/config or C:\Program Files\IBM\TPC\ca\ subagents\TPC\Data\config.

agentPortPort on which the Data agent listens for requests. By default, this set to 9510.serverHostFully qualified host name of the system on which the Data server installed.serverPortPort on which the Data server listens for requests. By default, this set to 9549.logFilesKeptMaximum number of Data agent logs that are retained. When the number is reached, the oldest log file is overwritten. By default, this is set to five.messagesPerLogMaximum number of messages in a Data agent log file. When th number is reached, the a new log file is created. By default, this to 100,000.maxBacklogMaximum number of uncompleted jobs that are permitted. When number is reached, if additional job requests are made, any error generated. By default, this is set to 500.sendFailWaitNumber of seconds to wait before the Data agent attempts to res a message to the Data server. By default, this is set to 30.maxIdleThreadsMaximum number of idle threads to retain for use by future jobs default, this is set to 10.uptimePollHow often (in seconds) should agent check to ensure it is up (20 hostAliasThis parameter appears if the H0ST_ALIAS is not specific and represents the name of the server. This value for this parameter i used when multiple computers have the same name or the name cannot be determined.	Parameter	Description					
serverHostFully qualified host name of the system on which the Data server installed.serverPortPort on which the Data server listens for requests. By default, thi set to 9549.logFilesKeptMaximum number of Data agent logs that are retained. When th number is reached, the oldest log file is overwritten. By default, this is set to five.messagesPerLogMaximum number of messages in a Data agent log file. When th number is reached, the a new log file is created. By default, this is to 100,000.maxBacklogMaximum number of uncompleted jobs that are permitted. When number is reached, if additional job requests are made, any error generated. By default, this is set to 500.sendFailWaitNumber of seconds to wait before the Data agent attempts to res a message to the Data server. By default, this is set to 30.maxIdleThreadsMaximum number of idle threads to retain for use by future jobs default, this is set to 10.uptimePollHow often (in seconds) should agent check to ensure it is up (20) hostAliasThis parameter appears if the H0ST_ALIAS is not specific and represents the name of the server. This value for this parameter i used when multiple computers have the same name or the name cannot be determined.	agentPort Port on which the Data agent listens for requests. By defause set to 9510.						
serverPortPort on which the Data server listens for requests. By default, this set to 9549.logFilesKeptMaximum number of Data agent logs that are retained. When the number is reached, the oldest log file is overwritten. By default, is set to five.messagesPerLogMaximum number of messages in a Data agent log file. When the number is reached, the a new log file is created. By default, this to 100,000.maxBacklogMaximum number of uncompleted jobs that are permitted. When number is reached, if additional job requests are made, any error generated. By default, this is set to 500.sendFailWaitNumber of seconds to wait before the Data agent attempts to res a message to the Data server. By default, this is set to 30.maxIdleThreadsMaximum number of idle threads to retain for use by future jobs default, this is set to 10.uptimePollHow often (in seconds) should agent check to ensure it is up (20) hostAliashostAliasThis parameter appears if the H0ST_ALIAS is not specific and represents the name of the server. This value for this parameter i used when multiple computers have the same name or the name cannot be determined.	serverHost	Fully qualified host name of the system on which the Data server is installed.					
logFilesKeptMaximum number of Data agent logs that are retained. When the number is reached, the oldest log file is overwritten. By default, is set to five.messagesPerLogMaximum number of messages in a Data agent log file. When the number is reached, the a new log file is created. By default, this is to 100,000.maxBacklogMaximum number of uncompleted jobs that are permitted. When number is reached, if additional job requests are made, any error generated. By default, this is set to 500.sendFailWaitNumber of seconds to wait before the Data agent attempts to res a message to the Data server. By default, this is set to 30.maxIdleThreadsMaximum number of idle threads to retain for use by future jobs default, this is set to 10.uptimePollHow often (in seconds) should agent check to ensure it is up (20) hostAliashostAliasThis parameter appears if the H0ST_ALIAS is not specific and represents the name of the server. This value for this parameter i used when multiple computers have the same name or the name cannot be determined.	serverPort	Port on which the Data server listens for requests. By default, this is set to 9549.					
messagesPerLogMaximum number of messages in a Data agent log file. When th number is reached, the a new log file is created. By default, this to 100,000.maxBacklogMaximum number of uncompleted jobs that are permitted. When number is reached, if additional job requests are made, any error generated. By default, this is set to 500.sendFailWaitNumber of seconds to wait before the Data agent attempts to res a message to the Data server. By default, this is set to 30.maxIdleThreadsMaximum number of idle threads to retain for use by future jobs default, this is set to 10.uptimePollHow often (in seconds) should agent check to ensure it is up (20) hostAliashostAliasThis parameter appears if the HOST_ALIAS is not specific and represents the name of the server. This value for this parameter i used when multiple computers have the same name or the name cannot be determined.	logFilesKept	Maximum number of Data agent logs that are retained. When this number is reached, the oldest log file is overwritten. By default, this is set to five.					
maxBacklogMaximum number of uncompleted jobs that are permitted. When number is reached, if additional job requests are made, any error generated. By default, this is set to 500.sendFailWaitNumber of seconds to wait before the Data agent attempts to res a message to the Data server. By default, this is set to 30.maxIdleThreadsMaximum number of idle threads to retain for use by future jobs default, this is set to 10.uptimePollHow often (in seconds) should agent check to ensure it is up (20) hostAliashostAliasThis parameter appears if the H0ST_ALIAS is not specific and represents the name of the server. This value for this parameter i used when multiple computers have the same name or the name cannot be determined.	messagesPerLog	Maximum number of messages in a Data agent log file. When this number is reached, the a new log file is created. By default, this is set to 100,000.					
sendFailWaitNumber of seconds to wait before the Data agent attempts to res a message to the Data server. By default, this is set to 30.maxIdleThreadsMaximum number of idle threads to retain for use by future jobs default, this is set to 10.uptimePollHow often (in seconds) should agent check to ensure it is up (20) hostAliasThis parameter appears if the H0ST_ALIAS is not specific and represents the name of the server. This value for this parameter i used when multiple computers have the same name or the name cannot be determined.	maxBacklog	Maximum number of uncompleted jobs that are permitted. When this number is reached, if additional job requests are made, any error is generated. By default, this is set to 500.					
maxIdleThreadsMaximum number of idle threads to retain for use by future jobs default, this is set to 10.uptimePollHow often (in seconds) should agent check to ensure it is up (20)hostAliasThis parameter appears if the H0ST_ALIAS is not specific and represents the name of the server. This value for this parameter i used when multiple computers have the same name or the name cannot be determined.	sendFailWait	Number of seconds to wait before the Data agent attempts to resend a message to the Data server. By default, this is set to 30.					
uptimePollHow often (in seconds) should agent check to ensure it is up (20hostAliasThis parameter appears if the HOST_ALIAS is not specific and represents the name of the server. This value for this parameter i used when multiple computers have the same name or the name cannot be determined.	maxIdleThreads	Maximum number of idle threads to retain for use by future jobs. By default, this is set to 10.					
hostAlias This parameter appears if the H0ST_ALIAS is not specific and represents the name of the server. This value for this parameter i used when multiple computers have the same name or the name cannot be determined.	uptimePoll	How often (in seconds) should agent check to ensure it is up (20).					
	hostAlias	This parameter appears if the H0ST_ALIAS is not specific and represents the name of the server. This value for this parameter is used when multiple computers have the same name or the name cannot be determined.					
honorSentScripts If this parameter is set to '1', 't', 'T', 'y', or 'Y', the Data agent can run scripts sent from the Data server. Otherwise, only scripts tha exist in the <b>scripts</b> directory on the system where the Data agent installed can be run.	honorSentScripts	If this parameter is set to '1', 't', 'T', 'y', or 'Y', the Data agent can run scripts sent from the Data server. Otherwise, only scripts that are exist in the <b>scripts</b> directory on the system where the Data agent is installed can be run.					
TPCInstallLocation         Directory where the Data agent is installed.	TPCInstallLocation	Directory where the Data agent is installed.					

Table 44. Parameters for the agent.config file

# Log files

There are several product logs files to check when you have a problem.

# **Default log file locations**

Check the following default log file locations when you have a problem.

Table 45.	Default	log file	locations	for IBM	Tivoli	Storage	Productivity	Center	components
		<u> </u>				<u> </u>			,

Component	Log file location
Data Server	
	For Windows:
	c:\Program Files\IBM\TPC\data\log
	For UNIX or Linux:
	/opt/IBM/TPC/data/log
Device server	
	For Windows:
	c:\Program Files\IBM\TPC\device\log
	For UNIX or Linux:
	/opt/IBM/TPC/device/log

Common agent For Windows: C:\Program Files\IBM\TPC\ca\logs For UNIX or Linux: /opt/IBM/TPC/ca/logs For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log Data agent For Windows: C:\Program Files\IBM\TPC\ca\subagents\TPC\Data\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC\Data/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log Fabric agent For Windows: C:\Program Files\IBM\TPC\ca\subagents\TPC\Fabric\log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log Fabric agent For Windows: C:\Program Files\IBM\TPC\ca\subagents\TPC\Fabric\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC\Fabric/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log GUI For Windows: C:\Program Files\IBM\TPC\ca\subagents/TPC\Fabric/log For UNIX or Linux: /opt/IBM/TPC/gui\log For UNIX or Linux: /opt/IBM/TPC/gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log Database schema For Windows: C:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema\log	Component	Log file location
For Windows:         c:\Program Files\IBM\TPC\ca\logs         For UNIX or Linux:         /opt/IBM/TPC/ca/logs         For agent on Virtual I/O Server (see note):         /home/padmin/agentInstall.log         Data agent         For Windows:         c:\Program Files\IBM\TPC\ca\subagents\TPC\Data\log         For UNIX or Linux:         /opt/IBM/TPC/ca/subagents/TPC\Data\log         For agent on Virtual I/O Server (see note):         /home/padmin/agentInstall.log         Fabric agent         For Windows:         c:\Program Files\IBM\TPC\ca\subagents/TPC\Fabric\log         For UNIX or Linux:         /opt/IBM/TPC/ca/subagents/TPC\Fabric\log         For UNIX or Linux:         /opt/IBM/TPC/ca/subagents/TPC\Fabric\log         For agent on Virtual I/O Server (see note):         /home/padmin/agentInstall.log         GUI         For Windows:         c:\Program Files\IBM\TPC\gui\log         For UNIX or Linux:         /opt/IBM/TPC/gui/log         Database schema         For Windows:         c:\Program Files\IBM\TPC\dbschema\log         For UNIX or Linux:         /opt/IBM/TPC/dbschema/log	Common agent	
c:\Program Files\IBM\TPC\ca\logs For UNIX or Linux: /opt/IBM/TPC/ca/logs For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log Data agent For Windows: c:\Program Files\IBM\TPC\ca\subagents\TPC\Data\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC/Data/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log Fabric agent For Windows: c:\Program Files\IBM\TPC\ca\subagents\TPC\Fabric\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC/Fabric/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log GUI For Windows: c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log Database schema For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema\log		For Windows:
For UNIX or Linux: /opt/IBM/TPC/ca/logs         For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log         Data agent         For Windows: c:\Program Files\IBM\TPC\ca\subagents\TPC\Data\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC/Data/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log         Fabric agent         For Windows: c:\Program Files\IBM\TPC\ca\subagents\TPC\Fabric\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC\Fabric/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log         GUI         GUI         For Windows: c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log         GUI         For Windows: c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log         Database schema         For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema\log		c:\Program Files\IBM\TPC\ca\logs
/opt/IBM/TPC/ca/logs For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log Data agent For Windows: c:\Program Files\IBM\TPC\ca\subagents\TPC\Data\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC/Data/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log Fabric agent For Windows: c:\Program Files\IBM\TPC\ca\subagents\TPC\Fabric\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC/Fabric/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log GUI GUI For Windows: c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log Database schema For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema\log		For UNIX or Linux:
For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log         Data agent         For Windows: c:\Program Files\IBM\TPC\ca\subagents\TPC\Data\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC/Data/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log         Fabric agent         For Windows: c:\Program Files\IBM\TPC\ca\subagents\TPC\Fabric\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents\TPC\Fabric/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log         GUI         For Windows: c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log         GUI         For Windows: c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log         Database schema         For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC\dbschema\log		/opt/IBM/TPC/ca/logs
/home/padmin/agentInstall.log Data agent For Windows: c:\Program Files\IBM\TPC\ca\subagents\TPC\Data\log For UNIX or Linux: //opt/IBM/TPC/ca/subagents/TPC/Data/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log Fabric agent Fabric agent For Windows: c:\Program Files\IBM\TPC\ca\subagents\TPC\Fabric\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC/Fabric/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log GUI GUI GUI For Windows: c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log Database schema For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema\log		For agent on Virtual I/O Server (see note):
Data agent For Windows: c:\Program Files\IBM\TPC\ca\subagents\TPC\Data\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC/Data/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log Fabric agent For Windows: c:\Program Files\IBM\TPC\ca\subagents\TPC\Fabric\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC/Fabric/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log GUI GUI For Windows: c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log Database schema For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema/log For UNIX or LinuX		/home/padmin/agentInstall.log
For Windows: c:\Program Files\IBM\TPC\ca\subagents\TPC\Data\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC/Data/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log Fabric agent For Windows: c:\Program Files\IBM\TPC\ca\subagents\TPC\Fabric\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC/Fabric/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log GUI GUI For Windows: c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log Database schema For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC\dbschema\log	Data agent	
c:\Program Files\IBM\TPC\ca\subagents\TPC\Data\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC/Data/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log Fabric agent For Windows: c:\Program Files\IBM\TPC\ca\subagents\TPC\Fabric\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC/Fabric/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log GUI For Windows: c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log Database schema For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC\dbschema\log		For Windows:
For UNIX or Linux:         /opt/IBM/TPC/ca/subagents/TPC/Data/log         For agent on Virtual I/O Server (see note):         /home/padmin/agentInstall.log         Fabric agent         For Windows:         c:\Program Files\IBM\TPC\ca\subagents\TPC\Fabric\log         For UNIX or Linux:         /opt/IBM/TPC/ca/subagents/TPC/Fabric/log         For agent on Virtual I/O Server (see note):         /home/padmin/agentInstall.log         GUI         For Windows:         c:\Program Files\IBM\TPC\gui\log         For UNIX or Linux:         /opt/IBM/TPC/gui/log         For UNIX or Linux:         /opt/IBM/TPC/gui/log         Database schema         For Windows:         c:\Program Files\IBM\TPC\dbschema\log         For UNIX or Linux:         /opt/IBM/TPC/dbschema\log         For UNIX or Linux:         /opt/IBM/TPC/dbschema/log		c:\Program Files\IBM\TPC\ca\subagents\TPC\Data\log
/opt/IBM/TPC/ca/subagents/TPC/Data/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log Fabric agent For Windows: c:\Program Files\IBM\TPC\ca\subagents\TPC\Fabric\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC/Fabric/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log GUI GUI For Windows: c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log Database schema For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema\log		For UNIX or Linux:
For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log         Fabric agent         For Windows: c:\Program Files\IBM\TPC\ca\subagents\TPC\Fabric\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC/Fabric/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log         GUI         For Windows: c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log         Database schema         For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema\log         For UNIX or Linux: /opt/IBM/TPC/dbschema\log		/opt/IBM/TPC/ca/subagents/TPC/Data/log
/home/padmin/agentInstall.log Fabric agent For Windows: c:\Program Files\IBM\TPC\ca\subagents\TPC\Fabric\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC/Fabric/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log GUI For Windows: c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log Database schema For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema\log		For agent on Virtual I/O Server (see note):
Fabric agent For Windows: c:\Program Files\IBM\TPC\ca\subagents\TPC\Fabric\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC/Fabric/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log GUI  GUI For Windows: c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log Database schema For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC\dbschema\log		/home/padmin/agentInstall.log
For Windows: c:\Program Files\IBM\TPC\ca\subagents\TPC\Fabric\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC/Fabric/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log GUI GUI For Windows: c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log Database schema For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema/log	Fabric agent	
c:\Program Files\IBM\TPC\ca\subagents\TPC\Fabric\log For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC/Fabric/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log GUI For Windows: c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log Database schema For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema/log		For Windows:
For UNIX or Linux: /opt/IBM/TPC/ca/subagents/TPC/Fabric/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log GUI For Windows:		c:\Program Files\IBM\TPC\ca\subagents\TPC\Fabric\log
/opt/IBM/TPC/ca/subagents/TPC/Fabric/log For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log GUI For Windows: c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log Database schema For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema\log		For UNIX or Linux:
For agent on Virtual I/O Server (see note): /home/padmin/agentInstall.log GUI For Windows: c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log Database schema For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema/log		/opt/IBM/TPC/ca/subagents/TPC/Fabric/log
/home/padmin/agentInstall.log GUI For Windows: c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log Database schema For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema/log		For agent on Virtual I/O Server (see note):
GUI For Windows: c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log Database schema For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema/log		/home/padmin/agentInstall.log
For Windows: c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log Database schema For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema/log	GUI	
c:\Program Files\IBM\TPC\gui\log For UNIX or Linux: /opt/IBM/TPC/gui/log Database schema For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema/log		For Windows:
For UNIX or Linux: /opt/IBM/TPC/gui/log Database schema For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema/log		c:\Program Files\IBM\TPC\gui\log
/opt/IBM/TPC/gui/log Database schema For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema/log		For UNIX or Linux:
Database schema For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema/log		/opt/IBM/TPC/gui/log
For Windows: c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema/log	Database schema	
c:\Program Files\IBM\TPC\dbschema\log For UNIX or Linux: /opt/IBM/TPC/dbschema/log		For Windows:
For UNIX or Linux: /opt/IBM/TPC/dbschema/log		c:\Program Files\IBM\TPC\dbschema\log
/opt/IBM/TPC/dbschema/log		For UNIX or Linux:
		/opt/IBM/TPC/dbschema/log

Table 45. Default log file locations for IBM Tivoli Storage Productivity Center components (continued)

Note: The agentInstall.log file is composed of these log files:

# TPC.log

This log is created by InstallShield.

log.txt This log is created by InstallShield.

### installStatus.log

Shows the Data agent installation status.

#### dataAgentInstall.log

The Data agent installation log.

### fabricAgentInstallIS.log

The Fabric agent installation log.

## install.status

Installation status of the Fabric agent installation.

#### agentInstall.log

The Common agent installation log.

#### epInstallStatus.log

The Common agent installation status.

#### msgAgent.log

The Common agent runtime log.

# Agent Manager log files

Agent Manager log files give important information about an installation, uninstallation, and so forth.

Agent Manager log files can be found in the following locations:

Table 46. Agent Manager Log file locations

Agent Manager log files	Location
Installation	<agent_manager_install_dir>\logs</agent_manager_install_dir>
Uninstallation	<agent_manager_install_dir>\logs</agent_manager_install_dir>
Run-time	<agent_manager_install_dir>\AppServer\agentmanager\logs\ AgentManager</agent_manager_install_dir>

# Agent Manager installation log files

Log files are created when you install Agent Manager.

The log files generated during the installation and initial configuration of the Agent Manager are located in the <Agent\_Manager\_install\_dir>\logs directory. The following table lists the logs.

Description Log File am\_install.log InstallShield MultiPlatform (ISMP) log for the installation of the Agent Manager. Check this log first to verify that the Agent Manager installed properly and the Agent Manager server is started. AMReturnValues.log Summary of return values of the steps of the Agent Manager installation. Information about whether a new installation was performed or an existing version of am\_upgrade.log the Agent Manager was found on the system and upgraded. auth\_stdout.log Standard output and standard error logs for the AuthXMLUpdate program. auth\_stderr.log certGen\_stdout.log Standard output and standard error logs for the generation of the root certificate for certGen\_stderr.log the Agent Manager certificate authority. datastore.out Log of the Data Definition Language (DDL) script that creates and initializes the registry database. datastore\_stdout.log Standard output and standard error logs for creating and initializing the tables in the datastore\_stderr.log registry database. ds\_install.log An ISMP log for installing the files necessary to create the registry database. db\_stdout.log db\_stderr.log Standard output and standard error logs for the creation of the registry database. encrypt\_stdout.logencrypt\_ Standard output and standard error logs for the EncryptAMProps program. stderr.log guid\_install.logguid\_stdout. Standard output and standard error logs for installing the Tivoli globally unique logguid\_stderr.log globally unique identifier (GUID). Messages and trace information generated during the installation and configuration of msg\_EPM\_Install.log trace\_EPM\_Install.log the Agent Manager applications in WebSphere Application Server. serverStatus\_out.log Standard output and standard error logs for starting the application server for the serverStatus\_err.log Agent Manager.

Table 47. Agent Manager installation log files

Table 47. Agent Manager installation log files (continued)

Log File	Description
startserver_stdout.log startserver_stderr.log	Standard output and standard error logs for starting the Agent Manager server under WebSphere.
jacl/amApp_out.log jacl/amApp_err.log	Standard output and standard error logs generated while installing the AgentManager and AgentRecoveryService applications and .WAR files. These logs are generated by the EPMInstallApp.jacl configuration script.
jacl/appServer_out.log jacl/appServer_err.log	Standard output and standard error logs generated while installing the application server for the Agent Manager. These logs are generated by the EPMAppServer.jacl script.
jacl/checkcell_out.log jacl/checkcell_err.log	Standard output and standard error logs for verifying the cell for the WebSphere configuration. These logs are generated by the EPMValidate.jacl script.
jacl/checknode_out.log jacl/checknode_err.log	Standard output and standard error logs for verifying the node for the WebSphere configuration. These logs are generated by the EPMValidate.jacl script.
jacl/jdbc_out.log jacl/jdbc_err.log	Standard output and standard error logs for the configuration of the WebSphere JDBC provider, data source, and J2C Authentication Data Entry. These logs are generated by the EPMJdbcProvider.jacl script.
jacl/ssl_out.log jacl/ssl_err.log	Standard output and standard error logs for the SSL configuration. These logs are generated by the EPMSSLConfig.jacl script.
jacl/virHost_out.log jacl/virHost_err.log	Standard output and standard error logs for creating the WebSphere virtual host. These logs are generated by the EPMVirtualHost.jacl script.

# Agent Manager uninstallation log files

Log files are created when you uninstall Agent Manager.

The log files generated when you uninstall the Agent Manager are located in the <Agent\_Manager\_install\_dir>\logs directory. The following table lists the logs that are created.

Table 48. Agent Manager uninstallation log files

Log File	Description
uninstall.log	InstallShield MultiPlatform (ISMP) log for uninstalling the Agent Manager.
AMUninstallReturn Values.log	Summary of return values of the steps of the Agent Manager uninstallation.
msg_EPM_Install.logtrace_ EPM_Install.log	Messages and trace information that is generated when uninstalling the Agent Manager applications in WebSphere Application Server.

# Agent Manager run-time log files

The run-time logs for the Agent Manager are located in the <Agent\_Manager\_install\_dir>\embedded\logs\<app\_server\_name> directory, where <app\_server\_name> is the name of the application server. By default, this is Agent Manager.

## Run-time Agent Manager-specific WebSphere log files

The run-time logs for the Agent Manager-specific WebSphere logs are located in the <Agent\_Manager\_install\_dir>\embedded\logs\AgentManager directory.

# Troubleshooting descriptions and solutions

This section provides information about troubleshooting topics for IBM Tivoli Storage Productivity Center problems.

For more information about troubleshooting, see *IBM Tivoli Storage Productivity Center Problem Determination Guide*.

# **General troubleshooting**

Use this section to troubleshoot and resolve problems with the IBM Tivoli Storage Productivity Center GUI.

# Unsuccessful probe in Create Volumes or Create Virtual Disk wizard

This error occurs in the Create Volumes and Create Virtual Disk wizards (depending on device type).

# Problem

When you attempt to launch either the Create Volumes or Create Virtual Disk wizard (depending on the device type) for a device that has not had a successful probe, you will see this error message:

HWN020002E Mandatory parameter PortIDs missing

When you click **OK** on the error dialog, you cannot proceed with the Create wizard because the information gathered by the probe is needed to populate the widgets in the wizard.

## Action

You must cancel out of the Create wizard, then create and schedule a probe for the device or devices. When the probe completes successfully, then you will be able to launch the Create Volumes or Create Virtual Disks wizard. If the probe fails, you will not be able to create the volumes or vdisks.

# Alerts are not triggered for some fabric groups

When you define a switch alert, endpoint device alert, or fabric alert for a group of entities, and an entity is later added to that group, IBM Tivoli Storage Productivity Center does not generate an alert for the entity that was added to the group after the alert was defined.

## Problem

For example, use the **Fabric Manager** > **Monitoring** > **Groups** > **Fabric** node to define a group of fabrics in your environment. Use Fabric Manager > Alerting > Endpoint Device Alerts to define an alert that is triggered when an Endpoint State Change condition is detected within a fabric. If a node is later added to that fabric, no Endpoint State Change alerts will ever be triggered for that node.

## Action

To workaround this issue, we recommend that you create fabric alerts, switch alerts, and endpoint alerts with the option of **All** *<entities>*, where *<entities>* is the type of entity for an alert. Consider the following examples:

- Example 1: Define a Fabric Manager > Alerting > Switch Alert for a Switch State Change condition. Click the **Switches** tab to view a list of switches. To avoid this problem, we recommend that you select the **All Switches** option under the **Switches** node rather than selecting any of the fabrics shown under the **Switches in Fabric** node.
- Example 2: Define a Fabric Manager > Alerting > Endpoint Device Alert for an Endpoint State Change condition. Click the **Endpoint Devices** tab to view a list of endpoint devices. To avoid this problem, we recommend that you select the **All Endpoint Devices** option under the **Endpoint Devices** node rather selecting a fabric from under the **Endpoint Device Groups** node.
- Example 3: Define a Fabric Manager > Alerting > Fabric Alert for a Zone State Change condition. Click the **Fabrics** tab to view a list of fabrics. To avoid this problem, we recommend that you select the **All Zones** option under the **Zones** node rather selecting options under the **Fabrics** or **Zone Sets** nodes.

## Fabric probe fails

This error occurs when a fabric probe fails because it can no longer interact with an inband fabric agent.

#### Problem

The following message appears in the job log of the fabric probe that failed. The IP address and port shown in this error message reflects the IP address and port of the system where the inband fabric agent is installed (in this example, 10.10.21:9510 represents that system):

2008-04-10 22:48:57.034+01:00 BTAQE1107E InbandScanHandler failed to start InbandScanner AttributePEOnly on managed host 10.10.10.21:9510. com.ibm.tpc.discovery.tsanm.InbandScanner run 2008-04-10 22:48:57.034+01:00 java.lang.NullPointerException at com.ibm.pvcws.wsdlgleaner.WSDLGleaner\$OSGIURL.openStream(WSDLGleaner.java:368) at com.ibm.pvcws.wsdlgleaner.WSDLGleaner.glean(WSDLGleaner.java:55) at com.ibm.pvcws.proxy.wsj2me.WSDLProxy.<init>(WSDLProxy.java:48) at com.ibm.pvcws.proxy.wsj2me.WSDLProxy.getProxy(WSDLProxy.java:41) at com.tivoli.agent.connector.client.WebServiceProxyFactory.getProxy (WebServiceProxyFactory.java:41) at com.tivoli.agent.connector.client.OSGIServiceProxyFactory.getProxy (OSGIServiceProxyFactory.java:81) at com.tivoli.sanmgmt.middleware.data.OSGiServiceProxy.init (OSGiServiceProxy.java:116) at com.tivoli.sanmgmt.middleware.data.OSGiServiceProxy.invoke (OSGiServiceProxy.java:91) at \$Proxy10.invoke(Unknown Source)

at com.ibm.tpc.discovery.tsanm.InbandScanner.run(InbandScanner.java:158) com.ibm.tpc.discovery.tsanm.InbandScanner run

You can view the job log for a fabric probe in the user interface. To do this, expand the **IBM Tivoli Storage Productivity Center**> **Monitoring** > **Probes** > *probe\_name* node in the navigation tree and click the appropriate job run. The log for that job run is displayed in the content pane.

This problem occurs when the certificates used by the Agent Manager are not synchronized with the certificates of your agent installation. Typically, this happens when Agent Manager is reinstalled, but the agents themselves are not changed.

When you view the status of that inband agent in the Tivoli Storage Productivity Center user interface, it still appears as **Active** because the Agent Manager can ping the agent. However, when the Agent Manager tries to establish a connection (through an inband fabric probe), that connection is refused.

You can also check the msgAgent.log (Common agent) log file to view the messages generated for this error. The IP address in the log file reflects the IP address of the system where the Device server is installed (in this example, 10.0.2.2 represents that system):

2008.04.10 22:37:20.333+02:00 BTC4045E Rejected connection attempt from 10.0.2.2. 2008.04.10 22:52:57.240+02:00 BTC4045E Rejected connection attempt from 10.0.2.2. 2008.04.10 22:52:57.246+02:00 BTC4045E Rejected connection attempt from 10.0.2.2. 2008.04.10 22:53:00.084+02:00 BTC4045E Rejected connection attempt from 10.0.2.2. 2008.04.10 22:53:00.090+02:00 BTC4045E Rejected connection attempt from 10.0.2.2.

msgAgent.log is located in the following default directories on the system where the agent is installed:

- Windows: c:\Program Files\IBM\TPC\ca\logs
- UNIX/Linux: /<usr or opt>/IBM/TPC/ca/logs

## Action

Perform the following steps to resolve the problem:

- 1. Log on to the system where the Common agent is located (in the example previously cited, 10.10.10.21 represents that system):
- 2. Navigate to the Common agent installation directory. The default installation directories are:
  - Windows: C:\Program Files\IBM\TPC\ca
  - UNIX/Linux: /<usr or opt>/IBM/TPC/ca
- **3**. Delete the contents of the /cert directory. This directory usually contains the following four files: agentKeys.jks, agentTrust.jks, pwd, and CertificateRevocationList. When you delete these files, the Common agent re-registers with the Agent Manager and retrieves the certificate files needed for proper communication with the Agent Manager.
- 4. Restart the Common agent. To do this, start a command prompt and run the following commands:
  - Windows: c:\Program Files\IBM\TPC\ca\endpoint.bat restart
  - UNIX/Linux: /<usr or opt>/IBM/TPC/ca/endpoint.sh restart

## Cluster resource group alerts are not triggered

This problem can occur on systems running High Availability Cluster Multi-Processing (HACMP) or Microsoft Cluster Server (MSCS).

## Problem

A computer alert is defined that uses one of the following triggering conditions:

- Cluster Resource Group Added
- Cluster Resource Group Removed
- Cluster Resource Group Moved

The event occurs, but no alert is triggered.

## Action

The Data agent checks to find out whether it is running in an HACMP or MSCS cluster at the following times:

- When the Data agent is started
- When a probe is run

If the HACMP or MSCS service is started after the Data agent, the agent is not aware of the cluster. Any cluster resource group alerts that you might have defined cannot be triggered.

To solve this problem, run a probe on one of the cluster nodes.

## Error message: No saved IP addresses could be found

This message is displayed if no base IP addresses have been specified for the SNMP address scan.

#### Problem

If no base IP addresses have been specified for the SNMP address scan in the out-of-band fabric discovery options, you will see this pop-up panel when you run an out-of-band fabric discovery job.

#### Action

The pop-up panel asks "Do you wish to continue with this discovery"? Click **Yes** to continue. This will run discovery for any IP addresses in the out-of-band Fabric agent list.

## Topology viewer queries fail with SQLCODE -101

This message is displayed when the topology viewer queries fail.

### Problem

The global DB2 variable (DB2\_REDUCED\_OPTIMIZATION) is set when IBM Tivoli Storage Productivity Center is installed or upgraded. This flag helps reduce time and resources spent on optimizing SQL queries during compilation. (For detailed information on this environment variable, see the DB2 Information Center under **Reference -> Registry and environment variables -> SQL compiler**.) Note that this flag affects all databases in the DBMS, and it also requires a DB2 restart to take effect. If the SQL -101 exception occurs, restart DB2 to make sure that the DB2\_REDUCED\_OPTIMIZATION variable has taken effect since Tivoli Storage Productivity Center was installed or upgraded.

## Action

If you do not want to use this flag in your environment, you may disable it and use an alternative solution for Tivoli Storage Productivity Center. To disable the flag, you must use the **db2set** command and restart DB2 so that changes can take effect. On the DB2 server, run this command: db2set DB2 REDUCED OPTIMIZATION=N

An alternative solution allows Tivoli Storage Productivity Center to temporarily reduce the compile-time optimization level of the SQL queries used in the topology viewer. This is done in real time and does not require DB2 restarts or Tivoli Storage Productivity Center server restarts. The default optimization level for the topology viewer can be retrieved and set through the Tivoli Storage Productivity Center CLI. To retrieve the optimization level, on the Tivoli Storage Productivity Center server, run this command:

tpctool getdscfg -user <user\_ID> -pwd <password>
-url localhost:9550 -property topo.query.optlevel

Where <user\_ID> and <password> are filled in appropriately.

The default optimization level is initially 5. Try setting this level to 2 and check if the SQL 101 exception occurs. You can furthermore lower the optimization level to 1 and 0 if the SQL -101 exception still occurs or if the topology viewer performance is slow. However, it is advisable to keep the optimization level as high as possible, as long as the SQL -101 exception is not seen and the topology viewer performance is good. To set the optimization level to X, run the following command:

```
tpctool setdscfg -user <user_ID> -pwd <password>
-url localhost:9550 -property topo.query.optlevel <x>
```

Where <user\_ID>, <password>, and <x> are filled in appropriately.

Note that this setting is local to the Tivoli Storage Productivity Center database and only affects queries in the topology viewer portion of Tivoli Storage Productivity Center.

# Slow performance when moving data from the database repository

Repocopy and other DB2 movement utilities might perform slowly or be in a wait state when moving data from the IBM Tivoli Storage Productivity Center database repository.

## Problem

The Tivoli Storage Productivity Center user interface, repocopy tool, or DB2 data movement utilities might be in a wait state or perform poorly when you attempt to move data from the database repository while running discovery, probe, scan, and performance monitor jobs at the same time.

# Action

Use the repocopy tool or DB2 data movement utilities to migrate data in the database repository during times when discovery, probe, scan, and performance monitoring jobs are not running or are scheduled to run.

# Error message when running repocopy on server that uses remote database

This error occurs when you run **repocopy** on a server machine that uses a remote database.

# Problem

You see these error messages when you run **repocopy** on a server machine that uses a remote database:

This application has failed to start because DB2APP.dll was not found. Re-installing the application may fix this problem.

```
Import/Export: Can't find library TSRMinsudb (TSRMinsudb.dll)
in <library_path> or java.library.path
<library_path>
<java_library_path>
```

# Action

Click **OK** to both messages.

# Using the VNC client with the minimap in the topology viewer

This condition occurs when you use the VNC client with the minimap in the topology viewer.

#### Problem

When you use the VNC client with 65 colors and use the minimap in the topology viewer, the colors in the minimap may not be distinguishable. This can lead to confusion about whether the minimap is working. This is only a visual aspect that is due to the VNC configuration.

#### Action

The minimap works correctly in the topology viewer. Use your VNC connection with Medium (256 colors) or Full (All available Colors) setting.

#### Chart and report values differ

This condition occurs when you use the charting and reporting functions of IBM Tivoli Storage Productivity Center.

### Problem

The following reports (listed below) show the capacity of a storage subsystem without counting certain flagged disks (like spare disks), whereas all the other Tivoli Storage Productivity Center reports include these flagged disks when calculating capacity. Also, the capacity history charts from these reports include these flagged disks, causing a discrepancy between the number seen in the report and the chart. The reports are:

```
Data Manager > Reporting > Capacity > DiskCapacity > By Storage
Subsystem
```

```
Data Manager > Reporting > Capacity > DiskCapacity > By Storage
Subsystem Group
```

```
Asset > System-Wide > Storage Subsystem > By Storage Subsystem
Asset > System-Wide > Storage Subsystem > By Capacity
```

## Action

Understand that the chart and report values differ.

## Computer probe fails for an HP machine

This condition occurs when you use the charting and reporting functions of IBM Tivoli Storage Productivity Center.

### **Problem**

A computer probe fails for an HP machine with the following error messages:

```
STA0123E: Controller not found for disk
GEN0131E: Unable to open file /etc/hba.conf
GEN6013E: OS Error 0; Error 0.
```

#### Action

The Data agent is trying to locate the common HBA API library in the etc/hba.conf file, but it is not found. Check to see that the HBA is loaded on the HP/UX machine.

# Message: "Sending results to server" and probe job hangs

This condition occurs when you run a probe job for the Data agent, if there is a communication error between the server and agent, or if the server is "unreachable".

## Problem

The job log displays "Sending results to server" and then the job seems to freeze for several hours. This can occur for the following reasons:

- There is a communication error between the server and agent.
- The server is in an "unreachable" state or if the server is too busy to accept probe job results.

## Action

If the problem occurs for a probe job with a Data agent, change the Data agent's agent.config file. Add the following parameter: patienceWithServer=<minutes>

Set this to the number of minutes you want the agent to wait before trying to contact the server again. Then open the Tivoli Storage Productivity Center GUI. Click **Administrative Services > Data Sources > Data Agents**. Click your agent and then press the **Read Config** button. The default is 240 minutes (4 hours).

Wait for the current probe to finish and rerun the computer probe when the server is less busy or communication has been restored.

If the problem occurs because of a communication error or the server is "unreachable", a restart of the server may be necessary.

# Swap space in Data Manager and rollup reports varies

This condition occurs when you display Data Manager and Rollup Reports swap space.

## Problem

The **Data Manager** and **Rollup Reports > Asset > Computer > By Computer** reports show up the wrong swap values for Windows machines. The swap space shows up correctly on some machines while on others, it is a little less.

## Action

Understand the problem as stated here.

# Cannot collect logs from the service tool

This error occurs when using the **service** tool.

# Problem

You cannot get the logs from the service tool.

# Action

When you install a remote Data agent or Fabric agent and want to collect service logs for them, you must run the **service** tool from the remote agent machine from this directory:

```
<common_agent_install_dir>\subagents\TPC\service
```

For example, if you used the default directory on UNIX or Linux, the directory path would be:

/opt/IBM/TPC/ca/subagents/TPC/service

The **service** tool is installed in several locations but you should only run the tool from the remote machine directory listed above.

# The Data Server service fails with a logon failure when restarted

This error occurs when using Window's Active Directory domain policy.

# Problem

When you restart the machine, the TSRMsrv1 user ID is no longer in the administrator's group and cannot log in to the machine. If there is a domain policy established that defined which users would be in the "Administrators" group, local users are automatically removed from the "Administrators" group when the system is restarted if the user ID is not one of the named accounts.

# Action

Make sure that the user ID is one of the named accounts in the domain policy.

# Specifying a LUN ID for the assignvol command

This error occurs when specifying a LUN ID for the assignvol command.

# Problem

When specifying a LUN ID for the **assignvol** command, the LUN ID value will not be taken into consideration for the DS8000, DS6000, and Tivoli Storage Enterprise Storage Server storage devices. The reason for this is because the CIMOM does not offer support for client selectable LUN IDs.

## Action

Understand the problem as described here.

# GUI panels do not automatically refresh

This condition occurs when you make a change in the IBM Tivoli Storage Productivity Center GUI.

# Problem

Most of the non-topology panels in Tivoli Storage Productivity Center do not automatically refresh after a change has been made.
After you make a change in the Tivoli Storage Productivity Center GUI, click **Refresh**. Some panels may not refresh after you click **Refresh**. In these instances, close and open the panel again.

The topology viewer refreshes the panels after a change has been made under these conditions:

- Automatic periodic refreshing: the default is once every 5 minutes. You can change this setting by right-clicking in the topology viewer. The Refresh Rate Setting dialog is displayed. Enter the minutes you want the topology viewer to refresh and click **OK**.
- You can manually refresh the topology view by right-clicking in the topology viewer. Click **Refresh View**.

# Cannot monitor an EMC CIMOM on a Solaris server

This condition occurs when you try to monitor a Pegasus-based CIMOM like the EMC CIMOM.

### Problem

When trying to log into a Pegasus-based CIMOM like the EMC CIMOM on a Solaris server, a login error is returned. If you are unable to log in, this could be a result of having the operating system language locale improperly set or not set at all. Check to see that the operating system language locale is properly set.

### Action

An example of a properly set language locale for a Solaris server is found in the /etc/default/init file. This file contains the lines below which are dependent on the geographical location.

TZ=US/Arizona CMASK=022 LC\_COLLATE=en\_US.IS08859-1 LC\_CTYPE=en\_US.IS08859-1 LC\_MESSAGES=C LC\_MONETARY=en\_US.IS08859-1 LC\_NUMERIC=en\_US.IS08859-1

Incorrect entries are LC lines with incorrect locale entries or the LC language locale lines are missing.

## Disk reporting under port adapter is incorrect

This error occurs when viewing the fibre channel LUNs through disk reporting under **Disk Manager > Reporting > Storage Subsystem > Computer Views > By computer**.

## Problem

The HBA incorrectly identifies SCSI adapters instead of fibre channel adapters. This problem occurs when there is an incorrect HBA configuration setup for Solaris and Windows systems. You can identify this problem when you set a trace for the Data agent to see if the HBA API is being invoked during a probe of the Data agent. The probe is used to determine the port node WWN of the HBA adapter port and the port node WWN of the target ports of the volumes.

**SUN Solaris system:** the /etc/hba.conf file does not point to the correct vendor HBA API library.

If a QLogic HBA API library is configured in the /etc/hba.conf file, a bad configuration would appear as: q12x00 libqlsdm.so

A good configuration would appear as: ql2x00 /usr/lib/libqlsdm.so

Windows system: this library is identified using the registry value at: HKEY LOCAL MACHINE/SOFTWARE/SNIA/HBA/<vendor name>

Using QLogic as an example, the registry location would be: HKEY LOCAL MACHINE/SOFTWARE/SNIA/HBA/QL2X00

In the registry, the Library File key is the fully qualified name of the dll. Ensure that the \*.dll file is located in the directory specified in the Library File key.

An example of a correct QLogic configuration, the Library File key is: C:\Program Files\QLogic Corporation\SANsurfer\ql2xhai2.dll

### Action

Install the HBA drivers with the SNIA HBA API which is included in the HBA driver package.

# SQLCODE-440 displayed if install IBM Tivoli Storage Productivity Center on system with bad system clock

This error occurs when you install IBM Tivoli Storage Productivity Center on a system with a clock that is set for a future time and not the current time.

#### Problem

You receive this DB2 error message when you try to open the topology view for the fabric:

com.ibm.db2.jcc.c.SqlException: DB2 SQL error: SQLCODE: -440, SQLSTATE: 42884, SQLERRMC: RTRIM;FUNCTION

#### Action

Correct the system clock and restart the Tivoli Storage Productivity Center services.

## Chart legend does not display all items in chart

This error occurs when you select the batch charting option and multiple charts per series.

For example, if you perform these steps and generate an HTML chart of the batch report, not all of the file systems will appear in the legend:

- 1. Expand **IBM Tivoli Storage Productivity Center > My Reports** in the navigation tree.
- 2. Right-click Batch Reports and select Create Batch Report.
- 3. Select Capacity > Filesystem Used Space > By Filesystem on the Report page.
- 4. Click the Options tab, select HTML Chart, and click Customize this chart.
- 5. Select 2 in the Maximum number of charts or series per screen field.
- 6. Select Bar Chart.
- 7. Select Vertical.

# Action

Understand the problem as described here.

# The PDF chart batch report displays a corrupted PDF chart

This error occurs when you display a PDF chart batch report.

# Problem

The PDF chart batch report for a set of data with a high degree of difference between the data sets (for example, **Usage > Files >File Size Distribution > By Computer**) results in a PDF file with a corrupted chart (a big block of color blocks some of the chart). The online version of the same report looks fine, as does the HTML chart batch report version. Only the PDF chart batch report version displays incorrectly.

## Action

Do not use the PDF chart batch reporting for the report.

# Cannot edit or delete probe; missing CIM agent or subsystem

This error occurs when you try to edit or delete a probe job after a CIM agent or storage subsystem has been deleted.

# Problem

After you run a probe job for a storage subsystem, and then delete that storage subsystem or CIM agent, you will not be able to edit or delete that probe job. This problem only occurs when the deleted subsystem is the only device for the probe job. If the probe job has multiple subsystems selected, then the deleted subsystem will be removed from this probe definition.

# Action

Because there is no auto-refresh for the probe jobs, manually refresh the probe job list to see if the job has been removed from the list. On the Navigation tree, click **IBM Tivoli Storage Productivity Center > Monitoring > Probes**. Right-click on **Probes**. Click **Refresh**.

# A hypervisor probe fails after deleting an assigned LUN

A hypervisor probe fails after deleting an assigned LUN.

This problem occurs after a IBM Tivoli Storage Productivity Center probe is performed for an ESX Server.

## Action

Rescan the disks for the ESX Server, then run the Tivoli Storage Productivity Center probe again.

# Duplicate entries in list of switches

This problem is seen on the Create Switch Alerts panel.

# Problem

On the **Create Switch Alerts** panel, Switches tab, the list of switches shows duplicate entries. The list of switches in the Create Switch Alerts panel are listed by the display name. However, if the display name is null, the logical name is used instead. If you have multiple switches with duplicate display names or duplicate logical names (if the display names are null), you will see duplicate entries in this panel.

# Action

Ensure that you have unique display names and logical names for your switches.

# Statistics are zero or blank for a computer in the data path explorer view

This problem occurs when using the data path explorer view in the topology viewer.

# Problem

This problem occurs with separate switches that are part of the same fabric, and you are using only out-of-band Fabric agents to discover entities.

# Action

Topology information is only gathered for the switch added as an out-of-band Fabric agent. The agent will not be able to gather the topology information for any connected switches unless they are also defined as out-of-band Fabric agents. If you are performing out-of-band discovery only on a fabric with several switches, you must install an out-of-band Fabric agent for each switch in the fabric to discover the whole fabric.

# Reports for Data Manager for Databases is incorrect

This problem occurs when viewing reports for Data Manager for Databases.

# Problem

When viewing usage reports for DB2 databases, the used size might show N/A.

## Action

If this is the case, rerun the scan job for Data Manager for Databases with the option "Perform runstats on all tables being scanned."

# Java Web Start and IPv6

This problem occurs when you use Java Web Start 1.4.2 and IPv6 to connect the IBM Tivoli Storage Productivity Center client to the server and start the GUI using Java Web Start.

## Problem

The error message Protocol Family Unavailable is issued. Java Web Start 1.4.2 does not support IPv6 addresses.

When you use Java 5 and use IPv6 addresses with Java Web Start, the error message Download Error : Exception: java.io.IOException is issued. You cannot use Java Web Start 5 without Service Release 8 for IPv6 addresses.

# Action

Install Java 5 with Service Release 8. If you use Java 5 without Service Release 8, specify a host name of the Tivoli Storage Productivity Center server that resolves to the IPv6 address and not the IPv6 address itself.

# **CIM agent operations timeout**

These errors occur for the CIM agent.

# Problem

You get the error message: HWNPM4103E CIM/OM operation timeout (30 seconds) expired.

## Action

Check whether the CIM agent is up and running. You can do this by clicking **Administrative Services** → **Agents** → **CIMOM**. Select **Test CIMOM Connection**.

# CIM agent runs slowly

This error occurs for the CIM agent.

# Problem

The CIM runs slowly.

# Action

Try stopping and restarting the IBM Tivoli Storage Productivity Center services. If this does not help, increase the value of com.ibm.tpc.perf.ConteConnectTimeOut in the following file:

<TPC\_install\_dir>\device\conf\pm.conf

# Incorrect information reported when using down-level CIM agents

This problem may occur when you are using an older version of a CIM agent with a newer version of device firmware, for example, a DS 5.2.1 CIMOM with a DS8000 R3 firmware.

The down-level CIM agent may report misleading or incorrect information if features are enabled and used with the device which have been introduced with a newer level of the firmware.

# Action

Always use the latest version of the CIM agent which corresponds to the device firmware used. For example, make sure you use a DS 5.3 CIMOM with a DS8000 running Release 3 (5.3) firmware.

# Incorrect information reported when using down-level CIM agents

This problem may occur when you are using an older version of a CIM agent with a newer version of device firmware, for example, a DS 5.2.1 CIMOM with a DS8000 R3 firmware.

# Problem

When displaying information for the CIMOM by clicking **Administrative Services** > **Data Sources** > **CIMOM Agents**, selecting a CIMOM, and then clicking **Show Managed Devices**, the IP address is not displayed for non-IBM devices in the CIMOM Managed Devices window.

# Action

Understand that the IP address will not be displayed for non-IBM devices.

# Changing password policy on Windows

If you change your system password policy, and install IBM Tivoli Storage Productivity Center, you might have to use the custom installation method.

## Problem

- You install DB2 on a server and use a db2admin password which might not conform to any system policy.
- You create a new password policy on your system.
- You install an IBM Tivoli Storage Productivity Center server on the same system.

If you install Tivoli Storage Productivity Center using typical installation, and do not provide any special password, the default user ID and password for the Common agent installation might fail in some cases if the password does not conform to the new password policy.

# Action

If this situation occurs, use the custom installation method to install Tivoli Storage Productivity Center. At the "Common agent selection panel," click **Windows service info** to provide a custom user ID and password that meets the password policy.

# Using Windows Vista for GUI display

When using the IBM Tivoli Storage Productivity Center GUI on a Windows Vista system, the scroll bars and tabs might not display well.

When using the Tivoli Storage Productivity Center GUI in a Windows Vista environment that has the look and feel set for a Windows environment, the scroll bars and tabs do not display as well in a Windows Vista display as on other Windows systems.

## Action

You can improve the display of the GUI by changing the setting in the Tivoli Storage Productivity Center GUI. On the menu bar, click **Preferences > Look and Feel**. Select **CDE/Motif** or **Metal**.

# IBM Tivoli Storage Productivity Center GUI online help does not work when launching the GUI from Java Web Start

The IBM Tivoli Storage Productivity Center GUI online help does not work when launching the GUI through Java Web Start.

### Problem

When launching the IBM Tivoli Storage Productivity Center GUI through Java Web Start (either from the Java Web Start Welcome HTML page or the IBM Tivoli Integrated Portal portlet), the help functions do not work. Clicking on the **Help** menu does not bring up the IBM Tivoli Storage Productivity Center online help.

### Action

Do not use the following versions of IBM JRE 1.5:

- 5.0 Service Release 8 (Windows / IA32)
- 5.0 Service Release 8a (Windows / IA32)

# Error message: Unable to launch Tivoli Storage Productivity Center

You receive this Java Web Start error message when you try to launch the IBM Tivoli Storage Productivity Center GUI using a URL with an IPv6 address on Windows.

## Problem

IPv6 is not supported by JRE 1.4 for Windows. IPv6 is supported by JRE 1.4 only for Solaris and Linux.

## Action

IPv6 is supported on Windows by the following releases:

- Sun JRE 1.6 or later
- IBM JRE 1.5 Service Release 8a or later

## No Refresh button for some user roles

There is no **Refresh** button on the dashboard for some IBM Tivoli Storage Productivity Center user roles.

The roles that have the **Refresh** button on the dashboard are:

- Superuser
- Productivity Center Administrator
- Data Administrator

The Refresh button is not available for the following user roles:

- Tape Operator
- Tape Administrator
- Fabric Operator
- Fabric Administrator
- Disk Operator
- Disk Administrator
- Data Operator

# Action

See the Problem description.

# Setting the default browser in AIX

This topic describes how to set the default browser in AIX.

# Problem

You cannot launch IBM Tivoli Storage Productivity Center for Replication using the default AIX browser.

# Action

To change the default browser on AIX, use SMIT:

- 1. Change to the root user.
- On a command line, enter: smit change\_documentation\_services
- This opens a SMIT panel. In the DEFAULT\_BROWSER field, enter the command that launches your new Web browser. Here is an example: /usr/bin/firefox

Click **OK**. Click **DONE** in the SMIT window. The browser change takes effect the next time that you log in to the computer.

4. If you are using a VNC server, after you set the DEFAULT\_BROWSER environment variable, you need to stop and restart the VNC server on the AIX system for the change to take effect in the VNC environment.

# Assigned LUN is not recognized by the host

A LUN assigned to a host using IBM Tivoli Storage Productivity Center is not recognized by the host, and Tivoli Storage Productivity Center does not report the error.

This problem can occur if the host connection for the selected host was incorrectly configured on the storage subsystem, and the host is unable to log in to the storage subsystem. Some examples of configuration settings that, if incorrectly configured, can cause this problem are the storage subsystem I/O port configuration (FICON/FcSf) or the OS selection.

# Action

Remove all LUNs from the storage subsystem for the selected host and delete the host connection. Recreate the host connection with the correct configuration settings, and once again assign the LUNs to the host.

# Cannot start IBM Tivoli Storage Productivity Center GUI using Java Web Start

You cannot start the IBM Tivoli Storage Productivity Center GUI using Java Web Start.

# Problem

There is a known issue when you try to start the IBM Tivoli Storage Productivity Center GUI under these conditions:

- Java Web Start is running on an AIX system.
- The AIX system has a 32-bit Java Runtime Environment installed.
- The IBM Tivoli Storage Productivity Center GUI is in the Java Web Start cache. This indicates that the GUI has been started previously using Java Web Start with HTTPS protocol. IBM Tivoli Storage Productivity Center has been launched using the HTTPS protocol from either the command line or a Web browser.

# Action

To work around this issue, you cando one of the following actions when starting the IBM Tivoli Storage Productivity Center GUI using Java Web Start on AIX:

- Use the HTTP protocol rather than the HTTPS protocol.
- If you are required to use the HTTPS protocol, clear the Java Web Start cache before starting the IBM Tivoli Storage Productivity Center GUI.

# On AIX systems, numbers in the Storage Resource agent registry are printed as formatted numbers

On AIX systems, numbers in the Storage Resource agent or configuration file are printed as formatted numbers.

# Problem

Numbers are printed in formatted format in the following Storage Resource agent registry or configuration files:

/etc/Tivoli/TSRM/registryNA
<SRA\_install\_directory>/agent/config/Agent.config

For example, instead of 9510, the number appears as 9,510. This is a known in AIX libraries. This problem occurs with a lower level C++ library (a level lower than 7.0.0.5) on the system.

Update your C++ libraries. To check your library version, run the following command:

lslpp -L | grep -i xlc

An example of the output is shown:

xlC.aix50.rte	7.0.0.3	С	F	C Set	++ Runtime for AIX 5.0
xlC.cpp	6.0.0.0	С	F	C for	AIX Preprocessor
xlC.msg.en_US.cpp	6.0.0.0	С	F	C for	AIX Preprocessor
xlC.msg.en_US.rte	7.0.0.0	С	F	C Set	++ Runtime
xlC.rte	7.0.0.1	С	F	C Set	++ Runtime

To upgrade your libraries, follow these steps:

- 1. Get the library updates. Go to http://www-933.ibm.com/support/fixcentral/.
- 2. Select the following:

Product Group	Rational
Product	XL C++ Runtime
Installed Version	8.0.0.0
Platform	AIX

- 3. Click Continue. then click Continue again.
- 4. Download the updates.

# Error message: Connection failed: SSL Handshake failed (when running probe job)

You see this error message in the agent.trace log file when you run a probe job for one of the Storage Resource agents. The IBM Tivoli Storage Productivity Center server remains in running mode without completing the probe job.

#### Problem

This situation can occur after you install the IBM Tivoli Storage Productivity Center server and deploy one or more non-daemon Storage Resource agents. You then replace the SSL communication certificates with the custom-generated certificates on the server. However, you do not replace the custom-generated certificates on the Storage Resource agents. When you run the probe job, the IBM Tivoli Storage Productivity Center server remains in running mode and the probe job does not complete. When you look at the agent.trace log file for the Storage Resource agent, you see this error message. This occurs because the certificates are not synchronized with the server and agent.

#### Action

Reinstall the Storage Resource agent using the **Force** option. The probe job will finish (with an error status, which is expected). Subsequent probe jobs will run successfully.

Error message: System error occurred (when running probe job)

You receive this error message when you run a probe job.

#### Problem

This situation can occur after you install the IBM Tivoli Storage Productivity Center server and deploy one or more daemon Storage Resource agents. You then replace the SSL communication certificates with the custom-generated certificates on the server. However, you do not replace the custom-generated certificates on the Storage Resource agents. When you perform a check operation on the Storage Resource agent, the agent status indicates a DEFECTED state. When you run a probe job for the agent, you will see this error message. This occurs because the certificates are not synchronized with the server and agent.

### Action

Reinstall the Storage Resource agent with the Force option.

# Error message: Failed to send request

You receive this error message when you try to open the **Configuration History** > **Switches** panel.

## Problem

The L0: Switches panel does not get updated (typically after a period of 30 minutes or more). Your IBM Tivoli Storage Productivity Center system might have more snapshots than it can process within the 30 minute timeout for the GUI.

## Action

Decrease the number of snapshots stored in the database. Follow these steps:

- 1. Open the IBM Tivoli Storage Productivity Center GUI.
- 2. Click **IBM Tivoli Storage Productivity Center > Administrative Services > Configuration > Configuration History Settings**.
- 3. Change the **Delete snapshots older than x days** to a lower value.
- 4. Change the **Create snapshot every x hours** to a new value, but remember the original value.
- 5. Click **Update**. After IBM Tivoli Storage Productivity Center has finished updating, the number of snapshots should decrease.
- 6. You may need to leave the **Configuration History Settings** panel and return to it to see the GUI change. Before leaving the panel, save the settings.
- 7. Change the **Create snapshot every x hours** value back to the original value (if desired).
- 8. Click Update, save your changes, and then leave the panel.

If the **Configuration History > Switches** panel still does not display properly, you might need to decrease the number of snapshots even further.

# Error message: GUI8347E

You can encounter this message when you try to start an external tool.

# Problem

You receive this error message: GUI8347E: Unable to retrieve External tools settings from repository due to following error: java.lang.NullPointerException

You can encounter this message if you try to start an external tool after you have upgraded from a previous version of Tivoli Storage Productivity Center.

To avoid this error, delete the tools.xml file from the following location on the computer where Tivoli Storage Productivity Center is installed:

- Windows: \Documents and Settings\Administrator\Application Data\IBM\TPC\config\tools.xml
- Unix: .TPC/config/tools.xml

Alternatively, you can add a new external tool. This action overwrites the old tools.xml file.

# Storage Resource agents display IP addresses instead of host names

The Storage Resource agents display IP addresses instead of host names.

# Problem

The Storage Resource agents display IP addresses instead of host names.

## Action

The Storage Resource agents installed on the systems need to be in the DNS file. If the host name does not exist in the DNS file, then they should be added to the hosts file on the IBM Tivoli Storage Productivity Center server system. The hosts file is found in the following directory:

```
/etc/hosts (for non-Windows)
<System32>\drivers\etc\hosts (for Windows)
```

# Wrong number of tables reported from a Microsoft SQL Server 2005 database

The wrong number of tables are reported by IBM Tivoli Storage Productivity Center from a Microsoft SQL Server 2005 database.

## Problem

Starting with Microsoft SQL Server 2005, the system tables are no longer available tin the Management Studio Graphical User Interface. System data is now stored in hidden "resource" tables, which can only be accessed directly by the server itself. IBM Tivoli Storage Productivity Center is able to access these tables and provide information about them, even if the user can no longer see them.

## Action

See the description under Problem.

# Database-tablespace alert not triggered for a database

The database-tablespace alert is not triggered for a database.

## Problem

A database-tablespace alert should be triggered when the following conditions occur:

- A table has less than a KB, MB, or GB.
- A table is dropped.

To get accurate alert information, here is an example of the steps to follow using a Microsoft SQL Server database:

- 1. Add the Microsoft SQL Server license.
- 2. Create a Microsoft SQL database.
- 3. Create tables in the database.
- 4. Create a Database-Tablespace group. Click Data Manager for Databases > Monitoring > Group > Databases-Tablespaces. Select the databases you want to include in this group. Save the information and close the window.
- Create a table group. Click Data Manager for Databases > Monitoring > Group > Table. Select tables by instance or instances by tables. Click the New Instance button. Make sure you specify the following information:
  - Database
  - Table creator
  - Table name

The resulting table entry should have the following format: <database\_name>.dbo.<table\_name>.

- 6. Create a Database-Tablespace alert. Click **Data Manager for Databases** > **Monitoring** > **Alerting** > **Database-Tablespace Alerts**. Make sure you select the SQL/Server RDBMS type and the Database dropped condition. Make sure you select the correct Database-Tablespace Group in the left pane (the one you created in step 4).
- Create a table alert. Click Data Manager for Databases > Monitoring > Alerting > Table Alerts. Make sure you select the SQL/Server RDBMS type and the Table dropped condition and the correct Table Group from the left pane (the one you created in step 5).
- 8. Run a probe on All Instances.
- **9**. Run a scan by selecting the correct Database-Tablespace and Table Groups (the ones created in steps 4 and 5).
- 10. Drop a database or table (one of those belonging to the groups you created).
- 11. Rerun the probe and then the scan.
- 12. The alerts should be triggered correctly.

## Fabric probe job failed

The fabric probe job failed.

#### Problem

A fabric probe job failed. Here is an example of the error messages you see in the fabric probe log:

3/13/09 12:53:32 PM BTADS0029I Scanner AttributePEOnly data from agent x.xx.xxx.sys910 has not changed since last scan. 3/13/09 12:53:33 PM BTADS0033E Error invoking AttributePEOnly on host x.xx.xxx.sys910 .

3/13/09 12:53:33 PM java.lang.reflect.UndeclaredThrowableException

- at \$Proxy16.invoke(Unknown Source)
- at com.ibm.tpc.discovery.tsanm.InbandScanner.process(InbandScanner.java:136)
- at com.ibm.tpc.infrastructure.threads.TPCThread.run(TPCThread.java:257)

Caused by: java.net.ConnectException: Connection refused: connect at java.net.PlainSocketImpl.socketConnect(Native Method)

3/13/09 12:53:46 PM BTADS0033E Error invoking Topology on host x.xx.xxx.sxx:9510 .

```
3/13/09 12:53:46 PM java.lang.reflect.UndeclaredThrowableException
at $Proxy16.invoke(Unknown Source)
at com.ibm.tpc.discovery.tsanm.InbandScanner.process(InbandScanner.java:136)
at com.ibm.tpc.infrastructure.threads.TPCThread.run(TPCThread.java:257)
Caused by: java.net.SocketException: Operation timed out: connect:could be
    due to invalid address
    at java.net.PlainSocketImpl.socketConnect(Native Method)
```

Check the IP address in the /etc/hosts file on the agent system. If the IP address has changed, enter the correct IP address and restart the agent on the system.

# Microsoft SQL Server 2008 database scan or probe fails

Sometimes a scan or probe for a Microsoft SQL Server 2008 database fails.

### Problem

Examples of messages you might see are as follows:

1/23/09 8:13:53 AM DBA0110I: Scanning database msdb on tb180-wi/mssqlinst com.microsoft.sqlserver.jdbc.SQLServerException: Transaction (Process ID 54) was deadlocked on lock resources with another process and has been chosen as the deadlock victim. Rerun the transaction.

at com.microsoft.sqlserver.jdbc.SQLServerException.makeFromDatabaseError
 (Unknown Source)

at com.microsoft.sqlserver.jdbc.SQLServerStatement.getNextResult(Unknown Source)

1/23/09 8:13:56 AM SRV0081E: SQL error. Unable to access table sysindexes Stmt Type: SELECT, Stmt Phase: GET SQLSTATE: 40001, Vendor error code: 1205 Transaction (Process ID 54) was deadlocked on lock resources with another process and has been chosen as the deadlock victim. Rerun the transaction. 1/23/09 8:13:57 AM DBA00311: Scan aborted"

### Action

Check the Microsoft Web site for any hot fixes and download any fixes. For example, there is a Cumulative Update 3 for the Microsoft SQL Server 2008. Go to http://support.microsoft.com/kb/960484/.

## Microsoft SQL Server 2008 database scan or probe fails

Sometimes a scan or probe for a Microsoft SQL Server 2008 database fails.

### Problem

Java core files are created on the agent system. Examples of messages you might see are as follows:

```
9-02-2009 05:45:15.469-08:00 Entry com.tivoli.itsrm.repository.
RepositoryAccessor sqlError(e) --Agent Thread-23
09-02-2009 05:45:15.484-08:00 EXCEPTION
com.microsoft.sqlserver.jdbc.SQLServerException: Cannot invoke a rollback
operation when the AutoCommit mode is set to "true".
at com.microsoft.sqlserver.jdbc.SQLServerException.makeFromDriverError
(Unknown Source)
...
cleanup Thread-23
09-02-2009 05:45:15.484-08:00 Exit com.tivoli.itsrm.repository.
RepositoryAccessor sqlError --Agent Thread-23
...
9-02-2009 05:45:15.484-08:00 Exit com.tivoli.itsrm.storage.StorageException
getMessage, rc=2/9/09 5:45:15 AM SRV0081E: SQL error. Unable to access
```

```
table sysobjects-sysindexes-systabstats
Stmt Type: SELECT, Stmt Phase: EXECUTE
SQLSTATE: 40001, Vendor error code: 1205
Transaction (Process ID 55) was deadlocked on lock resources with
another process and has been chosen as the deadlock victim. Rerun the
transaction. --Agent Thread-23
```

Check the Microsoft Web site for any hot fixes and download any fixes. For example, there is a Cumulative Update 3 for the SQL Server 2008. Go to http://support.microsoft.com/kb/960484/.

Try scheduling the probe or scan job so they do not overlap. Rerun the probe or scan job.

# Microsoft SQL Server 2008 database scan or probe fails when databases are under a heavy workload

Sometimes a scan or probe for a Microsoft SQL Server 2008 database fails when the databases are under a heavy workload.

# Problem

Examples of messages you might see are as follows:

```
1/23/09 8:10:13 AM DBA0012E: Unable to connect to RDBMS <xxx.xxx.xxx>/mssqlinst.
Driver: com.microsoft.sqlserver.jdbc.SQLServerDriver
URL: jdbc:sqlserver://<xxx.xxx>:1433;SelectMethod=Cursor
SQLSTATE: 08S01, Vendor error code: 0
SQL Server returned an incomplete response. The connection has been closed.
```

## Action

Before running probe or scan jobs for a Microsoft SQL Server 2008 database, change the timeout parameter for the Microsoft SQL Server as follows:

- 1. Open the Microsoft SQL Server Management Studio.
- 2. Right-click on the name of the server. Click **Properties** and select the **Connections** tab.
- **3**. On the bottom of the screen, you can select a value for the remote connection timeout. Set it to 5000.
- 4. Save the configuration and restart the Microsoft SQL Server.

# Error message: Unable to launch Tivoli Storage Productivity Center GUI

When you click on the icon to start the Tivoli Storage Productivity Center GUI, an updated jar file is downloaded automatically and you see this error message.

## Problem

The error message is:

Unable to launch Tivoli Storage Productivity Center GUI Jar resources in JLP file are not signed by same certificate

## Action

To work around this issue, first clear the Java cache on your system. Then follow these steps for Java Web Start 1.4.2:

- 1. Open Java Web Start (either through the icon on your desktop or in your Program Files folder).
- 2. Click **File > Preferences**.
- 3. Click the **Advanced** tab.
- 4. Click the Clear Folder button, then click OK.
- 5. Close the Java Web Start Application Manager.

# **IBM Tivoli Storage Productivity Center for Replication**

This section provides information about troubleshooting IBM Tivoli Storage Productivity Center for Replication problems.

For additional troubleshooting topics, check the Tivoli Storage Productivity Center technical support Web site: http://www.ibm.com/servers/storage/support/ software/tpc. Click on Tivoli Storage Productivity Center for Replication. Click **Troubleshoot**. Under Problem resolution, click on Version 4 Flashes, Technical notes, and APARs.

# Administrative password

This section provides information about characters you cannot use for the IBM Tivoli Storage Productivity Center for Replication administrative password.

You cannot use the following characters for the IBM Tivoli Storage Productivity Center for Replication administrative password:

- square brackets ([ and ])
- semicolon (;)
- backward slash (\)

# IBM Tivoli Storage Productivity Center for Replication installation for Three Site BC

This topic describes how to troubleshoot the installation of IBM Tivoli Storage Productivity Center for Replication Three Site BC.

If the product installation fails, there is information on the reasons for the failure in the logs. There is a separate log for each part of the installation process, and it is helpful in correcting the problem:

#### The log for prerequisite checking:

- Windows: C:\Documents and Settings\Administrator
- Linux: /root
- AIX: /home/root

The log for product installation:

- Windows: *install\_root*\AdvEdTPCRMInstall.log
- Linux or AIX: *install\_root*/AdvEdTPCRMInstall.log

## **Replication Manager tab not working**

When you try to open the **Replication Manager** tab in the IBM Tivoli Storage Productivity Center GUI, it does not open.

## Problem

If IBM Tivoli Storage Productivity Center is running on Linux or AIX, and a system reboot has taken place, IBM Tivoli Integrated Portal will not restart automatically.

IBM Tivoli Integrated Portal needs to be restarted after a system reboot. For information about restarting IBM Tivoli Integrated Portal, see "Starting and stopping the IBM Tivoli Integrated Portal server" on page 466.

# IBM Tivoli Storage Productivity Center for Replication login failed

You have successfully installed IBM Tivoli Storage Productivity Center using LDAP authentication and are unable to login to IBM Tivoli Storage Productivity Center for Replication with a valid user ID.

## Problem

You cannot login to IBM Tivoli Storage Productivity Center for Replication using a valid user ID.

# Action

Review the values you entered for the LDAP TPC Administrator username and LDAP TPC Administrator group; these are the exact values you should use to login to IBM Tivoli Storage Productivity Center for Replication. Once you have accessed IBM Tivoli Storage Productivity Center for Replication, then you can use the Administration interface in the IBM Tivoli Storage Productivity Center for Replication user interface to grant authorization to other LDAP users and groups.

# When opening the Replication Manager tab in the configuration utility, no buttons appear for the Replication Manager

When you expand **IBM Tivoli Storage Productivity Center**  $\rightarrow$  **Configuration Utility** and select the **Replication Manager** tab, no buttons appear for the Replication Manager.

# Problem

You cannot start the IBM Tivoli Storage Productivity Center for Replication GUI.

# Action

To resolve this issue, follow these steps:

1. In a command prompt window, enter the following command:

```
"C:\Program Files\IBM\Tivoli\tip\bin\wsadmin.bat" -lang jython -conntype
NONE -f "F:/Program Files/IBM/replication/Scripts/CSM_TIP_Install.py"
"C://Program Files//IBM//Tivoli//tip/systemApps/isclite.ear"
```

In this example, C:\Program Files is the directory where the user installed IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication.

2. Restart IBM Tivoli Integrated Portal. For information about starting IBM Tivoli Integrated Portal, see "Starting and stopping the IBM Tivoli Integrated Portal server" on page 466.

# DB2 and database troubleshooting

Use this section to troubleshoot and resolve problems with DB2 and the database.

# Cannot read Korean language logs from GUI

This problem occurs in Korean language environments.

You will not be able to view the log files from the IBM Tivoli Storage Productivity Center GUI because of a DB2 JDBC driver problem.

#### Action

You will have to read the files using another text viewer like Notepad.

# Error message: GUI0023M

This error occurs when performing a system reboot.

#### Problem

After a reboot of the system, you receive the following error message: GUI0023M Unable to connect to server after reboot.

If abnormal behaviors are observed which might be related to or impact DB2, be sure to stop your DB2 instance properly before you perform a system reboot. If you do not stop DB2 properly, DB2 might take a long time to start. This will also cause IBM Tivoli Storage Productivity Center to not start.

#### Action

The DB2 instance might not have stopped properly. Manually stop and restart DB2.

#### Error message: SRV0024E

This error occurs when DB2 is down or not running.

#### Problem

This might be a problem with DB2. The DB2 database can be down or DB2 is not running. Check to see if DB2 is running. You will see this message: PM SRV0024E The requested service provider has been shutdown.

## Action

If DB2 is not running, start DB2 and then stop and restart the Device server and Data server.

#### Error message: SRV0044E

This error occurs when the password for the DB2 user ID account for which IBM Tivoli Storage Productivity Center is installed under is changed.

#### Problem

The GUI will not start and an error occurs in the log:

PM SRV0044E: Unable to connect to repository database. Please ensure that the repository database is up and running. Connection authorization failure occurred. Reason: password invalid.

#### Action

To change the DB2 user ID password, follow these steps:

 From a command prompt, change to the directory where the file repository.config resides in the Tivoli Storage Productivity Center installation path. For example on Windows:

<TPC\_install\_dir>\data\config

2. Run the following command for the Data Server:

```
java -classpath "<TPC_install_dir>\data\server\lib\TSRMsrv.zip"
com.tivoli.itsrm.repository.Transform
-p <new_db2userid_password> repository.config
```

**3**. Make sure the Device server is running. Run the following command for the Device server:

```
srmcp -u <user_ID> -p <password> ConfigService setPw
<new_password>
```

Where <new\_password> is the new password. This sets the DB2 user ID password (not the DB2 administrator password).

- 4. Stop and then restart Tivoli Storage Productivity Center Data Server from the Windows Services window.
- 5. Restart IBM WebSphere Application Server V6 Device server from the Windows Services window.
- 6. Start the Tivoli Storage Productivity Center GUI.

# **DB2** instance crashes

This problem occurs when running an agent probe.

# Problem

An agent probe causes the DB2 instance to crash. You also receive this message in the DB2 logs:

ADM0501C A stack overflow exception has occurred. The DB2 instance has terminated abnormally.

## Action

To resolve this problem, increase the DB2 stack size. Go to the DB2 directory: C:\Program Files\IBM\SQLLIB

Follow these steps:

- 1. Stop the Device server and Data Server.
- 2. Stop the DB2 database.
- **3**. Run the following command:
  - .\misc\db2hdr .\bin\db2syscs.exe /s: 512
- 4. Start the DB2 database.
- 5. Start the Device server and Data Server.

# **DB2** connection errors

These errors occur when rebooting remote DB2 servers.

# Problem

Getting DB2 connection errors in IBM Tivoli Storage Productivity Center server log files

This could be caused by the remote DB2 server being rebooted. If this is the case, restart the Data Server and Device server.

## Table space is out of space

This error occurs when the file system storing the database table spaces runs out of space.

# Problem

This is shown by the following kinds of errors as seen in the DB2 log called db2diag.log:

2005-11-06-12.59.10.815891-420 E36562387C690 LEVEL: Error PID : 176316 TID : 1 INSTANCE: db2inst1 NODE : 000 PROC : db2pclnr 0 FUNCTION: DB2 UDB, buffer pool services, sqlbClnrAsyncWriteCompletion, probe:0 MESSAGE : ADM6017E The table space "TPCTBSPTEMP" (ID "5") is full. Detected on container "/home/db2inst1/db2inst1/TPCDB/TPC/TPCTBSPTEMP" (ID "0"). The underlying file system is full or the maximum allowed space usage for the file system has been reached. It is also possible that there are user limits in place with respect to maximum file size and these limits have been reached.

This problem is seen on AIX 5.x with JFS file system. Large files need to be enabled on the file system because the table space files can get quite large. Enable large files on JFS or JFS2.

#### Action

During installation of AIX 5.1 or later, ensure that JFS or JFS2 with large file system support is installed. Follow the AIX documentation for this purpose as well as to back up and restore data between file systems. It is recommended to ensure that the file system size (especially for /home) is not too small (for example, not less than 4 GB). Back up your existing data before you recreate your file system. For information on file systems, see: http://publib.boulder.ibm.com/infocenter/pseries/index.jsp?top.

#### Error message: SQL0968C

This error occurs when the file system storing the database table runs out of space.

## Problem

You see this error message from DB2: SQL0968C The file system is full.

This is the explanation from DB2:

One of the file systems containing the database is full. This file system may contain the database directory, the database log files, or a table space container.

The statement cannot be processed.

Free system space by erasing unwanted files. Do not erase database files. If additional space is required, it may be necessary to drop tables and indexes identified as not required.

On UNIX-based systems, this disk full condition may be due to exceeding the maximum file size allowed for the current user ID. Use the **chuser** command to update the **fsize**. A reboot may be necessary.

This disk full condition may be caused when containers are of varying sizes. If there is sufficient space in the file system, drop the table space and recreate it with containers of equal size.

For AIX systems, check to see if the AIX file size limit goes beyond 2 GB. Check the sizes of the files. As the root user, run this command: lsfs -qa

If you see "bf: false", then you need to enable the large file option to allow files to go over 2 GB.

It is suggested that you monitor DB2's database performance. You can do this through DB2's Health Center. For more information about DB2's Health Center, see "Running the DB2 health monitor" on page 116 and DB2 Information Center. Click **Monitoring > Database systems > Monitoring database systems > Monitoring database health**.

# Error message when installing DB2: An error occurred while updating the services file

You get an error message when installing DB2 on a Windows system.

You receive this error message:

```
An error occurred while updating the services file on the system for the service name 'db2c_DB2' with port '50000'.
```

You also receive this error message (because DB2 failed to configure the port at installation time).

No valid local database found on the system.

To work around this issue, follow these steps:

 Run the following DB2 command from the DB2 command prompt window: db2 get dbm cfg

You will see the following output: TCP/IP Service name (SVCENAME) = db2c DB2

2. Change the port number. Run the following DB2 commands from the DB2 command prompt window:

db2 update dbm cfg using SVCENAME 50000 db2stop db2start

 Run the following DB2 command again to verify that the service port is correct: db2 get dbm cfg

This command should return the following output:

TCP/IP Service name (SVCENAME) = 50000

4. Run the IBM Tivoli Storage Productivity Center installation program again.

## Error message: HWNOP0033 Database operation failed

You receive this error message after running several storage optimizer jobs.

#### Problem

You receive this error message after running several storage optimizer jobs: HWNOP0013E Database operation failed com.ibm.db2.jcc.b.SqlException:

DB2 SQL error: SQLCODE: -956, SQLSTATE: 57011, SQLERRMC: null

This message indicates that all available memory for the database has been used. There is not enough storage available in the database heap to process the statement.

#### Action

Increase the database heap size to allow a larger database heap. If the database heap size is set to AUTOMATIC, you need to increase either the DATABASE\_MEMORY database configuration setting, or the INSTANCE\_MEMORY database manager configuration setting.

When updating the configuration parameters, it is suggested to change them by 10% of the current size until the error condition is resolved.

Here is an example of how to change the database heap size to 2400: db2 UPDATE DB CFG FOR TPCDB USING DBHEAP 2400 (the Tivoli Storage Productivity Center database schema sets the database heap size to 1800)

Here is an example of how to change the database heap size when disconnected from the database:

db2 CONNECT RESET; db2 UPDATE DB CFG FOR TPCDB USING DBHEAP 2400;

If all associated configuration parameters are set to either AUTOMATIC or COMPUTED, and the memory demands of the instance exceed the amount of memory configured on the system, then possible solutions would be to reduce the database workload or adding additional memory to the system.

# Error message: DB2 SQL error: SQLCODE: -968, SQLSTATE: 57011

You receive this SQL exception when you migrate IBM Tivoli Storage Productivity Center data.

### Problem

When migrating IBM Tivoli Storage Productivity Center data, you get this error message in the database installation log:

Instruction SQL : insert into t\_stat\_file\_temp SQLSTATE: 57011, Vendor error code: -964 DB2 SQL error: SQLCODE: -964, SQLSTATE: 57011, SQLERRMC: null This message indicates that there is not enough storage available in the database heap to process the statement. This error message is a result of running out of space in the transaction log. The transaction log configuration is set as:

db2 update db cfg for \$DBNAME using logprimary 8 db2 update db cfg for \$DBNAME using logsecond 16

Each transaction log file is 10 MB ( logFileSize=2500 pages of 4 KB each). Eight primary log files are allocated all the time. Secondary log files are allocated as needed, and deleted when not needed, to the maximum of 16.

## Action

Increase the transaction log files. See the DB2 documentation for information about increasing the transaction log files. Go to http://publib.boulder.ibm.com/ infocenter/db2luw/v9r5/index.jsp. Search for **logprimary** and **logsecond**..

# Error message: DEBUG: Error 2836

After you install DB2, you might see this error message in the DB2 installation log file.

## Problem

The error message is:

```
DEBUG: Error 2836: The control image_noJava on the dialog SetupInitialization
can not take focus
Internal Error 2836. SetupInitialization, image_noJava
Action 14:29:48: SetupInitialization. Dialog created
Action ended 14:29:48: SetupInitialization. Return value 1.
```

## Action

This is an informational message for the Windows installation program and will not cause problems.

# **Agent Manager**

This topic describes how to troubleshoot Agent Manager problems.

# Port conflicts and Agent Manager

The Agent Manager will not start properly if you install it on a computer system that runs another application that uses the same ports as the Agent Manager, WebSphere Application Server, or DB2 Enterprise Server Edition.

Common port conflicts are listed in Table 49, along with techniques for resolving them.

Default port	Used by	Potential conflicts	How to resolve
80	Agent recovery service	On all operating systems, check for conflicts with an HTTP server such as IBM HTTP Server or Microsoft Internet Information Server.	<ul><li>Disable the agent recovery service</li><li>Disable or uninstall the HTTP server</li></ul>

Table 49. Common port conflicts and how to resolve them

Default port	Used by	How to resolve
9511	Agent Manager	Specify a different port number when you install the Agent Manager
9512	Agent Manager	Specify a different port number when you install the Agent Manager
9513	Agent Manager	Specify a different port number when you install the Agent Manager
50000	DB2 ESE	Specify a different port number when you install DB2 ESE

Table 50. Other ports used by the Agent Manager and its prerequisites

The best way to deal with port conflicts is to check for and resolve them *before* you install the Agent Manager or its prerequisites, WebSphere Application Server and DB2 ESE.

Use both of the following techniques to verify that each of the ports listed in Table 49 on page 535 and Table 50 are available:

• Examine the /etc/services or %SYSTEMROOT%\System32\drivers\etc\services file to see a list of port definitions for the system.

The list includes ports that can be used by services on your system, even if the port is not currently in use. The file does not include ports that are opened dynamically by applications.

• Use the netstat -an command to list the active ports on this system.

If you have already installed the Agent Manager and suspect port conflicts, check the installation log for messages about port conflicts. The installation program records trace information about port conflicts for the Agent Manager and the DB2 Server. The installation program can report a successful installation even when port conflicts exist.

After the installation is complete, and before starting the Agent Manager server, look in the am\_install.log file in the <Agent\_Manager\_install\_dir/logs> directory for the following text:

Warning: The installation has detected that a required port is currently in use by another program: *portNumber*. The agent manager cannot start successfully if this port is in use.

If you find this message, take the action appropriate to the port number:

#### 9511, 9512, 9513

Uninstall the Agent Manager and then reinstall specifying available port numbers.

# Error message "Password Expired"

When a Common agent or resource manager tries to register with the Agent Manager, the Agent Manager tries to access the database. If the Agent Manager cannot access the database because of a password problem, this message is issued.

#### Problem

This can occur when the database password expires or is changed. Applications accessing the database must also change their database password. When the Agent

Manager WebSphere application queries the database using the old or expired password, this message is displayed in the activity.log file under the Agent Manager directory:

Agent Manager/embedded/logs/AgentManager

You will see a message similar to this:

```
SqlException: SQL30082N Attempt to establish connection failed with security reason "1" ("PASSWORD EXPIRED"). SQLSTATE=08001
```

## Action

For information about how to change the DB2 password, see "Changing the DB2 password for the Agent Manager on Windows" on page 477 or "Changing the DB2 password for the Agent Manager on UNIX or Linux" on page 479.

# Error message "The following command failed: Description: Configuring Port Numbers for WebSphere Application Server"

If the installation program for the Agent Manager cannot configure the WebSphere ports, you will see this message.

# Problem

Agent Manager cannot configure the WebSphere ports.

# Action

For information about how to change port numbers, see "Configuring Agent Manager to use different ports" on page 415 and "How to change port 80" on page 416.

# **Correcting registration failures**

Common reasons for a registration failure includes the following problems:

- When the Agent Manager was installed, a short host name was specified instead of a fully qualified host name (for example, myserver instead of myserver.ibm.com) and the agent cannot resolve the registration URL (which contains the short name) to the Agent Manager server
- The wrong truststore file was used when installing the agent or resource manager
- The wrong agent registration password was used when installing the agent
- The wrong resource manager registration user ID or password was used when installing the resource manager
- Agent Manager configuration files, such as AgentManager.properties or Authorization.xml, are missing or have been altered
- Security credentials are invalid, expired, or revoked

# Get error message that one or more services could not be started

This error occurs when you reboot the Agent Manager server.

When you reboot the Agent Manager server, you get a message saying that one or more services could not be started and to look in the Event Log for more details. When you open the Event Log, you see this message:

```
Could not determine the process id of the java process.
Changing the IBMWAS5Service - Tivoli Agent Manager service
status to the "stopped" state. To prevent this error, try
recreating this service with the -logRoot parameter.
The value of the logRoot parameter should be the directory in
which the server's .pid file is created.
```

This message does not provide a solution to the problem. When you issue the Agent Manager **startServer** command:

C:\Program Files\IBM\AgentManager\bin>startServer

You get this output:

```
The IBM WebSphere Application Server V6 - Tivoli Agent Manager service
is starting..... The IBM WebSphere Application Server V6 - Tivoli Agent
Manager service could not be started. A system error has occurred. System
```

error 100 has occurred. Cannot create another system semaphore.

#### Action

The message "Cannot create another system semaphore" indicates that another process is using one of the ports needed by Agent Manager. For example, if you are using the IIS web server which uses port 80, stop the IIS web server and specify a different port for the web service.

This error could also occur even if no other process is using port 80. The Agent Manager service actually does start but does not show up as started in the Windows Services panel. You can ignore this issue and use the commands **startServer** and **stopServer** to start and stop Agent Manager.

#### Error reinstalling Agent Manager on Windows

This error occurs when you reinstall the Agent Manager on Windows.

#### Problem

You get the following error message after you reinstall Agent Manager:

The Embedded WebSphere Installer encountered an error while attempting to unpack the archive "Z: \TPC\_V3.1\AgentManagerEmbeddedWS\_1.2.2\_Windows\EmbeddedInstaller\images\

```
EmbeddedExpress_wintel_jdk.zip". Examine the file "C:\DOCUME~1\tivoli\
LOCALS~1\Temp\logs\embedded_install.log" for more details.
```

#### Action

There might be some residue in the \temp directory. Delete the contents of the following directory:

C:\Documents and Settings\<user\_ID>\Local Settings\Temp

Rerun the Agent Manager installation program.

## **Error configuring WebSphere Application Server port numbers** This error occurs during installation.

If the installer cannot configure the WebSphere ports, you will see this message. The following command failed: Description: Configuring Port Numbers for WebSphere Application Server

### Action

If you see this message, refer to "Port conflicts and Agent Manager" on page 535 for information about port conflicts.

## GUID files have been deleted from system

This error occurs when the GUID files have been manually deleted from the system.

### Problem

You see this error message from the logs:

```
(Feb 15, 2007 2:29:18 PM), AM Install, com.certGen stderr.log100644 ...
java.lang.Exception: 231628960
at com.tivoli.agentmgr.resources.GUIDHelper.getHostId
     (GUIDHelper.java:53)
at com.tivoli.agentmgr.AgentManager.getSystemGuid
    (AgentManager.java:1415)
Caused by: 231628960
at com.tivoli.srm.guid.GuidOFactory.<init>
     (GuidOFactory.java:79)
at com.tivoli.agentmgr.resources.GUIDHelper.getHostId
     (GUIDHelper.java:48)
 ... 5 more
com.tivoli.agentmgr.wsdl.util.AgentMgrServerException:
  Cannot get system GUID
at com.tivoli.agentmgr.AgentManager.getSystemGuid
     (AgentManager.java:1426)
at com.tivoli.agentmgr.AgentManager.loadAgentManagerID
    (AgentManager.java:1368)
  . . .
```

## Action

Either remove the GUID program from the system or clean up any GUID residue. Then reinstall Agent Manager.

To remove the GUID program from the system on Windows, follow these steps:

- 1. Go to Start > Settings > Control Panel > Add/Remove Programs > TivGuid. Click Remove.
- 2. Reboot the system.
- 3. Reinstall the Agent Manager.

To remove GUID residue from the Windows system, follow these steps. You might have GUID residue if you have deleted the GUID folder by mistake.

- 1. Go to Start > Settings > Control Panel > Add/Remove Programs > TivGuid. Click Remove.
- 2. Start the Windows registry editor: Start > Run. Enter regedit.
- **3.** Go to **My Computer > HKEY\_LOCAL\_MACHINE > SOFTWARE > Tivoli**. Right-click on **GUID** and click **Remove**.

- 4. Reboot the machine.
- 5. Reinstall the Agent Manager.

To remove the GUID from Linux, follow these steps:

1. Run these commands:

rpm -qa | grep TIV rpm -ev | <Tivguid\_package\_name> (from previous output)

2. Reinstall the Agent Manager.

To remove GUID residue from the Linux system, follow these steps. You might have GUID residue if you have deleted the GUID folder by mistake.

1. Run these commands:

rpm -qa | grep TIV
rpm -ev | <Tivguid\_package\_name>
 (from previous output)

2. Reinstall the Agent Manager.

# Could not install Agent Manager because of database problem

This error occurs when you try to install the Agent Manager.

## Problem

You see these error messages in the following log files:

db\_stdout.log:

InstallDatastore determined that Database "IBMCDB" (db2) does not exist: No suitable driver

db\_stderr.log:

### Action

If you have created a DB2 user ID to install Agent Manager (for example on UNIX, you create a db2inst1 user ID), check to make sure that you have created a .profile for that user and the .profile sources the corresponding user's db2profile.

# Installation and uninstallation troubleshooting

Use this section to troubleshoot and resolve problems with IBM Tivoli Storage Productivity Center installation and uninstallation.

#### Error message: "Specified directory is not empty"

This message applies to the Common agent.

#### Problem

You get the message "Specified directory is not empty" when installing the Common agent. This condition can occur when you uninstall and reinstall the Common agent.

If you get this message, ensure that the ca and log directories are empty. For example if you used the default directory, check the following directory: C:\Program Files\IBM\TPC (for Windows)

or

/opt/IBM/TPC (for UNIX or Linux)

# Error message: INS3105E Failure to install remote agent

This error occurs when you are installing a remote agent on a UNIX or Linux system. .

# Problem

You get this error message:

PM INS3105E: Host <fully\_qualified\_hostname> is associated with an invalid loopback IP 127.0.0.1

In the /etc/hosts file, the line for the specified IP address should be:

```
127.0.0.1 localhost.localdomain localhost
```

#### and **not**

```
127.0.0.1 <fully_qualified_hostname> <short_hostname>
localhost.localdomain localhost
```

You should have a separate entry for the regular IP address and hostname of the IBM Tivoli Storage Productivity Center server. For example:

9.47.98.63 <fully\_qualified\_hostname> <short\_hostname>

## Action

The DB2 instance might not have stopped properly. Manually stop and restart DB2.

## Error message: INS0081E

You get this error message when using the silent mode installation script (setup.iss).

# Problem

You get this error message: <code>INS0081E=The server {0}:{1}</code> connection is unsuccessful - check the server name and port.

## Action

Be careful when modifying the setup.iss script. Do not add or delete spaces for the variables.

# Agent uninstallation program reports failure on command: uninstall.sh "false"

This problem occurs when uninstalling the IBM Tivoli Storage Productivity Center agent.

The Tivoli Storage Productivity Center agent uninstallation program reports that it has failed on the command: uninstall.sh "false".

### Action

This problem can be ignored if it was caused by the Common agent uninstallation program failing to delete missing startup scripts. If this was the cause, the Common agent uninstall.log file will contain entries like this:

## Installing a remote agent fails

This error occurs when you install a remote agent and it fails.

# Problem

You are getting a connection error to the remote computer when you try to install a remote agent.

#### Action

When you are installing a remote agent from a Windows computer, you must have the HOSTS file set properly on the Windows computer. For information about the HOSTS file, see "Changing the HOSTS file" on page 323.

#### Failure to register agent when running AIX with IPv6

This error occurs when you try to register the agent and it fails when running on AIX with IPv6.

## Problem

The agent registration fails.

## Action

To work around this problem, follow these steps:

1. First install the Common agent with a flag set. Use the agent CD or go to the directory where you have the Common agent installation program and run the **setup.sh** program:

<common\_agent\_install\_dir>/commonagent/setup.sh
-W beanArguments.agentJVMParms="-Djava.net.preferIPv4Stack=true"

2. Use the IBM Tivoli Storage Productivity Center installation program to upgrade the Data agent or Fabric agent.

#### Agent uninstallation program fails

This error occurs when you uninstall the agent using the IBM Tivoli Storage Productivity Center uninstallation program.

#### Problem

The Tivoli Storage Productivity Center agent uninstallation program reports that it has failed on the command: **uninstall.sh** "**false**".

This problem can be ignored if it was caused by the Common agent uninstallation program failing to delete missing startup scripts. If this was the cause, the Common agent uninstall.log file will contain errors like this:

```
Agent, com.tivoli.agent.install.Service, dbg, Utility.executeCommand
  (sh -c rm -r /etc/rc.d/rc0.d/K7litca0) returned 1
```

# Silent mode installation warning

This error message occurs when you install the Data agent using silent mode.

# Problem

You receive the following error message in the log file that was specified with the "-is: log option" :

```
ErrOut:
```

```
java.util.NoSuchElementException
at java.util.StringTokenizer.nextToken(StringTokenizer.java:280)
at com.installshield.wizard.commandline.DatabaseVariable
PropertiesOption.execute(Unknown Source)
at com.installshield.wizard.Wizard.executeStartupBeans
(Wizard.java:1626)
at com.installshield.wizard.Wizard$RunThread.run
(Wizard.java:1739)
WARNING: an unhandled error occurred during the processing of
command line option V: java.util.NoSuchElementException
```

# Action

If there are no other error messages and the Data agent appears to have been installed successfully, you can ignore these messages.

## Remote agent installation fails

This topic provides information when a remote agent installation fails.

#### Problem

The remote agent installation fails.

### Action

If the remote agent installation fails on a target computer, consider the following items:

- The computer from which you are performing the remote installation must have domain authority over the computer or computers on which you are installing the agent.
- The computer from which you are performing the remote agent installation must be able to connect with the computer on which you are installing the agent.
- The remote deployment of the Fabric agent fails. This might be caused by insufficient space on the target computer. Check the log file. For example, in the log file you might see an error saying it failed to install the GUID because the installguid.sh file was missing. This was probably caused by a lack of space.

This is a current limitation of remote deployment for the Fabric agent. There is no capability to check space like the Data agent remote deployment.

## Installing the agent on HP-UX fails

This topic provides information when installing the agent on HP-UX 11.11.

When installing the agent on HP-UX 11.11, the installation hangs with an exception message in InstallShield:

```
(Jan 25, 2007 5:03:31 PM), Install, com.installshield.wizard.
platform.legacyhpux.service.registry.LegacyHpuxRegistryServiceImpl,
dbg.registry, reading VPD from /var/adm/sw/products/INDEX
(Jan 25, 2007 5:03:31 PM), Install, com.installshield.wizard.
platform.legacyhpux.service.registry.LegacyHpuxRegistryServiceImpl,
err, java.lang.StringIndexOutOfBoundsException: String index
out of range: -1
STACK_TRACE: 52
...
```

The message does not appear in the GUI installation window. Check the fabricAgentInstallIS.log file. You can find this log file with a Java stack trace using the **find** command.

```
# find /opt/IBM/TPC -type f -name "*.log" -exec
grep -l java.lang {} \;
/opt/IBM/TPC/log/subagents/TPC/Fabric/install/
fabricAgentInstallIS.log
#
```

This can be caused by not enough space in the /tmp directory.

### Action

Increase the space in the /tmp directory to the required amount (500 MB) and reinstall the agent.

#### InstallShield parameters

When you are having problems with installing IBM Tivoli Storage Productivity Center, this topic provides some useful InstallShield parameters you can use to help with problem solving.

#### Problem

When you have problems with installing Tivoli Storage Productivity Center, you can append these parameters to the **./setup.sh** or **setup.exe** command to help you identify where the problem is.

### Action

These are some helpful InstallShield parameters:

#### -is:tempdir <directory>

Sets the path to the temporary directory to which the launcher should write its temporary files. If the specified directory does not exist or is not a directory, the launcher will use the system "temp" directory instead, and no error message is provided.

#### -is:javaconsole

Overrides the Distribution bean's Show Console property value of "False" by turning on the Java console during installation. This has no effect on how the installation wizard runs.

#### -is:javahome <Java\_home\_directory>

Specifically tells the launcher the home directory location of the JVM to use. This option works when executing an Application launcher, as well as

for an installation launcher. The JVM that resides in the specified directory must be one of the JVMs specified in the JVM Search Instructions property of the JVM Resolution view in order for it to work. Otherwise, this command line option has no effect.

### -is:log <file\_name>

This option is useful for setup launchers that hide the Java console because it logs the detailed information about the launcher's processing, including the actual Java commands that were used to start the Java program, to the specified <file\_name>. This includes all of the "std out" and "std err" messages from the Java process.

#### -is:silent

Prevents the display of the launcher user interface to the user. This option does not execute the application itself in silent mode, that is, this option prevents the display of the wizard. To execute the application in silent mode, use the **-silent** option.

#### -is:version

Reports the version of the setup launcher itself. When this option is specified, the launcher simply reports its version and exists without launching the application.

#### -cp:a <classpath;classpath> or -cp:p <classpath;classpath>

Modifies the classpath used by the installation launcher to install or uninstall the program. This option cannot be used with a JAR archive, for example, "setup.jar."

The option **-c:a** appends (adds to the end) of the classpath. The option **-c:p** prepends (adds to the beginning) of the classpath.

To add more than one class, separate each with the platform-specific delimiter. You can also specify that an ASCII file containing the additional classpaths be used by preceding the file name with "@." Each classpath in this file must be on a separate line.

# Remote Fabric agent information panel

When installing the Fabric agent remotely, the Remote Fabric agent information panel allows you to drag and drop column headings but the information under the column headings do not move with the column headings.

## Problem

This problem occurs when you are installing the Fabric agent remotely and the Remote Fabric agent information panel is displayed listing the remote common agents to deploy.

## Action

Do not drag and drop the column headings.

## Error message: "There is not enough space in the filesystem".

This problem can occur when installing or upgrading IBM Tivoli Storage Productivity Center.

## Problem

When installing or upgrading Tivoli Storage Productivity Center, you get this error message:

There is not enough space in the filesystem.

InstallShield does not provide the name of the file system that lacks the space.

# Action

If you get this error message, increase the /tmp directory. Retry the installation or upgrade.

# Installing a remote Data agent fails using Windows domain authentication

This error occurs when you install a remote Data agent from an AIX IBM Tivoli Storage Productivity Center server using the Windows Domain Administrator for authentication.

# Problem

You cannot remotely install a Data agent using the Windows Domain Administrator for authentication.

# Action

Do one of the following to work around this problem:

- Specify a local administrator (non-domain) to authenticate the remote Data agent installation on the Windows server.
- Install the Data agent locally. In this case, you can use the Windows Domain Administrator for authentication.

# Cleaning up a failed installation or uninstallation on Windows

This topic provides information on what to clean up after a failed IBM Tivoli Storage Productivity Center installation or uninstallation on Windows.

# Problem

To clean up a failed Tivoli Storage Productivity Center installation or uninstallation on Windows, follow the steps below.

# Action

To clean up a failed Tivoli Storage Productivity Center installation on Windows, follow these steps. These steps assume you are using the default directories.

- 1. Using the Windows Services panel, stop the Device server and Data Server.
- 2. Stop the Common agent service.
- **3**. Make sure that any Java or nonstop processes from Tivoli Storage Productivity Center are not running.
- 4. Go to the following directories:
  - C:\Document and Settings\TSRMsrv1

Delete all existing TSRMsrv1 folders.

• C:\Program Files\Common Files\InstallShield\Universal\IBM-TPC

Delete IBM-TPC.

• Delete the Tivoli Storage Productivity Center installation location directory: C:\Program Files\IBM\TPC

## Delete Tivoli Storage Productivity Center.

Remove the Common agent entry from the following:
 C:\Program Files\Tivoli\

Delete the **ep.reg** file and **ep.bak** (if this exists).

Remove the Tivoli Storage Productivity Center folder from the Start menu.
 C:\Documents and Settings\All Users\Start Menu\Programs\

#### Delete Tivoli Storage Productivity Center.

5. Delete specific keys from the Windows registry.

**Note:** You can edit the registry by using Registry Editor (**regedit**). Be careful when using **regedit**. If you use the Registry Editor incorrectly, you can cause serious problems that may require you to reinstall your operating system. To start **regedit**, follow these steps:

- a. Click Start > Run.
- b. On the Run dialog panel, enter regedit.
- c. Click OK.
- d. When the Registry Editor window is displayed, click Edit > Find.
- e. The Find panel is displayed. On the Find panel, enter the key you are searching for in the Find what field. Select Keys. Do not select Values, Data, or Match whole string only. Click Find Next. Search for the following keys:
  - TSRM
  - TPCDagt# (where # can be any number; usually it is 1).
  - IBMTivoliCommonAgent
  - IBMWAS6Service DeviceServer
  - TSRMsrv# (where # can be any number; usually it is 1).

Delete all keys from your search result. Do **not** delete keys starting with **LEGACY\_name**.

- 6. Drop the Tivoli Storage Productivity Center database using the DB2 Control panel.
  - a. Open a DB2 command line window. Go to Start > Programs > IBM DB2 > Command Line Tools > Command Line Processor.
  - b. Enter:

list datase directory

- c. If the database name is **TPCDB** and it is listed, then enter: drop database TPCDB
- 7. Remove the following users from the system:
  - TSRMSrv# (where # can be any number; usually it is 1).
  - itcauser# (where # can be any number; usually it is 1).

To remove these users, go to Start > Settings > Control Panel > Administrative Tools > Computer Management . Under Computer Management (Local), expand Local Users and Groups and open the Users notebook. Delete the users listed above.

8. Reboot the system (required).

To clean up a failed Tivoli Storage Productivity Center uninstallation, follow these steps:

1. During uninstall, you get a screen stating:

```
Cannot uninstall component Device Server:
Reason: Port 9550 is in use.
Make sure component has shutdown then click next to continue.
```

or

```
Cannot uninstall component Device Server:
Reason: File C:\Program Files\IBM\TPC\data\server\lib\TSRMsrv.zip is in use.
Make sure componet has shutdown then click next to continue.
```

- 2. A service is active and must be terminated. Follow these steps:
  - a. Go to Start > Settings > Control Panel > Administrative Tools > Services.
  - b. Right-click on WebSphere Application Server V6 DeviceServer.
  - c. Select Properties. At Startup type, click Manual. Click OK.
  - d. Stop the WebSphere service by right clicking on it, and click Stop.
  - e. Reboot the system.
  - f. When the system returns, start the uninstallation of Tivoli Storage Productivity Center through Add or Remove Programs. Go to Start > Settings > Control Panel >Add or Remove Programs.
- **3**. If the server host name has been changed where Tivoli Storage Productivity Center is installed, follow these steps. If a shortcut icon had been created on the Desktop prior to the change, then clicking on this icon will display the old host name as the default signon **Server**. To modify the default host name to the new host name, follow these steps.
  - a. Go to the desktop, right-click on the Tivoli Storage Productivity Center shortcut icon, and click **Properties**.
  - b. In the Target field, find the old host name and replace with the new host name.
  - c. Click **OK**. The login prompt will now contain the correct host name in the Server field.

# Cleaning up a failed installation or uninstallation on UNIX

This topic provides information on what to clean up after a failed IBM Tivoli Storage Productivity Center installation or uninstallation on UNIX.

# Problem

To clean up a failed Tivoli Storage Productivity Center installation or uninstallation on UNIX, follow the steps below.

## Action

To clean up a failed Tivoli Storage Productivity Center installation or uninstallation on UNIX, follow these steps. These steps assume you are using the default directories.

- 1. Stop the Device server and Data Server.
- 2. Stop the Common agent service.
- **3**. Make sure that any Java or nonstop processes associated with Tivoli Storage Productivity Center are not running.
- To clean up the product registry, delete the following directory: /etc/Tivoli/TSRM
- 5. To clean up the installation registry, delete the following directory:
For AIX, delete IBM-TPC: /usr/lib/objrepos/InstallShield/Universal/IBM-TPC

For Linux, delete IBM-TPC: /root/InstallShield/Universal/IBM-TPC

6. To clean up the subsystem in AIX, enter this command:

rmssys -s TSRMsrv# (where # can be any number; usually it is 1)

- 7. Drop the database:
  - a. Log in as db2inst1 (the database instance owner ID).
  - b. Drop the database using the following command:

db2 drop db TPCDB (if TPCDB is the name of your database; this is the default name)

c. Delete the Tivoli Storage Productivity Center installation directory. /<usr or opt>/IBM/TPC

### Cannot reinstall an agent

This topic provides information on what to do and clean up if you cannot reinstall a Common agent, Data agent, or Fabric agent.

#### Problem

This topic provides some hints and tips on how to clean up the environment if you cannot reinstall an agent.

#### Action

#### How to force the Common agent to uninstall

There may be times when you want to uninstall the Common agent, and there are still Data or Fabric agents installed. You can force it to uninstall with a special parameter. To uninstall the Common agent under these circumstances, follow these steps:

- 1. Open a command prompt (on Windows) or Terminal session (on UNIX).
- 2. Go the Common agent uninstaller directory:

For Windows with a TPC V3.1 or V3.3 agent: C:\Program Files\IBM\ca\\_uninst

For Windows with a TPC V2.3 agent: C:\Program Files\Tivoli\ep\\_uninst

For AIX with a TPC V3.1 or V3.3 agent: /usr/tivoli/ep/\_uninst

3. Enter the uninstall command (for GUI mode):

For Windows: uninstall.exe -W beanArguments.forceUninstall=true

For UNIX:
./uninstall -W beanArguments.forceUninstall=true

- 4. The GUI uninstaller will be launched. For non-GUI mode, specify the **-console** option in the command syntax in step 3.
- **5.** Delete the removed Data agent and in-band Fabric agent from the IBM Tivoli Storage Productivity Center GUI (**Administrative Services > Agents**).

Cleaning up Common agent residue on Windows

You might encounter situations where there is residue from a previous Common agent installation that keeps you from being able to install a new Common agent.

To clean up the Common agent residue on Windows, follow these steps:

1. Remove the following files:

C:\Program Files\Tivoli\ep.bak C:\Program Files\Tivoli\ep.reg

2. Remove the following directories:

```
C:\Program Files\IBM\TPC\ca
C:\Program Files\Common Files\InstallShield\
Universal\IBM-TPC
```

#### Cleaning up Common agent residue on AIX

Follow these steps:

1. Remove the following files:

```
rm -f /etc/Tivoli/swdis*
rm -f /usr/tivoli/ep*
```

2. Remove the following directories:

```
rm -rf /home/root/.swdis/work
rm -rf /etc/Tivoli/TSRM
rm -rf /opt/IBM/TPC
rm -rf /usr/lib/objrepos/InstallShield/Universal/IBM-TPC
rm -rf /usr/tivoli/ep
```

- 3. Edit the file /usr/lib/objrepos/vpd.properties.
  - a. Make a backup copy of this file before making any changes.
  - Remove any lines that contain the path /opt/IBM/TPC/ca or /usr/tivoli/ep/subagents/TPC.
  - c. If the entire file refers only to entries for /usr/tivoli/ep/subagents/TPC, you can delete the entire file.

#### Cleaning up the Windows registry

There may be residue in the Windows registry if the Common agent was not uninstalled cleanly.

**Note:** You can edit the registry by using Registry Editor (**regedit**). Be careful when using **regedit**. If you use the Registry Editor incorrectly, you can cause serious problems that may require you to reinstall your operating system.

To edit the registry, follow these steps:

- 1. Click Start > Run.
- 2. On the Run dialog panel, enter regedit.
- 3. Click OK.
- 4. When the Registry Editor window is displayed, click Edit > Find.
- 5. The Find panel is displayed. On the Find panel, enter the key you are searching for in the Find what field. Search for the following keys:
  - Node=IBMTivoliCommonAgent...
  - Value=Program Files\TPC\CA...
  - Node=TSRMAGT...

Delete all keys from your search result.

## Cleaning up a failed installation for Virtual I/O agents

When you have a failed installation for Virtual I/O agents, use the AIX cleanup procedure.

### Problem

You have a failed installation for the Virtual I/O agent and need to reinstall the agent.

Clean up instructions for a failed install is no different from any AIX agent machine. You must be root and not padmin user. To do this you type oem\_setup\_env as padmin user and you become root. At that point cleanup is the same. The install will always be located in /opt/IBM/TPC

### Action

Follow these steps:

1. To clean up any residue on the system, you must be the root user and not the padmin user. To do this, enter the following command as the padmin user and this changes your user ID to root.

oem\_setup\_env

- 2. Remove the following files:
  - rm -f /etc/Tivoli/swdis\*
  - rm -f /usr/tivoli/ep\*
- 3. Remove the following directories:
  - rm -rf /home/root/.swdis/work
  - rm -rf /etc/Tivoli/TSRM
  - rm -rf /optIBM/TPC
    rm -rf /usr/lib/objrepos/InstallShield/Universal/IBM-TPC
  - rm -rf /usr/tivoli/ep
- 4. Edit the file /usr/lib/objrepos/vpd.properties.
  - a. Make a backup copy of this file before making any changes.
  - b. Remove any lines that contain the path /usr/tivoli/ep/subagents/TPC.
  - c. If the entire file refers only to entries for /usr/tivoli/ep/subagents/TPC, you can delete the entire file.

## Upgrading the Fabric agent causes program to hang

This topic provides information on what causes the installation program to hang when upgrading the Fabric agent.

### Problem

When you upgrade the Fabric agent, the installation program hangs.

## Action

If the Fabric agent cannot detect the Host Bus Adapter, the installation will hang. The reasons could be: there is no HBA in the system, or the device driver for the HBA is not working correctly or is an unsupported version.

# The Solaris HBA identifies a SCSI device instead of fibre channel LUNs

This problem occurs when the Solaris HBA identifies a SCSI device instead of fibre channel LUNs.

This problem may be a result of a configuration setup problem with the HBA.

### Action

In SUN Solaris, make sure that the /etc/hba.conf file points to the correct vendor HBA API library.

For example, if the QLOGIC HBA API library is set as follows in the /etc/hba.conf file: ql2x00 libqlsdm.so

This is incorrect and should be changed to:

ql2x00 /usr/lib/libqlsdm.so

In windows, this library is identified using the registry value at: HKEY LOCAL MACHINE/SOFTWARE/SNIA/HBA/<vendor name>

For example, for QLogic you will have this value: HKEY\_LOCAL\_MACHINE/SOFTWARE/SNIA/HBA/QL2X00

The property for the library is in the LibraryFile key.

For QLogic, a correct configuration has the LibraryFile key set as: C:\Program Files\QLogic Corporation\SANsurfer\ql2xhai2.dll

Also, the RDAC controller does not have a common HBA API interface. Therefore, the WWN and fibre identification does not work at this time.

## Common agent times out trying to register with Agent Manager

This problem occurs when the Common agent tries to register with the Agent Manager.

### Problem

The Common agent times out trying to register with the Agent Manager. You will see this:

- The endpoint.properties file is populated with returned information from the Agent Manager.
- The lastError.properties file is created in the Common agent configuration directory displaying the timeout error.
- The msgAgent.log shows that the agent was unable to register with the Agent Manager.

#### Action

When the Agent Manager is installed, it is configured to be associated with a network name which it broadcasts to agents. Even though the Agent Manager listens on all IP addresses, the agent machine ultimately needs to be able to resolve the host name returned by the Agent Manager.

Time out problems are often caused by the server trying to resolve the client IP address to a DNS name. Either DNS is not configured properly on your server or

the client machines are not known to DNS. If you are not using DNS, add the client machine name and IP to your /etc/hosts file on the server.

The /etc/hosts file does the mapping of host names to IP addresses before DNS can be referenced. In the absence of a name server, any network program on your system consults this file to determine the IP address that corresponds to a host name.

Alias

The following example is an /etc/hosts file on a UNIX machine.

132.0.0.1 localhost myhost.agent1.com 227.182.172.1 myhost.agent1.com agent1

Hostname

The first column is the IP address to be resolved. The second column is the host's name. Any subsequent columns are aliases for the host.

After you are finished configuring your networking files, restart your network for the changes to take effect.

## Remote agent installation creates two directories

When you remotely install the Data agent and specify a specific directory, and then install the Fabric agent, there are two directories created.

### Problem

IPAddress

When you remotely install the Data agent and specify a specific directory, for example:

/rootfs1/opt/IBM/TPC/ca

and then you remotely deploy the Fabric agent, the agent also gets installed in /rootfsl/opt/IBM/TPC/ca. However, the Fabric agent installation creates the InstallShield uninstall binary and other directories and files in /opt/IBM/TPC (for example, TPC.log and version.txt).

### Action

When you uninstall the agents, you must uninstall files from both directories created.

### Cannot uninstall component Device server

You receive this error message when you try to uninstall IBM Tivoli Storage Productivity Center.

#### Problem

When you try to uninstall Tivoli Storage Productivity Center, you receive this error message:

```
Cannot uninstall component Device Server:
Reason: Port 9550 is in use.
Make sure component has shutdown then click
next to continue.
```

### Action

When you uninstall Tivoli Storage Productivity Center, the uninstallation program tries multiple times to see if the Device server has stopped. If Tivoli Storage

Productivity Center Device server does not stop, you can issue the following command from the command prompt window:

cd /opt/IBM/TPC/device/bin/linux
./stopTPCF.sh

The uninstallation program should complete the uninstallation process.

# Installing IBM Tivoli Storage Productivity Center on Windows with installation files on a Samba fileshare

When WebSphere is installed, a required directory is not copied. This causes the creation of the Device server profile to fail and the Device server installation to fail.

#### Problem

UNIX and Linux filesystems use Samba software to mount filesystems on Windows. UNIX and Linux mark hidden files with a leading dot '.' in the file or the folder name. In the Samba default configuration, the files and folders with the leading dot get the Windows "hidden" files attribute to ensure consistent behavior.

#### Action

Change the Samba configuration setting to:

```
hide dot files = no
```

for the Samba share or as a general setting in the Samba configuration file smb.conf. The files and folders are no longer marked as hidden.

# No warning message when GUI is open during uninstall or upgrade

No warning message is issued when you have the GUI open during an uninstall or upgrade.

#### **Problem**

If you have the IBM Tivoli Storage Productivity Center GUI open during an upgrade or uninstall on UNIX machines, the installer will not give a warning message.

### Action

This will not affect the uninstallation or upgrade. The uninstallation program will clean up the GUI directory and the upgrade will update the required files.

### Failed to validate Common agent registration password

You receive this error message when you install the agent.

#### Problem

When you install the agent, you receive this error message: Failed to validate the common agent registration password for the Common Agent Service. Caught Exception: Unknown certificate Please verify that the information provided is correct and that the agent manager is running.

## Action

Check the system dates on all your servers that are managed by IBM Tivoli Storage Productivity Center. All system dates on all servers managed by Tivoli Storage Productivity Center must match the Tivoli Storage Productivity Center server and Agent Manager machines. Time zone differences are taken into account during the installation process.

## Successful uninstall does not delete JRE directory

This problem occurs when you do not follow the standard procedure for uninstallation.

#### Problem

When you uninstall IBM Tivoli Storage Productivity Center successfully, the JRE directory is not deleted.

#### Action

When you uninstall Tivoli Storage Productivity Center on Windows, use the Add/Remove Programs window. See Chapter 5, "Uninstalling the IBM Tivoli Storage Productivity Center family," on page 383. If the JRE directory still remains after a successful uninstallation, manually delete the JRE directory.

When you run the uninstallation program for UNIX or Linux, run the uninstallation program **outside** of the installation directory tree. For example, if you installed Tivoli Storage Productivity Center on /opt/IBM/TPC, run the uninstallation program from another directory:

./opt/IBM/TPC/\_uninst/uninstall

### Common agent ignores umask setting

On some operating systems, the Common agent ignores the umask setting.

#### Problem

On some operating systems, the Common agent ignores the umask setting and creates log files that are writeable. With Common agent 1.2.3.8, there is a umask setting in the nonstop.properties file that is set to 022 by default.

#### Action

You can edit the nonstop.properties file to the umask setting you wish to create log files with the right permissions.

### DB2ADMIN password should not begin with dash character

The IBM Tivoli Storage Productivity Center installation program fails when the DB2ADMIN password used begins with a dash character.

## Problem

The Tivoli Storage Productivity Center installation program fails when the DB2ADMIN password begins with a dash character (-).

## Action

Change the DB2ADMIN password to not begin with a dash character. Then rerun the Tivoli Storage Productivity Center installation program.

## When installing Fabric agent remotely, progress bar not shown

When installing the Fabric agent remotely, the status screen does not show a progress bar.

## Problem

The status screen shows a percentage instead of a progress bar.

### Action

No action is required. The installation should complete successfully.

## IBM Tivoli Storage Productivity Center agent installation fails when files are mapped to a drive in a Windows Terminal Services environment

The IBM Tivoli Storage Productivity Center agent installation fails when files are mapped to a drive in a Windows Terminal Services environment.

### Problem

The IBM Tivoli Storage Productivity Center agent installation fails when files are mapped to a drive in a Windows Terminal Services environment.

### Action

There are two ways to correct this problem:

- Map the installation source files through the UNC path (for example, \\<server\_name>\<disk>) rather than using the drive letter (do not use net use x:\\<server\_name>\<disk>).
- 2. Manually copy the installation files manually to the target host and run the installation program locally.

For more information about this problem, see http://support.installshield.com/kb/ view.asp?articleid=Q107137.

# Using Windows domain user ID when installing IBM Tivoli Storage Productivity Center

You cannot specify a domain user ID when installing IBM Tivoli Storage Productivity Center.

### Problem

The only places that you can specify a domain user ID are on the following installation panels:

- For remote agent installation, the Windows Service Account and Listener Port panel
- Common agent service information panel

## Message: GEN0039E: Unknown host <host\_name>

For Solaris systems, GEN0039E messages are logged in the discovery logs and the discovery job takes a long time.

## Problem

The Data agents are installed on the Solaris servers within an NIS environment. During discovery on these Solaris agents, the agents tries to contact the list of hosts that are defined in automaps using SNMP.

## Action

To resolve this problem, see "Planning for the Data agents on Solaris" on page 61.

# Remote system runs out of space when installing a Fabric agent

When remotely installing a Fabric agent, the remote system runs out of space.

## Problem

The Fabric agent APIs are not able to check space on the remote system. Therefore, the remote system runs out of space.

## Action

When performing an initial remote installation of both the Data agent and Fabric agent, allow at least 350 MB of space on the remote system.

## A Java core dump is received when installing IBM Tivoli Storage Productivity Center on Windows

When installing the IBM Tivoli Storage Productivity Center server on Windows, a Java core dump is received.

### **Problem**

When paging is not correctly set, an error occurs when installing the IBM Tivoli Storage Productivity Center server.

Ensure that the paging file size is set to the recommended size for Windows. The paging file size is usually 1.5 times the memory size. For example, if you have 4 GB of memory, you should have a 6 GB paging file size. When you change the paging file size, the Virtual Memory window shows the recommended paging file size.

To see the Virtual Memory window, right-click on the **My Computer** icon on the desktop. Click **Properties**. On the Advanced tab, click **Settings** in the Performance section. On the Advanced tab, click **Change** in the Virtual Memory section.

# DB2 services do not start when you restart the system on a UNIX platform

The DB2 services do not start when you perform a system reboot on UNIX.

### Problem

On UNIX operating systems, the instance is not enabled for autostart by default.

## Action

On UNIX operating systems, to enable an instance to start automatically after each system restart, enter the following command:

db2iauto -on <instance\_name>

where <instance\_name> is the login name of the instance.

## **Restarting Windows 2008**

After restarting Windows 2008, you do not see the file systems that you created if the disks go offline during the restart process.

## Problem

If you used IBM Tivoli Storage Productivity Center to assign volumes from various storage systems and display the file systems on the disks from these volume assignments, then restart the Windows 2008 system, the file systems are not visible when the disks on which they were created goes offline.

## Action

To resolve this problem, manually bring the disks back online after you restart the system.

Other actions you might need to perform include the following ones:

- Remote volumes must be attached so that the Windows system can recognize them. For example, set the host connection type to the platform where the assignment was made. If a volume is attached using AIX (to report on LUNs), a Windows system cannot correctly identify the disk.
- Multiple paths must be managed with a multipath driver. If each path surfaces a unique disk, this results in problems in which the operating system cannot identify the logical representation of the device on one path with the logical representation of the device on another path.
- The persistent binding properties on the HBA must be set so that the same LUN information is consistent each time you restart the system. Use the vendor HBA utilities to perform this operation.

## Cannot install server on an AIX 64-bit system

You cannot install the IBM Tivoli Storage Productivity Center server on an AIX 64-bit system.

### Problem

This problem occurs with the DB2 db2nodes.cfg file in which the host name must be the short name and not the long host name. You will see this error message:

DB2 database manager must be active in order to continue the installation process.

 $\ensuremath{\mathsf{Please}}$  ensure that DB2 instance is running before continuing the installation.

## Action

To resolve this problem, follow these steps:

1. Find the short host name on the AIX system by running the following command:

hostname -s

Add the short host name returned by the **hostname** -s command to the /etc/hosts file. Add the short host name (for example, myhost) and not the long host name. Save the file.

The /etc/hosts file might contain a line that specifies the long host name; however, you must also include a line for the short host name. If a short host name is not already included in the file, you must add it.

2. Log in as the DB2 instance owner, which is by default "db2inst1." Change db2nodes.cfg so that it is enabled for writing:

```
# su - db2inst1
> chmod 611 /home/db2inst1/sqllib/db2nodes.cfg
```

3. Open the db2nodes.cfg file. This file should contain the short host name (for example, myhost) and not the long host name (for example, myhost.my.com). Correct the file name to contain the short host name and save the file. If this file does not contain the short host name found in step 1, correct the file name and save the file. For example, if the db2nodes.cfg file contains this:

```
>cat db2nodes.cfg
0 myhost.my.com 0
```

Correct or add this to the file:

>cat db2nodes.cfg
0 myhost 0

4. Install Tivoli Storage Productivity Center.

## Cannot install the Storage Resource agent on AIX through RSH

You cannot install the Storage Resource agent on an AIX system that has the Remote Shell (RSH), but does not have the Secure Shell (SSH).

## Problem

The AIX agent system does not have SSH but does have RSH. You can connect with RSH from the server through a command line, but the Storage Resource agent deployment fails with the following message:

 $\mathsf{RSH} : \ldots$  Could not establish a connection to the target machine using the credentials supplied

### Action

Check the .rhosts file on the AIX agent system to see if it allows the server and user to connect to AIX through RSH. The \$HOME/.rhosts file defines which remote hosts (computers on a network) can invoke certain commands on the local host without supplying a password.

The format of the \$HOME/.rhosts file is: <host\_name\_field> [<user\_name\_field>]

Ensure that you add the server and user name to this file and save the file. Deploy the Storage Resource agent again.

## Database schema installation fails on Linux

The database schema installation fails on Linux.

DB2 9.5 needs a larger amount of shared memory space to be allocated on Linux.

### Action

Modify the shared-memory kernel parameter for Linux (SHMMAX).

The minimum required shared memory space on x86 systems (32-bit) is 268435456 (256 MB). For best results, use 536870912 (512 MB); for 64-bit systems, use 1073741824 (1 GB). To modify the maximum value for the shared memory to 512 MB on 32-bit systems, add or modify the following line to /etc/sysctl.conf. kernel.shmmax=536870912

Run the **sysctl** -**p** command (using the root user ID) to see if the value was set properly.

**Note:** An insufficient value for this parameter might cause DB2 generate the SQL1084C error. If you get this error, increase the value of the SHMMAX parameter up to the size of the physical memory of the system.

See the following topics for more information about modifying kernel parameters for Linux:

- http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp?topic=/ com.ibm.db2.luw.qb.server.doc/doc/t0008238.html
- https://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp?topic=/ com.ibm.db2.luw.messages.sql.doc/doc/msql01084c.html

## Remote Data agent installation fails on UNIX or Linux

The remote Data agent installation fails after an uninstallation of the IBM Tivoli Storage Productivity Center Common agent or server from the target machine.

#### Problem

The remote Data agent installation fails with the following messages in the log file:

```
10/3/08 11:35:51 AM INS8050I: Connecting to grifter using Windows protocol.
10/3/08 11:35:51 AM INS8051W: Connection to grifter failed using Windows
protocol: java.net.ConnectException: CTGRI0001E The application could not
establish a connection to grifter..
10/3/08 11:35:51 AM INS8050I: Connecting to grifter using SSH protocol.
10/3/08 11:35:53 AM INS8052I: Connected to grifter using SSH protocol.
10/3/08 11:35:53 AM INS3052I: grifter was added to selected list.
10/3/08 11:35:55 AM INS1138I: Status of computer grifter changed to Getting
GUID on remote computer..
10/3/08 11:35:55 AM INS1138I: Status of computer grifter changed to Getting
a list of common agents.
10/3/08 11:40:55 AM GEN0324E: Failed to send request <1:31> to host <host name>
10/3/08 11:40:55 AM GEN0008E: Cannot read from host <host name> java.net.
SocketTimeoutException: Read timed out
10/3/08 11:40:55 AM INS5107E: Could not get list of common agents
10/3/08 11:40:55 AM INS1138I: Status of computer grifter changed to Could not
get list of common agents.
. . .
```

## Action

GUID information has been left after an uninstallation of the Tivoli Storage Productivity Center Common agent or server from the target machine. To delete the GUID information, delete the following directory from /opt:

/tivoli/guid

# Cannot install Tivoli Storage Productivity Center on Red Hat Linux V5

You cannot install Tivoli Integrated Portal on Red Hat Linux V5.

## Problem

The Tivoli Storage Productivity Center installation program is not able to run on Red Hat Linux V5 because of a dependency on the shared library libXp.so.6 which is not installed by default.

## Action

Before installing Tivoli Storage Productivity Center, install the 32-bit version of libXp.so.6 which is available on the Red Hat installation media: <DVD>/Server/libXp-1.0.0-8.1.el5.i386.rpm.

## Common agent does not start on Windows

The common agent does not start on Windows.

## Problem

The common agent does not start and you see this error message in the log: Error is not a valid Win32 application

## Action

Check for files that are named "Program." If you find a file by that name, rename or delete the file. This file causes the Windows interpreter to fail.

## Storage Resource agent failed to install using install command

The Storage Resource agent failed to install when using the install command.

### Problem

When you specify the install command for the Storage Resource agent, check to see if you specified an agent installation location that contains an ending slash ( $\)$ . For example, C:\agent1\. This causes the installation to fail.

## Action

Do not specify an ending slash when you specify the agent installation location. For example, specify C:\agent1.

# Installing and uninstalling IBM Tivoli Storage Productivity Center for Replication multiple times

You might get an error message when you install or uninstall IBM Tivoli Storage Productivity Center for Replication multiple times.

On rare occasions, installing on AIX might result in a null pointer exception. This might occur when the product has been installed and uninstalled multiple times. You would see an error message similar to this one:

java.lang.NullPointerException at com.installshield.product.service. registry.VPDDef.pack(Unknown Source)

### Action

If you encounter this error message, you can work around it by deleting the full name (VPD) registry directory (Gen1) and then installing again.

The VPD registry directory location is Gen1 in the following path: /usr/lib/objrepos/InstallShield/Universal/common/Gen1

#### Error message: Exception Processing Message c0000013

When you install IBM Tivoli Storage Productivity Center, you get this error message in a pop-up window: Windows - No Disk.

#### Problem

You might see this message when you install IBM Tivoli Storage Productivity Center. You can ignore this message.

#### Action

Click **Continue** to complete the installation process.

### Data server installation fails on Red Hat Linux

When you install IBM Tivoli Storage Productivity Center, the Data server installation fails.

### Problem

The Data server fails to install on Red Hat Linux version 4 and 5. You see these error messages in the installation log:

2/17/09 4:51:27 AM INS2089I: IBM Tivoli Storage Productivity Center -Data Server start up scripts created.

/opt/IBM/TPC/data/server/tpcdsrv1: line 41: /opt/IBM/TPC/jre/java15/bin/java: Success

2/17/09 4:51:28 AM INS2087E: Start up script /opt/IBM/TPC/data/server/tpcdsrv1 failed.

## Action

For Red Hat Linux version 4 and 5, if SELinux is set to anything other than "disabled", the installation of the Data server fails. For more information about the SELinux parameter, see http://www.crypt.gen.nz/selinux/disable\_selinux.html.

# After upgrading agents remotely, get inconsistent version.txt files

After upgrading the agents remotely, the version.txt files are inconsistent.

After you upgrade the agents remotely, the version.txt files are inconsistent in the <TPC\_install\_directory> and the <TPC\_install\_directory>\ca\subagents\TPC\ Data\ directories.

#### Action

This is a limitation of the installation process.

## Installation fails on Windows with 4 GB of RAM

When installing IBM Tivoli Storage Productivity Center on Windows, you receive a warning message that you have 4-6 GB of RAM.

#### Problem

You have 4 GB or more of RAM on Windows but cannot install IBM Tivoli Storage Productivity Center. You have verified that you have 4 GB or more of RAM by running the **systeminfo** command on Windows.

## Action

Check the configuration parameters Data Execution Prevention (DEP) and Physical Address Extension (PAE) on Windows and reset as appropriate. For information about these parameters, see http://msdn.microsoft.com/en-us/library/ aa468629.aspx and http://www.microsoft.com/whdc/system/platform/server/ PAE/PAEdrv.mspx.

# You cannot install Tivoli Storage Productivity Center on UNIX and Linux systems

You cannot install Tivoli Storage Productivity Center on UNIX and Linux systems. You receive an error message indicating that the DB2 user ID does not exist.

### Problem

You receive this error message: User ID db2inst1 does not exist on the system

You receive this error message even though the db2inst1 user ID exists and DB2 is working properly. This occurs because the shadow util package has not been installed and configured on the system. A shadow password file is a system file in which encrypted user passwords are stored. Normally, user information for each user is stored in an encrypted format in /etc/passwd. However, for shadow passwords, the shadow password file is moved to a separate database for local files, usually in /etc/shadow on Linux and UNIX systems. The shadow password file can only be read by the root user. The Red Hat Linux installation program enables shadow passwords by default which enhances the security of system authentication files, especially in a multiuser environment.

#### Action

Check to see if the shadow passwords are installed and configured on the system. If the file /etc/shadow exists on the system, then the shadow passwords are already installed and configured. If not, install and configure the shadow passwords. Install the shadow utils package from the operating system CD.

For example, if you have Red Hat Linux 5.1, follow these steps:

- 1. Install the shadow utils package (shadow-utils-<version\_release\_architecture>.rpm).
- 2. To configure the shadow passwords after installing the package, run the following commands:
  - /usr/sbin/pwconv /usr/sbin/grpconv

**Note:** The instructions and package name and version might differ between operating systems. Also the instructions for how to configure the shadow passwords might differ. Check the operating system CD or your vendor for instructions on how to install and configure the shadow passwords.

# After reboot of the system, Tivoli Storage Productivity Center cannot communicate with DB2

After a reboot of the system on Windows, DB2 starts up but Tivoli Storage Productivity Center cannot communicate with DB2.

### Problem

To determine if this is the issue, open a command prompt window and run the command **netstat -na**. Port 50000 should not be listed anywhere as a result of this command.

## Action

If port 50000 appears, follow these steps to enable the DB2 service port for remote connections:

- Open the Windows service file: C:\WINDOWS\system32\drivers\etc\services
- Search for the following line: db2c\_DB2 50000/tcp

Note the port number (the port number is probably 50000).

**3**. Open a DB2 command prompt window by running **db2cmd**. Run the following commands:

```
db2 update dbm cfg using SVCENAME db2c_DB2
db2set DB2COMM=tcpip
db2stop
db2start
```

### Note:

- If "db2c\_DB2" is not the service name of the DB2 instance name on the system, use the name listed in the service file.
- If on a subsequent reboot of the system, this problem occurs again, then DB2 is not storing this information in the configuration file. Try running these commands:

```
db2 update dbm cfg using SVCENAME db2c_DB2 deferred
 (This forces DB2 to update the configuration file.)
db2set DB2COMM=tcpip
db2stop
 (If DB2 displays an error message saying that the database manager was
 not stopped because the databases are still active, use the command
 db2stop force.)
db2start
```

- Determine if the problem is fixed by running netstat -na.
- Verify that port 50000 is listed. For example, your output should be similar to this:

TCP 0.0.0.0:50000 0.0.0.0:0 LISTENING

As long as that port is active, DB2 should be able to connect to Tivoli Storage Productivity Center.

## Upgrading troubleshooting

Use this section to troubleshoot and resolve problems when upgrading IBM Tivoli Storage Productivity Center.

## Installation error when copying files

This topic provides information when you receive an error message copying files during the installation upgrade process.

### Problem

You receive the following error message when you are copying files during the installation upgrade process:

Errors occurred during the installation. One or more errors occurred during the copying of files (beanCopyAgentBundles). Please refer to the install log for additional information.

When you copy a disk2 installation image into a disk1 folder, you will get this message when upgrading IBM Tivoli Storage Productivity Center.

### Action

After installation, check the following directory: c:\Program Files\IBM\TPC\data\upgrade

Make sure that the following subdirectories have an upgrade.zip file:

aix\_power hp-ux\_pa-risc linux\_i386 linux\_power linux\_s390 solaris\_sparc windows i386

If the upgrade.zip files are not in the subdirectories, copy the disk2 upgrade directory to c:\Program Files\IBM\TPC\upgrade.

## Assets not appearing in Rollup reports

This problem occurs when you upgrade to IBM Tivoli Storage Productivity Center 3.3 from a previous version.

### Problem

After upgrading to Tivoli Storage Productivity Center v3.3 or later from a previous version of the application, information about the storage assets monitored by a master server does not appear in Tivoli Storage Productivity Center > Rollup Reports.

## Action

You must run probes against a master server's monitored storage assets to have information about those assets appear in Tivoli Storage Productivity Center > Rollup Reports.

- 1. Start the Tivoli Storage Productivity Center user interface and log into the upgraded master server.
- 2. Go to Tivoli Storage Productivity Center -> Monitoring -> Probes.
- 3. Right-click Probes. A pop-up menu appears.
- 4. Select **Create Probe** and define information about that probe in the content pane. Make sure to select the assets whose information you want to appear in Rollup reports.
- 5. Save and run the probe.
- 6. Go to **Tivoli Storage Productivity Center** → **Rollup Reports** to view information about the assets monitored by the master server.

## Error message: "There is not enough space in the filesystem".

This problem can occur when installing or upgrading IBM Tivoli Storage Productivity Center.

### Problem

When installing or upgrading Tivoli Storage Productivity Center, you get this error message:

There is not enough space in the filesystem.

InstallShield does not provide the name of the file system that lacks the space.

### Action

If you get this error message, increase the /tmp directory. Retry the installation or upgrade.

## Get warning messages when upgrading IBM Tivoli Storage Productivity Center

This problem occurs when upgrading IBM Tivoli Storage Productivity Center.

#### Problem

When upgrading Tivoli Storage Productivity Center, you might get warning messages to replace the following files:

ibmlogo.gif
generalHelp.html
device\_discovery\_co
libUsers.dll
activation.jar
migrationLogging.properties

These files are in the following directories:

C:\Program Files\IBM\TPC\tool\tpcAssist\
C:\Program Files\IBM\TPC\tool\tpcAssist\lib\en\help\
C:\Program Files\IBM\TPC\tool\tpcAssist\lib\en\help\
screenshots\
C:\Program Files\IBM\TPC\tool\tpcAssist\lib\
C:\Program Files\IBM\TPC\cli\libs\
C:\Program Files\IBM\TPC\tool\dbMigration\conf\

## Action

Click Yes to each of the warning messages.

# JRE not upgraded after IBM Tivoli Storage Productivity Center upgrade

After upgrading IBM Tivoli Storage Productivity Center, the JRE is not upgraded.

## Problem

This problem occurs after a Tivoli Storage Productivity Center upgrade.

## Action

To work around this problem, follow these steps:

- 1. Manually stop the Data server.
- 2. If the Tivoli Storage Productivity Center user interface is open, close the user interface.
- 3. In a Command Prompt window, go to the installation directory.
- 4. Rename the jre file to jre\_old.
- 5. Run the installation program again and select at least one component to upgrade. (The CLI component is the smallest component to upgrade.)

The new JRE is installed.

## Error message: Cannot upgrade component Device server

After upgrading the IBM Tivoli Storage Productivity Center server, you see this error message.

## Problem

This problem occurs after a Tivoli Storage Productivity Center server upgrade. You see this error message:

Cannot upgrade component Device Server: Reason: File C:\Program Files\IBM\TPC\device\apps\was is in use. Make sure the component has shutdown then click next to continue.

## Action

To see if the service is running, follow these steps:

- Open the Services panel. Click Start > Run. Enter services.msc on the run dialog.
- 2. On the Services panel, look for the following service:

IBM WebSphere Application Server V6 - DeviceServer

3. Make sure the Device server is in the "Stopped" state on the Services panel.

# After upgrading Data agents remotely, trying to upgrade agents show wrong build

After upgrading the Data agents remotely, the custom installation window "Select one or more components to install on the local or remote computer" shows the wrong build for the Data agents. The Data agents box is selected and cannot be changed.

This is a limitation of the Data agent installation. The installation program does not update the InstallShield registry. The InstallShield registry is updated only when running a Fabric agent local installation or upgrade.

### Action

No action is required.

## Upgrading database schema fails on Windows 2003

When upgrading the TotalStorage Productivity Center database schema to IBM Tivoli Storage Productivity Center 4.1, the database schema upgrade fails.

### Problem

If you are upgrading the database schema from TotalStorage Productivity Center 3.3.x to Tivoli Storage Productivity Center 4.1 on Windows Server 2003, there is an issue with the maximum size of environment variables like the PATH variable. The maximum size of the PATH variable is 2048. However, in some cases, the PATH variable is truncated to 1024 characters.

## Action

You need to install a hot fix from Microsoft. For information about the hot fix, go to http://support.microsoft.com/kb/906469.

# Upgrading IBM Tivoli Storage Productivity Center on AIX causes system to hang

When upgrading IBM Tivoli Storage Productivity Center on AIX, the system hangs.

### Problem

This issue can occur if you do not have the latest AIX C++ run time library.

## Action

Make sure you have the latest AIX C++ run time library. The minimum level required is xlC.aix50.rte.9.0.0.5 or later.

### The Windows 2008 Start menu displays an invalid selection

After upgrading IBM Tivoli Storage Productivity Center on Windows 2008, the Windows **Start** menu displays an invalid selection.

### Problem

When you click **Start**, the menu displays two values for **IBM Tivoli Storage Productivity Center > Productivity Center**.

### Action

To avoid this situation, you can reboot your system to clear the menu or check the Windows menu setting before you upgrade. To check the menu setting, follow these steps:

- 1. On Windows, right-click on the Taskbar.
- 2. Click Properties.

- 3. Click Start Menu tab.
- 4. Clear the check box for Store and display a list of recently opened programs.
- 5. Click OK.
- 6. Run the IBM Tivoli Storage Productivity Center upgrade program.

## Memory, space and performance troubleshooting

Use this section to troubleshoot and resolve Java problems.

## Error Messages: Get SQLCODE: -964, SQLSTATE: 57011, Unexpected error occurred while performing [a function]

You might receive these error messages when performing tasks within IBM Tivoli Storage Productivity Center.

## Problem

When performing tasks within Tivoli Storage Productivity Center that require accessing and storing data in the database repository, you might receive error messages similar to the following:

[message #]: Unexpected error occurred while performing the following [functions]

where [message #] represents the number of the error message and [functions] represents a task that you were performing.

You might also see the following error message in the database installation log:

Instruction SQL : insert into t\_stat\_file\_temp SQLSTATE: 57011, Vendor error code: -964 DB2 SQL error: SQLCODE: -964, SQLSTATE: 57011, SQLERRMC: null

These error messages are a result of running out of space in the transaction log. The transaction log configuration is set as:

db2 update db cfg for \$DBNAME using logprimary 8 db2 update db cfg for \$DBNAME using logsecond 16

Each transaction log file is 10 MB ( logFileSize=2500 pages of 4 KB each). Eight (8) primary log files are allocated all the time; secondary log files are allocated as needed, and deleted when not needed, to the maximum of 16.

## Action

Increase the transaction log files. See the DB2 documentation for information about increasing the transaction log files.

## Java out-of-memory errors when running reports

These errors occur when running large reports.

### Problem

Reports which generate a lot of data can crash the tpctool CLI with Java out of memory errors.

## Action

To work around this problem, reduce the report size by requesting less information. For example, rather than specifying all columns for a report, you can specify less columns for the report.

### Java out-of-memory exception

You might run into a situation where you are seeing a Java out–of–memory exception for the Data Server, Device server, Data agent, or Fabric agent. You should investigate the cause of this before increasing the memory allocation for either the server or the agent.

If you need to substantially increase agent memory for one agent or several agents, then you will need to increase the memory on the server at **least** 25% greater than that of the largest agent memory setting. This is so the server will be able to handle the entire agent result set in memory.

The causes of an agent out–of–memory situation are almost always linked to a scan job. The possible reasons that a scan job can do this are as follows:

- Many directories are being scanned.
- Profiles assigned to scan are configured to bring back large file lists (up to 32767 in any profile entrée box).
- You are using a single scan jog to scan many local file systems or remote file systems.
- Many thousands of users own files on file systems being scanned.
- Several jobs are running simultaneously.
- Any combination of the above.

Remember that things like users, operating system groups, file systems, and directories are all buckets of information that the agent must create in memory. The more there are the more buckets the agent must create and maintain until the scan job is complete. Forethought and understanding in configuring the various jobs can usually avoid agent out–of–memory issues. However, there are situations where you must increase the agent's memory.

The causes for a server out-of-memory error are as follows:

- The history aggregation job in combination with the server receiving job results from agents.
- The agent result set for a scan is larger than the server available memory.

Some useful Java parameters are:

#### -Xmx256m

Sets the maximum memory allocation pool size to 256 MB.

#### -classic -Djava.compiler

Turns off optimization to allow stack traces to show all information.

For information about increasing memory allocation, see "Increasing memory allocation" on page 472.

#### Data server crashes on AIX

This error occurs when you are running the Data server on AIX.

The Data server crashes on AIX with the following messages in the system error logs:

ERROR LOGGING BUFFER OVERFLOW caused by EXCESSIVE LOGGING BY SOFTWARE PROGRAM.

## Action

Increase the paging space on the server.

## Improving scan or probe performance and memory usage

This topic provides information about space and performance.

## Problem

Things to understand about a scan:

- 1. A scan job will only scan one file system at a time.
- 2. A file system can only be under one scan job at a time.
- 3. An agent can run multiple jobs at a time.
- 4. Adhering to the above rules, a NAS device can have as many agents as it has file systems to scan, scanning each file system simultaneously.
- 5. A single scan jog will keep in memory all data from all file systems and directories until the scan job is complete. (Do not scan 50 NetWare or NAS machines with a single agent or scan job.)

### Action

The section below describes some performance scenarios.

A machine with 20 file systems on it and a local Data agent installed could have as many as 20 scan jobs running at the same time (one per each file system). You would need to create a job to scan each file system and schedule them to start at the same or different times.

A NAS device with 20 file systems could be scanned with as many as 20 agents at once, one agent and one job configured for each file system to be scanned, or as few as one agent running 20 scan jobs (one per file system) simultaneously.

**Note:** You can do any combination of these as long as items 1, 2 and 3 above are met. You may need to increase the agent memory allocation if you do this.

#### Memory usage scenarios (lowers memory usage)

On a system with large file systems with many users and files, you can run out of memory on the agent. Instead of scanning all the file systems with a single job, you can create several jobs (one per file system) and stagger the start times so that only one job is running at a time. This will keep the memory requirement low.

# Certain devices do not show up in the selection list when defining a performance monitoring job

This topic explains why devices do not show up in the selection list when defining a performance monitoring job.

Certain devices such as switches or subsystems do not show up in the selection list when defining a performance monitoring job.

### Action

The device will only show up in the selection list if it supports performance data collection. This situation can occur if the CIM agent is not at the proper version, or an incorrect namespace was used for discovery. Also check to see if the CIM agent discovery has completed successfully and a probe was completed successfully on the appropriate storage subsystem or fabric containing the switch.

## No performance data is retrieved

This error occurs when you try to get performance data.

## Problem

You are not successful in getting performance data.

### Action

For a successful performance data collection to occur, the device must have been discovered and probed successfully.

### Performance monitoring job fails immediately after it starts

This error occurs when you run a performance monitoring job and it fails immediately after it starts.

#### Problem

The performance monitoring job fails immediately after it starts.

#### Action

This problem usually occurs when there is a network connectivity problem with the CIM agent.

### Error message "performance data files could not be correlated"

This error occurs when you uninstall the agent using the IBM Tivoli Storage Productivity Center uninstallation program.

#### Problem

You get this error message for the SAN Volume Controller subsystem during performance data collection.

#### Action

For SAN Volume Controller subsystems, this error message can occur during performance data collection. This is usually a problem with mismatching timestamps for the I/O statistics dump files on the SAN Volume Controller itself. This problem can be resolved by setting the time zone properly on the cluster.

### Performance correlation step takes a long time

This error occurs when a performance correlation step is done.

The performance correlation step takes a long time.

## Action

The performance correlation step can take a long time to complete if there are a lot of volumes. This causes a delay in collecting the first performance sample. To work around this problem, place the CIM agent and IBM Tivoli Storage Productivity Center servers on faster machines. You can also use multiple CIM agents to monitor a set of storage subsystems.

## Cannot define a performance monitor for a switch

This error occurs when trying to define a performance monitor for a switch.

## Problem

You cannot define a performance monitor for a switch.

## Action

If you cannot define a performance monitor for a switch because it does not appear in the list of switches that can be monitored, do the following:

- Check to see that the SMI-S version supported by the switch vendor is 1.1 or higher.
- Check to see if the CIM agent supports the switch sub-profile.
- Check to see if the CIM agent discovery completed successfully.
- Check to see if a fabric probe was run on the fabric that contains the switch after the CIM agent discovery completed successfully for that switch. Then verify that this fabric probe also completed successfully.

## Subsystem performance monitor shows wrong configuration

The subsystem performance monitor shows the wrong configuration.

## Problem

The subsystem performance monitor shows the wrong configuration.

## Action

For the DS6000 and DS8000 subsystems, any place that IBM Tivoli Storage Productivity Center talks about "array" should really be "array site". This applies to all logs and reports, and so on.

## File system storing database tables runs out of space

This problem occurs on systems running AIX 5.x.

## Problem

The file system storing the database table spaces runs out of space. This is shown by the following kinds of errors as seen in the DB2 log called db2diag.log:

 2005-11-06-12.59.10.815891-420
 E36562387C690
 LEVEL: Error

 PID
 : 176316
 TID
 : 1
 PROC : db2pclnr 0

 INSTANCE:
 db2inst1
 NODE : 000
 NODE : 000

 FUNCTION:
 DB2 UDB, buffer pool services, sqlbClnrAsyncWriteCompletion, probe:0

```
MESSAGE : ADM6017E The table space "TPCTBSPTEMP" (ID "5") is full.
Detected on
container "/home/db2inst1/db2inst1/TPCDB/TPC/TPCTBSPTEMP"
(ID "0").
The underlying file system is full or the maximum allowed
space usage
for the file system has been reached. It is also possible
that there
are user limits in place with respect to maximum file size
and these limits have been reached.
```

This problem is seen on AIX 5.x with JFS file system. Large files need to be enabled on the file system because the table space files can get quite large. Enable large files on JFS or JFS2.

### Action

During installation of AIX 5.1 or later, ensure that JFS or JFS2 with large file system support is installed. Follow the AIX documentation for this purpose as well as to back up and restore data between file systems. It is recommended to ensure that the file system size (especially for /home) is not too small (for example, not less than 4 GB). Back up your existing data before you recreate your file system. For information on file systems, see: http://publib.boulder.ibm.com/infocenter/pseries/index.jsp? topic=/com.ibm.aix.doc/aixbman/admnconc/fs\_types.htm

## Error message: GEN7046E

This error occurs with Performance Manager.

## Problem

If you create a switch or subsystem alert using a Performance Manager trigger condition, then save it and change the trigger by editing it, this can cause the message GEN7046E to be displayed:

<code>GEN7046E=The device ID [{0}]</code> is not available for use with alert condition  $\{1\}$ 

## Action

You can avoid this problem by not editing alerts to change trigger conditions or devices. Just delete the old alert you do not want and create a new one.

## Old devices reappear in the list of selected devices

This problem occurs with Performance Manager.

### Problem

Editing switch or subsystem alerts causes old devices to appear in the list of selected devices.

If you create a switch or subsystem alert using a Performance Manager trigger condition, then save, edit, and reopen the alert, this can cause the old device to reappear in the list of selected devices.

### Action

You can avoid this problem by not editing alerts to change trigger conditions or devices. Just delete the old alert you do not want and create a new one.

# Cancelling Disk Manager reports crashes IBM Tivoli Storage Productivity Center

This problem occurs with Performance Manager.

## Problem

IBM Tivoli Storage Productivity Center could crash when canceling Disk Manager reports when you display Disk Manager reports in the GUI: **Disk Manager**  $\rightarrow$  **Reporting**  $\rightarrow$  **Storage Subsystem Performance**  $\rightarrow$  **By Volume.** For this condition to occur, you have run Performance Manager on the subsystem and have a lot of data. When you try to run this report, then cancel the report (red circle X on the upper left side), this could cause Tivoli Storage Productivity Center to crash. This condition is dependent on the machine resources, what the user has set the JVM heap size to, and the number of volumes and switches the user is collecting performance data on.

### Action

Do not cancel this report.

## DS4000 and FAStT troubleshooting

Use this section to troubleshoot and resolve DS4000 and FAStT problems.

## DS4000 and FAStT probe errors

These errors occur for DS4000 and FAStT.

## Problem

Probe failures for DS4000 and FAStT may be encountered if a job for creation of one or more volumes through the same Engenio Provider is running at the same time as the probe job.

### Action

Do not run a job for creation of volumes at the same time as a probe job using the same Engenio Provider.

## FAStT or DS4xxxx subsystem is not discovered

This problem occurs for FAStT or DS4xxxx on Windows systems.

### Problem

After rebooting the Windows system where an Engenio Provider is installed, a IBM Tivoli Storage Productivity Center discovery job did not discover the FAStT or DS4xxxx subsystem (or both subsystems) that are managed by the Engenio Provider.

## Action

Try restarting the Engenio Provider from the Windows Services panel.

# Assigning ports from a FAStT default group causes loss of access

This problem occurs with FAStT groups.

Assigning ports from a FAST default group causes loss of access to other default group volumes.

Whenever a host on FAStT has no special mapping, it is kept in the "Default Group". When the host is explicitly assigned to a volume, the host is moved out of the host group. Therefore, this condition will cause loss of access to all volumes that are assigned to the host group. When all mapping of a host that is not part of the Default Group are removed, the host will be moved to the default automatically. IBM Tivoli Storage Productivity Center has no impact on the Default Group handling.

## Action

Do not assign any volumes to the default group, to prevent inadvertent loss of volume access.

# Error message: ProviderException Description: Expose Paths failed

This error occurs for DS4000 and FAStT.

### Problem

Assignment of DS4000 or FAStT Volumes to a host port WWN fails with 'ProviderException Description: Expose Paths failed'.

#### Action

The storage subsystem is unable to assign a volume to a host port WWN that is not known. Do not assign FAStT or DS4000 volumes to hosts unless they are zoned with these hosts, or unless the assignment operation is in conjunction with a zoning change through IBM Tivoli Storage Productivity Center. If the assignment operation is still failing even when using these guidelines, use the IBM Tivoli Storage Manager for DS4000 or FAStT software to find and remove any 'PLACEHOLDER\_HOST' logical elements from the StorageManager software. Then retry the assignment.

## Error message: HWN021677E Volume creation failed

This error occurs for FAStT or DS4xxxx.

## Problem

A Volume Creation Job for a large number of volumes on a FAStT or DS4xxxx failed with 'HWN021677E Volume creation failed'. This is a known limitation with FAStT or DS4xxxxs that can occur when the subsystem becomes busy creating all of the volumes.

### Action

Try separating the job into several volume creation jobs. For example, if this problem is encountered when trying to create 100 volumes of size 1 GB each, try 10 separate volume creation jobs of 10 volumes with a size of 1 GB each.

## DS4000 and FAStT were not discovered

IBM Tivoli Storage Productivity Center did not discovery the FAStT or DS4000 subsystem.

## Problem

After rebooting the Windows system where an Engenio Provider is installed, a Tivoli Storage Productivity Center discovery job did not discover the FAStT or DS4000 subsystem (or both subsystems) that are managed by the Engenio Provider.

## Action

Try restarting the Engenio Provider from the Windows Services panel.

## Assigning multiple ports fails

This problem occurs when assigning multiple ports to a volume.

## Problem

The assignment of multiple ports to a volume, including initiator ports that are not known to the subsystem, failed. This condition was observed intermittently and could not be reliably recreated for certain host ports.

## Action

To work around this problem, try one of the following:

- Reprobe the subsystem. Identify the missing assignments and retry the procedure or
- Define the initiator ports directly on the subsystem through an Element Manager. Probe the subsystem again and then use these ports.

## Multipathing problems with FAStT

This problem occurs when using FAStT subsystems with Windows multipathing Subsystem Device Driver (SDD).

## Problem

Before the support of the data path explorer view, support for Subsystem Device Driver (SDD) was to discover devices managed by SDD. Now the data path explorer view support for SDD requires that all paths be discovered. This requires that the operating system identify all possible paths. The Windows operating system will not surface the possible paths through the device object manager for Physical Drives. Therefore, the IBM Tivoli Storage Productivity Center Data agent cannot discover the alternate paths when they have been masked by a multi-pathing software program like SDD (because they are masked from the operating system)

Problems could occur such as:

- There is no way to tell if a disk is under an alternate path.
- FAStT "access" volumes are not reported correctly.

## Action

This will be resolved in a future release.

## Error message: HWN021515E

This message can occur when you try to create volumes on the DS4000.

#### Problem

If there is no storage array created on the DS4000, you will see this error message:

```
HWN021515E The Invocation of CIM method GetSupportedSizeRange
failed on CIMOM
http://10.10.38:5988 with the following exception text:
org.sblim.wbem.cim.CIMException: CIM_ERR_FAILED(Remote
exception at the CIMOM:1:
getSupportedSizes not supportd: Pool: Null;;)
```

#### Action

Use the DS4000 Storage Manager GUI to create a storage array (which needs to be done before the DS4000 can be managed with IBM Tivoli Storage Productivity Center).

### Error message: HWN021514E when creating a volume

This message occurs when you try to create volumes on the DS4000.

### Problem

You are trying to create a volume on the DS4000 and you see this error message: HWN021514E The invocation of CIM method CreateOrModifyElementFromStoragePool failed on CIMOM https://9.11.123.210:5989 . The return code is 3.

A return code of 3 indicates a timeout between the CIMOM and the storage device.

#### Action

Use the DS4000 Storage Manager GUI to disable the password for the array.

# DS6000, DS8000, and Tivoli Storage Enterprise Storage Server troubleshooting

Use this section to troubleshoot and resolve DS6000, DS8000, and Tivoli Storage Enterprise Storage Server problems.

## Assigning multiple ports fails

This problem occurs when assigning multiple ports to a volume.

### Problem

The assignment of multiple ports to a volume, including initiator ports that are not known to the subsystem, failed. This condition was observed intermittently and could not be reliably recreated for certain host ports.

#### Action

To work around this problem, try one of the following:

• Reprobe the subsystem. Identify the missing assignments and retry the procedure or

• Define the initiator ports directly on the subsystem through an Element Manager. Probe the subsystem again and then use these ports.

## Subsystem performance monitor shows wrong configuration

The subsystem performance monitor shows the wrong configuration.

## Problem

The subsystem performance monitor shows the wrong configuration.

## Action

For the DS6000 and DS8000 subsystems, any place that IBM Tivoli Storage Productivity Center talks about "array" should really be "array site". This applies to all logs and reports, and so on.

## Error code 33294

This error occurs for the DS6000 or DS8000.

## Problem

Volume creation on the DS6000 or DS8000 fails with the following error: Errorcode 33294 (0x820E): 'Cannot find an available volume number to create volume'.

The logical subsystem (LSS) has hit the maximum volume limit.

## Action

To work around this problem, use another LSS, or remove unused and unassigned volumes from the selected LSS.

# Tivoli Storage Productivity Center and DS8000 warning messages

Whenever the DS8000 detects a drive failure, Tivoli Storage Productivity Center provides a warning indicator for a drive failure in the topology view.

### Problem

Whenever the DS8000 detects a disk drive failure, a repair action may or may not be immediately required. The DS8000 has spare drives that can be used to allow the service to be deferred. However, Tivoli Storage Productivity Center will present a warning indicator in the topology view.

## Action

For Tivoli Storage Productivity Center disk drive warnings related to the DS8000, no action is required. The DS8000 system will notify the user when service is needed (this depends on how you set up the alerts for the DS8000).

# Get out-of-memory conditions with the DS6000, DS8000 and SAN Volume Controller CIM agents

These errors occur for the DS6000, DS8000 and SAN Volume Controller CIM agents.

Get out-of-memory conditions with the DS6000, DS8000, and SAN Volume Controller CIM agents.

#### Action

If you are getting out-of-memory conditions, try increasing the Java heap size for the CIM agent. Increase the Java heap size by an increment of 256 MB. For example, if the Java heap size is "-Xmx256", try changing this to "-Xmx512". If you have enough memory, try increasing this to 1.5 GB of RAM with "-Xmx1536". Save the file and restart the CIM agent.

The DS6000, DS8000, and Tivoli Storage Enterprise Storage Server use the same CIM Agent.

For the CIM Agent 5.1, modify the Java heap size parameter in the startcimom file for AIX and Linux. For Windows, modify the cimom.bat file.

For the CIM Agent 5.2.x, use the **dscimcli** command to modify the **jvmargs** parameter. **Dscimcli** is documented in the installation guide for the 5.2.x CIM Agent.

If you are running a performance monitor job for the DS6000 or DS8000 and encounter out-of-memory conditions, you may be experiencing the following error messages from IBM Tivoli Storage Productivity Center:

HWNPM4165E: Unable to retrieve performance statistics data for this device: <device\_ID>.

HWNPM2052E: No performance data was collected from device <device\_name> for the current collection interval <timestamp> due to an error.

### Get warning messages STA0044I, STA0035W, and STA0036I

These warning messages occur when you perform an agent probe.

#### Problem

If a job log of an agent probe shows warnings similar to the following messages:

3/15/07 9:22:10 AM STA0044I: Reading capacity 3/15/07 9:22:10 AM STA0035W: Error reported by device \\.\PhysicalDrive24 3/15/07 9:22:10 AM STA0036I: Sense code: xxxx ASC: xxxx ASC2: xxxx

#### Action

There may be a problem with the operating system or the environment. The corresponding volumes should be checked.

### Invalid host connection to storage subsystem

When IBM Tivoli Storage Productivity Center creates an initial assignment on a DS8000, the host connection that is created might result with the default host connection type of AIX, which is not compatible with other host types like Windows and Linux.

This problem can also occur on non-DS8000 storage subsystems because Tivoli Storage Productivity Center might create invalid host connections if none is specified by the Tivoli Storage Productivity Center user.

There are two causes for this problem:

- 1. When creating an initial assignment on a DS8000 with no other monitored DS8000s with the same port assignment, the host type for the port is set to "unknown." If the host type is not specified in the assignment panel for the volume, the default host type is used when creating the host connection on the DS8000.
- 2. When creating an initial assignment on a DS8000 with other monitored DS8000s that have incorrectly created a port assignment, the host type for the port is set to "AIX." Tivoli Storage Productivity Center does not allow the host type to be specified in the assignment panel, and the host connection type has to be removed using the DSCLI on the other monitored DS8000s because the DS8000 GUI does not allow this removal.

The reason that this occurs is that the SMIS standard only defines some basic host types, while more specific types like VMware are vendor specific. For example, a host assigned with "VMware ESX" host type on SAN Volume Controller has a Client Type 32780, but this client type cannot be used for the DS CIMOM. The reason the client type cannot be used is because this is defined as "IBM iSeries - iLinux" and Client Type 32778 has to be used on the DS CIMOM for "VMware."

### Action

Avoid the following activities when creating new host connections using Tivoli Storage Productivity Center:

- Assigning volumes to ports from different host types.
- Assigning volumes to ports with no possible connectivity to the storage subsystem.

These activities can be done after the correct host connection type has been defined either through Tivoli Storage Productivity Center, the DS8000, or the DSCLI.

To work around this problem, remove all Bad Host Connection Types from the monitored DS8000s. Follow these steps:

- 1. Unassign the bad host connection ports from all volumes using Tivoli Storage Productivity Center.
- 2. Run the following DSCLI command for each port:

rmhostconnect -dev <storage\_system\_id> <host\_connection\_id>

Note: Alternatively, the DSCLI command chhostconnect -dev <storage\_system\_id> -profile "Valid\_Profile" <host\_connection\_id> could be run for each port so that steps 5–7 are not required. However, this would not be testing Tivoli Storage Productivity Center's ability to create new host connections on the DS8000. If you do not want Tivoli Storage Productivity Center to create any new host connections, then the DS8000 should be set up with host connections for all possible host ports before using Tivoli Storage Productivity Center.

3. Restart the DS CIM agent.

**Note:** This should not be required, but sometimes the CIM\_StorageHardwareID objects remain until a restart is performed.

- 4. Reprobe the DS8000s.
- 5. Create the initial host connection type with the correct host type. Multiple ports can be assigned, but they all must be ports of the same host connection type.

**Note:** For the work around where the DS8000 does not recognize the "Intel - SUSE Linux" type, a Linux type should be specified, but it should be consistent across all monitored storage subsystems. For example, do not create "pSeries - pLinux" on one storage subsystem and "Intel - Linux Red Flag" on the other subsystem for the same host port. If such a state exists, the assignments should be removed as indicated in steps 1–4.

6. Restart the DS CIM agent of the DS8000 where the assignment occurred.

**Note:** This should not be required, but sometimes the CIM\_StorageHardwareID objects remain until a restart is performed.

7. Reprobe the DS8000 where the assignment occurred.

**Note:** This should not be required, but given the problem requiring a restart of the DS CIM agent, the change in host type is not immediately reflected in the volume assignment panel.

8. After the host connections have all been defined and correctly identified, volumes can be created and assigned using the existing host connections, regardless of the specification because the default host connection type will be the one that exists in the DS8000.

## SAN Volume Controller troubleshooting

Use this section to troubleshoot and resolve SAN Volume Controller problems.

### All ports of a host lose access to the volume

This problem occurs with SAN Volume Controller.

#### Problem

Unassigning one or more ports of a host unassigns all ports of the host.

If you use the SAN Volume Controller user interface or theSAN Volume Controller CLI to create a host that has several ports, and then unassign one or more ports of a host using IBM Tivoli Storage Productivity Center, all ports of the host will lose access to the volume.

#### Action

Do not create hosts with several ports.

### Error message: HWNPM4117W

This error occurs with the SAN Volume Controller.

#### Problem

Currently the message, "HWNPM4117W Encountered incomplete SVC performance data sample." is logged every time a poll for performance statistics is made against an SAN Volume Controller storage subsystem and the statistics are not ready to be copied over from the device. This does not necessarily indicate an error, because

the performance statistics collection task will continue to retry retrieving the statistics until they are ready. If the performance monitor is unable to retrieve the statistics for a given interval collection, a different error message will be logged to indicate that fact.

The time stamps on the v\_stats and Nm\_stats files are not the same. This is caused by a failure to associate SAN Volume Controller performance data from the non-configuration node with SAN Volume Controller performance data from the configuration node. Incomplete SAN Volume Controller performance data sample is given.

## Action

Run the following command: svctask settimezone -timezone 509

This command forces the cluster into the Universal time zone. Then run the following command: svctask settimezone -timezone <required timezone>

This command will set the time zone to what you want the cluster to be in. Look at the VPD file and the **svqueryclock** command. If they agree, then the files should be back in synchronization.

## Probe jobs for SAN Volume Controller takes a long time

This problem occurs for the SAN Volume Controller.

## Problem

Probe jobs are taking a long time for the SAN Volume Controller.

## Action

The CIM agent responses might be slower due to heavy SAN Volume Controller GUI usage.

# Get out-of-memory conditions with the DS6000, DS8000 and SAN Volume Controller CIM agents

These errors occur for the DS6000, DS8000 and SAN Volume Controller CIM agents.

## Problem

Get out-of-memory conditions with the DS6000, DS8000, and SAN Volume Controller CIM agents.

## Action

If you are getting out-of-memory conditions, try increasing the Java heap size for the CIM agent. Increase the Java heap size by an increment of 256 MB. For example, if the Java heap size is "-Xmx256", try changing this to "-Xmx512". If you have enough memory, try increasing this to 1.5 GB of RAM with "-Xmx1536". Save the file and restart the CIM agent.

The DS6000, DS8000, and Tivoli Storage Enterprise Storage Server use the same CIM Agent.

For the CIM Agent 5.1, modify the Java heap size parameter in the startcimom file for AIX and Linux. For Windows, modify the cimom.bat file.

For the CIM Agent 5.2.x, use the **dscimcli** command to modify the **jvmargs** parameter. **Dscimcli** is documented in the installation guide for the 5.2.x CIM Agent.

If you are running a performance monitor job for the DS6000 or DS8000 and encounter out-of-memory conditions, you may be experiencing the following error messages from IBM Tivoli Storage Productivity Center:

HWNPM4165E: Unable to retrieve performance statistics data for this device: <device\_ID>.

HWNPM2052E: No performance data was collected from device <device\_name> for the current collection interval <timestamp> due to an error.

## Error message: performance data files could not be correlated

This error occurs with the SAN Volume Controller.

#### Problem

For SAN Volume Controller subsystems, this error message can occur during performance data collection.

#### Action

This is usually a problem with mismatching timestamps for the I/O statistics dump files on the SAN Volume Controller itself. This problem can be resolved by setting the time zone properly on the cluster.

# General IBM Tivoli Storage Productivity Center symptoms following SAN Volume Controller CIM upgrade

Having two or more SAN Volume Controller CIM agents of different release versions (4.2.0 and 4.2.1) manage the same SAN Volume Controller cluster causes general failures in IBM Tivoli Storage Productivity Center. The failures can occur in volume creation, volume deletion, host port assignment, host port unassignment, and while running performance monitor jobs.

### Problem

After installing a new SAN Volume Controller CIM agent, failures occur in volume creation, volume deletion, host port assignment, host port unassignment, and while running performance monitor jobs.

#### Action

The SAN Volume Controller IBM CIM Agent 4.2.1 is compatible with SAN Volume Controller firmware levels 4.1.1.x, 4.2.0.x, and 4.2.1.x. Do not manage the same SAN Volume Controller cluster with SAN Volume Controller CIM agents of different release versions.

To recover from this problem:

1. Remove or replace SAN Volume Controller CIM agents so that all SAN Volume Controller CIM agents that manage the same SAN Volume Controller clusters are on the same release level (version 4.2.0 or 4.2.1).
- 2. Rerun the Tivoli Storage Productivity Center discovery process.
- **3**. Rerun the Tivoli Storage Productivity Center probe against the clusters that had the mismatched SAN Volume Controller CIM agent versions.

#### SAN Volume Controller reports are incorrect

The SAN Volume Controller reports are incorrect.

# Problem

An example of an incorrect report is when the report shows 0 for the allocated volume space when the report should show a value.

#### Action

When you have hosts connected to storage subsystems that have multipathing enabled, install the multipathing subsystem device drivers (SDD) on the hosts.

# Storage Optimizer

Use this section to troubleshoot and resolve Storage Optimizer problems.

#### Optimization report contains no recommendations

The Storage Optimizer optimization report contains no recommendations.

# Problem

The Storage Optimizer optimization report contains no recommendations. Some typical reasons for this are the following:

- the performance threshold value used as input to the optimization report was set too low or too high
- there is not enough disk space in the target pools, so none of the source pools can be migrated
- the source and target storage subsystems are incompatible

Furthermore, if "Space" is the only utilization metric that exceeds the specified performance threshold, Storage Optimizer will not provide recommendations based on space alone, since it is not designed to be used as a space planner.

#### Action

Storage Optimizer attempts to provide optimization recommendations based on the inputs provided, but it may not be able to create recommendations in all cases. Keep in mind that generating an optimization report is an iterative process. Try one or more of the following actions to increase the likelihood that recommendations will be created:

- specify different values for the performance threshold
- specify different combinations of source and target entities

#### Performance heat map cells are all white

The heat map in a Storage Optimizer analysis report consists only of white cells, which means that no data was returned.

# Problem

Each cell in a Storage Optimizer heat map represents a storage pool. If all the cells in an analysis report heat map are white, then some possible reasons are:

- no data was returned by the storage subsystem performance monitor used as input in the analysis
- data values of zero were returned by the subsystem performance monitor for the time interval chosen for the Storage Optimizer analysis

#### Action

To determine if subsystem performance data exists for the time interval chosen for the Storage Optimizer analysis, generate storage subsystem performance reports, as follows:

- 1. Navigate to **Disk Manager > Reporting > Storage Subsystem Performance**.
- 2. Using daily summation, generate the following storage subsystem performance reports:
  - By Storage Subsystem
  - By Array
  - By Volume
- 3. Include the following columns in each report:
  - Read I/O rate (normal)
  - Read I/O rate (sequential)
  - Read I/O rate (overall)
  - Write I/O rate (normal)
  - Write I/O rate (sequential)
  - Write I/O rate (overall)
  - Read Cache Hits Percentage (overall)
  - Write Cache Hits Percentage (overall)
  - Cache to Disk Transfer Rate
- 4. Use the information provided in the reports to determine if you need to adjust the time interval used for the Storage Optimizer analysis, make other adjustments to the Storage Optimizer analysis settings, or make adjustments to the settings used for subsystem performance monitors.
- 5. Run the Storage Optimizer analysis again.

# Analysis report includes additional subsystems

The analysis report for a SAN Volume Controller includes additional subsystems.

#### Problem

In the analysis report for a SAN Volume Controller, additional subsystems are listed. These additional subsystems are included in the analysis report because they are the back-end storage to the SAN Volume Controller.

If no performance data was collected for these back-end subsystems, or if the back-end subsystems are non-IBM devices, the utilization percentages for these subsystems will be listed as "N/A" (not applicable) in the analysis report.

# N Series Gateway servers troubleshooting

Use this section to troubleshoot and resolve N Series Gateway server issues.

# Rollup reports display two entries for N Series Gateway server

The rollup reports display two entries for the N Series Gateway server if you add the N Series Gateway server after previously removing it from IBM Tivoli Storage Productivity Center.

# Problem

You also install the agents for the server using different agent types (Windows and UNIX).

When the N Series Gateway server is added using first the Windows agent, then the N Series Gateway server is seen as having the Name Server (the fully-qualified name with the domain name, for example, xxx.srm.storage.ibm.com). If you later add the server again using the UNIX agent, this Name does not change.

If the N Series Gateway server is added using the UNIX agent first, then the N Series Gateway server is seen as having the Name Server (the fully-qualified name without the domain, for example, xxx.storage.ibm.com). If you later add the server again using the Windows agent, this Name does not change.

If at a later time the N Series Gateway server is removed from IBM Tivoli Storage Productivity Center, and then added back into IBM Tivoli Storage Productivity Center by reversing the order of the agent type, then the name server for the N Series Gateway will be different from the first time the N Series Gateway server was monitored. This results in two rows for the same N Series Gateway agent with different names (for example, xxx.srm.storage.ibm.com and xxx.storage.ibm.com) in the rollup reports.

For example, if you had added the N Series Gateway server using a Windows agent first, the name of the N Series Gateway server will contain the domain (xxx.srm.storage.ibm.com) and then add it using the UNIX agent, the name remains the same. But, if you remove the N Series Gateway server, and then add it back into IBM Tivoli Storage Productivity Center using the UNIX agent first, and then the Windows agent, the name of the N Series Gateway server will be the fully-qualified name but without the domain (xxx.storage.ibm.com). In this case, the rollup reports will display two entries (xxx.srm.storage.ibm.com and xxx.storage.ibm.com). The correct data is the one that appears under the N Series Gateway server name as it appears in the Data Manager reports. In this case, the correct data would be under the name discovered by the UNIX agent (xxx.storage.ibm.com).

# Action

To avoid this problem, when you remove the N Series Gateway server, then add it back, add the server back using the agents in the same order. For example, when you add the N Series Gateway server using the Windows agent first and then the UNIX agent second, then when you add the server a second time, use the Windows agent first also. If you do not follow this order, then the rollup reports will display two entries for the same N Series Gateway server (with different names). You can find the correct values under the name of the N Series Gateway server as it appears in all the Data Manager reports.

# XIV Storage System troubleshooting

Use this section to troubleshoot and resolve XIV Storage System problems.

# Error message when starting element manager for XIV Storage System

An error message is displayed when you try to start the element manager for an IBM XIV Storage System.

# Problem

You see this error message when you try to start the element manager for an XIV Storage System:

The element manager failed to launch when executing "xivgui" as a command. Ensure that the application is installed on the same server as the Tivoli Storage Productivity Center GUI and is correctly configured to work with the GUI.

"xivgui" is the XIV Storage System graphical user interface (GUI) application that serves as the front-end to XIV Storage System devices. When an XIV device is discovered, Tivoli Storage Productivity Center configures the xivgui application as the element manager for the XIV GUI device. Tivoli Storage Productivity Center assumes that the xivgui application is installed on the same server where Tivoli Storage Productivity Center is installed.

This error message appears if one of the following has occurred:

- xivgui is not installed on the same server as Tivoli Storage Productivity Center
- xivgui is installed on the same server but Tivoli Storage Productivity Center cannot locate the xivgui application because it is not specified in the system path

On Windows systems, the file name of the xivgui application is "xivgui.exe". On Linux systems, the file name of the xivgui application is "xivgui".

# Action

- 1. Verify that the xivgui application is installed on the same server as Tivoli Storage Productivity Center.
- 2. Verify that the xivgui application is specified in the system path.
- 3. (Linux only) Restart Tivoli Storage Productivity Center.
- 4. Start the element manager for an XIV Storage System.

# Tape troubleshooting

Use this section to troubleshoot and resolve tape problems.

# Tape library probe status not updated if probe fails

This problem occurs when a tape library probe is successful even though the tape library is offline.

# Problem

A tape library probe job is reported successful even if IBM Tivoli Storage Productivity Center looses the connection to the tape library. The test if the library is online is done at the very beginning of the probe job. All problems encountered later will make the probe job fail, but not change the status of the library. This will be updated by the next discovery or probe job. If the tape library is already gone when the probe job starts, then it will be correctly reported as missing.

# Action

Run another discovery job for the tape library to detect if the tape library is missing or disconnected.

# Not all drives for a TS3500 Tape Library are shown

This error occurs for a TS3500 Tape Library.

#### Problem

IBM Tivoli Storage Productivity Center may list one drive less for a given tape library than its TS3500 Specialist displays.

# Action

Upgrade the SMI-S Agent for Tape to version 1.2.1.

# No tape cartridges are collected during a tape probe

This error occurs during a TS3500 Tape Library probe.

# Problem

In case the set of tape libraries registered with a given instance of the IBM SMI-S Agent for Tape is modified, the agent may no longer return information about cartridges to IBM Tivoli Storage Productivity Center, even though there are cartridges in the library. The same symptom may occur if one of the libraries registered with the agent cannot be reached by the agent, for example, because of network problems.

# Action

Restart the agent. If this does not resolve the problem, try to identify which library cannot be reached by the agent and either remove it from the agent's registration, or fix the connection problem.

# Have two tape cartridges with same serial number, report shows one tape cartridge

If you have two tape cartridges with the same serial number, and a probe is done on the tape library, IBM Tivoli Storage Productivity Center shows one less tape cartridge in the report.

# Problem

You will see one less tape cartridge in the IBM Tivoli Storage Productivity Center report.

# Action

Assign different serial numbers to the two tape cartridges that have the same serial numbers.

# **Tivoli Integrated Portal troubleshooting**

Use this section to troubleshoot and resolve problems with IBM Tivoli Integrated Portal.

# Data server and Device server are inaccessible from Tivoli Integrated Portal

This problem occurs when you attempt to start IBM Tivoli Storage Productivity Center from IBM Tivoli Integrated Portal

# Problem

An error message displays because the Tivoli Storage Productivity Center Data server and Device server are inaccessible when you try to start Tivoli Storage Productivity Center from Tivoli Integrated Portal. The status of both the Data server and the Device server also displays.

# Action

If the status of the Device server and Data server is inaccessible and you started Tivoli Integrated Portal from a remote computer, it is possible that a fully-qualified domain name was not defined for the Tivoli Storage Productivity Center server during installation. A fully-qualified domain name consists of two parts: the host name and the domain name. An example of a fully-qualified domain name is xyzhost.xyzcompany.com, where xyzhost is the host name and xyzcompany.com is the domain name.

Check the following portlet.xml files to determine if the Device server and Data server names are fully-qualified domain names:

- <TIP\_install\_dir>/systemApps/isclite.ear/TpcWebLaunch.war/WEB-INF/
  portlet.xml (this is the master file)
- <TIP\_install\_dir>/profiles/TIPProfile/config/cells/TIPCell/applications/ isclite.ear/deployments/isclite/TpcWebLaunch.war/WEB-INF/portlet.xml(this is the run-time copy of the master file)

If the names are not fully-qualified, you must edit both portlet.xml files as follows:

- 1. Open the master portlet.xml file in a text editor.
- Find the <portlet-preferences> tag and change the hostname values for DataServerAddress , LICURL (this is the Device server address), and TPCRServerAddress. The following are example values shown in bold:

```
<portlet-preferences>
   <preference>
   <name>DataServerAddress</name>
   <value>xyzhost.xyzcompany.com:9549</value>
   </preference>
   <preference>
    <name>LICURL</name>
   <value>xyzhost.xyzcompany.com:9550</value>
   </preference>
    <preference>
      <name>TPCRServerAddress</name>
      <value>xyzhost.xyzcompany.com:9550</value>
    </preference>
    <preference>
    <name>ServerCheckTimeout</name>
    <value>3000</value> <!-- in milliseconds -->
    <read-only>true</read-only>
   </preference>
  </portlet-preferences>
```

- 3. Save and close the master portlet.xml file.
- 4. Open the run-time copy of the master portlet.xml file and make the same edits that you made to the master file.

5. Save and close the run-time portlet.xml file.

**Note:** If you only edit the master portlet.xml file, you will need to restart Tivoli Integrated Portal to automatically update the run-time copy of the master portlet.xml file.

#### Tivoli Integrated Portal cleanup procedure on Windows

If you uninstall Tivoli Integrated Portal and cannot reinstall Tivoli Integrated Portal, follow this procedure to clean up your system.

# Problem

You cannot reinstall Tivoli Integrated Portal.

# Action

To query the Deployment Engine registry on Windows, follow these steps:

- 1. Open a command prompt window (assuming you are logged in as the Administrator).
- Go to the following directory: cd C:\Program Files\IBM\Common\acsi\bin
- **3**. Run the following command:

..\setenv.cmd

4. Run the following command: listiu

If you cannot run the **listiu** command, then that is an indication that the Deployment Engine has been uninstalled.

To clean up your system, follow these steps on Windows:

1. Remove the deployment engine. Run the following commands:

```
"c:\Program Files\IBM\Common\acsi\setenv.cmd"
"c:\Program Files\IBM\Common\acsi\bin\si_inst.bat" -r -f
rmdir /s /q "C:\Program Files\IBM\Common\acsi"
```

**Note:** If a directory path includes spaces (for example, "Program Files"), the path must be in quotation marks.

**2.** Stop the Tivoli Integrated Portal if it is running. Run the following command to determine if the service is running:

```
>net start | find "TIPProfile"
Tivoli Integrated Portal - TIPProfile_Port_16310
```

If the service is found, stop the service with the following command: >net stop "Tivoli Integrated Portal - TIPProfile Port 16310"

**Note:** 16310 is the default port. If you selected a different port number for Tivoli Integrated Portal, change this port number to the number you selected.

**3**. Delete the Tivoli Integrated Portal service, if it is installed. Use the following command to determine if the service is installed:

```
>sc query | find "TIPProfile"
SERVICE_NAME: IBMWAS61Service - TIPProfile Port_16310
DISPLAY NAME: Tivoli Integrated Portal - TIPProfile Port 16310
```

If the service was found, delete the service with the following command.

>sc delete "IBMWAS61Service - TIPProfile\_Port\_16310"

**Note:** 16310 is the default port. If you selected a different port number for Tivoli Integrated Portal, change this port number to the number you selected.

 Delete the Tivoli Integrated Portal installation directory: >rmdir /s /q "<TIP\_install\_directory>

The default for <TIP\_install\_directory> is c:\Program Files\IBM\tivoli\tip.

**Note:** If a directory path includes spaces (for example, "Program Files"), the path must be in quotation marks.

5. Remove the following files from c:\Documents and Settings\ <administrator\_user\_ID> (for Windows): IA-TIPInstall-\*\*.log

IA-TIPUninstall-\*\*.log

- 6. Reboot the system.
- 7. Rerun the installation program.

# Tivoli Integrated Portal cleanup procedure on UNIX or Linux

If you uninstall Tivoli Integrated Portal and cannot reinstall Tivoli Integrated Portal, follow this procedure to clean up your system.

#### Problem

You cannot reinstall Tivoli Integrated Portal.

#### Action

To check to see if you have Tivoli Integrated Portal files left on your system, follow these steps:

- 1. Open a command session (assuming you are logged into the machine as the root user).
- Go to the following directory: cd /usr/ibm/common/acsi/bin
- 3. Run the following command:
  - . /var/ibm/common/acsi/setenv.sh
- 4. Run the following command:

./listIU.sh

If you cannot run the listIU.sh script, then that is an indication that the Deployment Engine has been uninstalled.

To clean up your system, follow these steps on UNIX or Linux:

1. Create a script with these command:

```
#!/bin/sh
```

```
# Source the Deployment Engine environment
if [ -f /var/ibm/common/acsi/setenv.sh ]; then
   . /var/ibm/common/acsi/setenv.sh
fi
# Uninstall Deployment Engine
if [ -f /usr/ibm/common/acsi/bin/si_inst.sh ]; then
   /usr/ibm/common/acsi/bin/si_inst.sh -r -f
fi
```

```
# Kill Deployment Engine
kill -9 `ps -aef | grep acsi | grep -v grep | awk '{ print $2 }'` 2> /dev/null
# Kill the Tivoli Integrated Portal server
kill -9 `ps -aef | grep tip | grep -v grep | awk '{ print $2 }'` 2> /dev/null
# Remove the install directories
rm -rf /var/ibm/common/acsi /usr/ibm/common/acsi /opt/IBM/Tivoli/tip
# Remove the Deployment Engine logs
rm -rf ~/IA-TIPInstall*log
```

Save the file.

- Before running this script, run this command: chmod 755 <file\_name>.sh
- 3. Run the script program.
- 4. Rerun the installation program.

# Installation fails after host name change

After the host name has been changed on the system, the Tivoli Integrated Portal installation fails.

# Problem

Tivoli Integrated Portal installation fails after a host name change on the system.

#### Action

To work around this problem, follow these steps:

1. Modify the ACUApplication.properties file. Go to the following directory:

```
c:\program files\ibm\common\acsi\ACUApplication.properties
  (for Windows
/var/ibm/common/acsi/ACUApplication.properties
```

```
(for AIX and Linux)
```

- 2. Change the value of acu.hostname property in the ACUApplication.properties file to the new host name.
- 3. Save the file.
- 4. Reinstall Tivoli Integrated Portal.

# Error message: GUI8335E

When you try a launch in context with single sign-on operation from the Tivoli Storage Productivity Center GUI to a DS8000 Element Manager, you receive an error message about your token type not being supported.

# Problem

When you try a launch in context with single sign-on operation from the Tivoli Storage Productivity Center GUI to a DS8000 Element Manager, you receive this error message:

GUI8335E: Login failed. Attempted to log into the DS8000 Element Manager. The type of token submitted is not supported by the Storage Authentication Service.

This error occurs because Tivoli Integrated Portal does not re-synchronize its LTPA keystore with the Authentication Services Server keystore when you click the

**Generate Keys** button in the Tivoli Integrated Portal console to generate new LTPA keys for Tivoli Integrated Portal.

#### Action

To work around this problem, you must manually re-synchronize the Tivoli Integrated Portal LTPA keystore with the Authentication Services Server keystore. Follow these steps:

- Start a Web browser and direct it to this URL: http://<TPC\_server>:16310
- 2. Log into Tivoli Integrated Portal as a user with administrative privileges.
- 3. Click Security > Secure administration, applications, and infrastructure > Authentication mechanisms and expiration.
- 4. In the "Cross-cell single sign-on" section, enter this information:
  - a. Enter and confirm a TIP Key File Password of your choosing.
  - b. Enter a **TIP Key File name** of your choosing.
  - c. Click Export keys.
- 5. Log out of Tivoli Integrated Portal.
- 6. Open a command prompt window on your Tivoli Storage Productivity Center server system.
- 7. Change to the following directory:

```
AIX and Linux: cd <TIP_install_directory>/profiles/TIPProfile/bin
Windows: cd <TIP_install_directory>\profiles\TIPProfile\bin
```

**8**. Run the command to re-sychronize the Tivoli Integrated Portal LTPA keystore with the Authentication Services Server keystore:

AIX and Linux:

```
./wsadmin.sh -lang jacl -user <TIP_admin_ID>
-password <TIP_admin_password>
-f ./setAuthnSvcLTPAKeys.jacl
"<TIP_install_directory>/profiles/TIPProfile/<TIP_Key_File>"
<TIP_key_file_password>
```

Windows:

```
wsadmin -lang jacl -user <TIP_admin_ID>
-password <TIP_admin_password>
-f setAuthnSvcLTPAKeys.jacl
"<TIP_install_directory>/profiles/TIPProfile/<TIP_Key_File>"
<TIP_key_file_password>
```

**Note:** The path to the TIP Key File should contain forward slashes and the TIP Key File name should not have any spaces in it.

9. Stop and restart the Tivoli Integrated Portal server.

# Cannot log on to Tivoli Integrated Portal

You cannot log on to IBM Tivoli Integrated Portal after a role-to-group mapping change in IBM Tivoli Storage Productivity Center.

# Problem

When you create and save role-to-group mappings in Tivoli Storage Productivity Center, these mappings are propagated into Tivoli Integrated Portal, where the groups are given the operator authorization. Occasionally, you might find that after creating and saving the role-to-group mappings in Tivoli Storage Productivity Center, you are unable to access Tivoli Integrated Portal as a valid user (in a valid group that is mapped to the operator authorization in Tivoli Integrated Portal).

# Action

To work around this problem, follow one of these steps:

- Stop and restart the Tivoli Integrated Portal server.
- In the Tivoli Integrated Portal console, click **Users and Groups** → **Administrative User Roles**. Grant the user a particular role or authorization within Tivoli Integrated Portal.

# Cannot access reports in the Tivoli Common Reporting component

You cannot access reports in the Tivoli Common Reporting component due to default authentication configuration.

# Problem

Tivoli Common Reporting provides authorization checking that allows the administrator to control access to Tivoli Common Reporting reports on a per user basis. This authorization checking is only supported in LDAP or File Based Realm configurations. In an OS Registry configuration the authorization check fails, preventing user access to the reports. TCR provides a setting to disable this authorization check, allowing access to reports in OS Registry configurations.

# Action

To work around this problem:

- Check the value of the SECURITY\_ENABLED property in C:\Program Files\IBM\tivoli\tip\products\tcr\conf\reportingConfig.xml. If this property is set to **true**, change the value to **false**. This will disable the authentication checking and allow any user that is authenticated in Tivoli Integrated Portal and is in the tcrSuperAdmin or tcrOperator administrator role groups to have full permission to all reports. Users not in either role will not see **Reporting** in the navigation task list and will not have access to the reports.
- Stop and restart the Tivoli Integrated Portal server.

# Independent software vendors troubleshooting

Use this section to troubleshoot and resolve independent software vendor problems.

# HDS HiCommand shows a different set of volumes

This problem occurs with the Hitachi Data Systems.

# Problem

The HDS **HiCommand** shows a different set of volumes for an Hitachi Data System subsystem from what is reported by IBM Tivoli Storage Productivity Center. This is a known problem with either the **HiCommand** CIMOM or the **HiCommand** GUI.

# Action

Contact Hitachi Data Systems customer support to see if a fix is available.

# Reports for an Hitachi Data Systems subsystem do not show current information

The IBM Tivoli Storage Productivity Center reports do not show the current information for an Hitachi Data Systems (HDS) subsystem after the HDS Storage Navigator is used to create and assign LUNs.

# Problem

This problem occurs after you have used the HDS Storage Navigator to create and assign LUNs, add the HDS SMI-S agent, and then run a discovery and probe job.

#### Action

To get current information, follow these steps:

- 1. Go to the HDS HiCommand Device Manager that contains the SMI-S agent. Click **Resources > Subsystems** in the navigation tree.
- 2. Click on the HDS subsystem you want to refresh. You will see the **Refresh** button under Subsystem IP. Click **Refresh**.
- 3. Probe the HDS subsystem in Tivoli Storage Productivity Center.
- 4. You can now look at your reports for the HDS subsystem.

#### Error message: HWN021651E

You get this error message when you try to delete a Hitachi Data Systems volume: HWN021651E Job on CIMOM http://<IP\_address>:5988 failed.

#### Problem

This problem occurs if you try to delete a Hitachi Data Systems volume. The complete error message is:

HWN021651E Job on CIMOM http://<IP\_address>:5988 failed. Job Status: FAILED. Error code is 5308, error description: You cannot delete the LU. You can only delete the last logical unit created. The last LU created was "29".. Check TPC and CIMOM logs.

This message applies to Hitachi Data Systems models 9570V, AMS, and WMS arrays. This does not apply to models 9900V, USP, and NSC (TagmaStore).

#### Action

You cannot delete the current logical unit. You can only delete the last logical unit created.

# Engenio shows different storage pool status from topology viewer

The Engenio Storage Manager shows a different storage array status from the IBM Tivoli Storage Productivity Center topology viewer storage pool status. This error occurs on the DS4000 series disk systems.

#### Problem

The Storage Manager software (from Engenio) sometimes reports different storage pool status than what is shown by the topology viewer. This occurs because the Engenio software (including the CIMOM) does not always immediately update its storage pool status. For example, pulling out all the disk drives in a volume group would not alone affect the operational status of the array or the volume group. To see a change in the operational status, you would need to perform I/O on one of the drives recently pulled out.

# Action

Understand the differences between the Tivoli Storage Productivity Center topology viewer from the Engenio Storage Manager with DS4000 series disk systems.

# Tool to dump MSCS cluster configuration

This topic provides information on the dump tool for the MSCS cluster configuration.

# Problem

When looking at an MSCS cluster problem, the current state of the clustering environment is often needed. Microsoft provides a tool to dump the MSCS cluster configuration into a set of files.

# Action

For more information about the tool to dump the MSCS cluster configuration, go to this Web site: http://www.microsoft.com/downloads/ details.aspx?displaylang;=en&familyid=cebf3c7c-7ca5-408f-88b7-f9c79b7306c0 &displaylang=en

# McDATA switch domain number

This error occurs with McDATA switches.

# Problem

The McDATA switch domain number in the IBM Tivoli Storage Productivity Center GUI should be consistent with what the switch software is displaying, but is not.

# Action

If you are using a McDATA switch, the domain ID displayed by Tivoli Storage Productivity Center has a different value from the one displayed by McDATA's management application. Tivoli Storage Productivity Center displays the domain ID on the Properties dialog for a selected switch or on the Zone dialog for zone control. The reason for this difference for the domain ID is because Tivoli Storage Productivity Center API call to the McDATA switch has some additional encoded information in the high-order bits. For example, a McDATA switch with the domain ID of 1 (as displayed on McDATA's management application) is displayed as 97 (hexadecimal 61 where the 6 represents the high-order bit encoding information).

# Error message: BTASD1932E

This problem occurs when using a heterogeneous fabric with Brocade switches and no out-of-band Fabric agent.

# Problem

You receive the following error message:

BTASD1932E: Agent capable of configuring zoning could not be found on this Fabric.

# Action

To work around this problem, follow these steps:

- 1. Open the GUI.
- 2. Click Administrative Services > Data Sources > Out of Band Fabric Agents.
- 3. Click Add on the Out of Band Fabric Agents pane.
- 4. The Add Out of Band Fabric Agent pop-up is displayed. Under Brocade Advanced Properties (Optional), click **Enable Advanced Brocade Discovery**. Enter a Username and Password for the Brocade switch. Click **OK**. IBM Tivoli Storage Productivity Center will select an out-of-band Fabric agent and the error message will not be issued.

# Brocade switch, zoning update failed

This problem occurs when using a Brocade switch and performing a zoning update.

# Problem

When using the Fabric Manager to update and activate a zoneset from an IBM Tivoli Storage Productivity Center server on an AIX or Linux machine to a Brocade switch, the user interface might indicate that the zoning update failed because the operation to activate the zoneset failed. However, it is possible that the zoning updates (including activation of the zoneset) actually did take place on the switch and completed successfully, but the success of the operation was not communicated by the switch to the Tivoli Storage Productivity Center server. In this case, you can verify that the operation was successful by looking at the zone configuration on the switch or by performing a probe and viewing the zone information for that fabric again. This situation can occur in certain network configurations such as a server having dual IP addresses (a public and private IP address) and the switch having a private IP address. This error occurs between the Tivoli Storage Productivity Center servers on AIX or Linux machines and Brocade switches only.

# Action

Resolution of the problem might require network configuration changes such as using only public or private IP addresses. Please contact IBM support.

# Using a McDATA switch in direct mode

You cannot find a McDATA switch when you run an IBM Tivoli Storage Productivity CenterCIMOM discovery.

# Problem

If a McDATA SMIS agent (also known as a Brocade SMIS agent for EOS products) is set up in direct mode, and Tivoli Storage Productivity Center's CIMOM discovery did not find the switch through this SMIS agent, the cause might be because the switch is not available to the SMIS agent. Each McDATA switch can have an open handle to only one McDATA management application, such as EFCM Server or SMIS agent. The switch might already be managed by an EFCM Server or a different SMIS agent. If this is the case, you are not warned when adding a McDATA switch to the SMIS agent in direct mode and will not be aware

of the problem until you run Tivoli Storage Productivity Center's CIMOM discovery.

# Action

Find the McDATA application that is managing the switch. If the pre-existing McDATA application is an EFCM Server, run the SMIS agent in proxy mode to that application. If the pre-existing McDATA application is another SMIS agent, either use that existing SMIS agent or remove the switch from that SMIS agent's configuration.

Check your vendor's documentation for any current information in this area. See *Brocade SMI Agent for EOS products: User Guide*.

# Cannot collect performance data from EMC CLARiiON

You cannot collect performance data from the EMC CLARiiON.

# Problem

The EMC CIM agent incorrectly reports that it supports BSP even when the CIM agent has not been enabled to run the BSP service.

#### Action

To enable the CIM agent for performance data, follow these steps:

- 1. Run the **testsmiprovider** command to discover the Symmetrix devices.
  - a. Open a Command Prompt window. Go to the EMC directory: <EMC\_SMIS\_Provider\_base\_dir>\symcli\storbin

Example:

C:\Program Files\EMC\SYMCLI\storbin

- b. Run the **testsmiprovider** command in the Command Prompt window. Provide the information for the Host, Connection Type, Port, Username, and Password fields. Use the default values unless you have changed them.
- c. When you get to the Command Prompt window, run the **disco** command to discover the Symmetrix devices. The command runs and ens with an output of 0 (success). It does not show any discovered devices at this point.
- d. Press the Enter key and then q to exit.
- 2. Use the **symcfg list** command to list the Symmetrix devices that have been discovered. This command displays each Symmetrix device that the **testsmiprovider** command discovered.
- **3**. Register the EMC SMI-S provider in IBM Tivoli Storage Productivity Center as a CIM agent. Use the following values:

Host name or IP address of the EMC SMI-S provider host.

#### Port and Protocol

- 5988 (unsecure http)
- 5989 (secure https)

#### Userid/password

The EMC SMI-S provider user ID and password that was defined when you configured the SMI-S provider. If user authentication is not enabled on the CIM agent, enter any values you want.

# Description of the CIM Agent

A value that is used to identify the managed device or devices.

- 4. Run an Tivoli Storage Productivity Center CIMOM discovery.
- 5. To enable performance monitoring, run the symcfg command. For example: symcfg authorization add -host <HostName> -username <UserName> -password <password>
- 6. Run the command in step 5 for each of the EMC controllers.

# Disks under EMC PowerPath control not displayed on AIX 5.3

Disks under EMC PowerPath control are not displayed in topology view or asset reports on AIX 5.3.

# Problem

In the IBM Tivoli Storage Productivity Center GUI, navigate to **Data Manager** > **Reporting** > **Asset** > **By Computer** > (*computer name*) > **Disks**. Any disks that are under EMC PowerPath control are not displayed in asset reports. The disks also are not displayed in topology view.

# Action

No action is required. On AIX 5.3, IBM Tivoli Storage Productivity Center is unable to collect information for disks under EMC PowerPath control. Therefore, information for those disks cannot be displayed in topology view or asset reports.

# Software level not displayed for CIM agent

The software level for the CIM agent is not displayed for a non-IBM storage subsystem or switch.

# Problem

In the IBM Tivoli Storage Productivity Center GUI or a storage subsystem, navigate to Administrative services > Data sources > CIMOM Agents. Open the details panel for the CIM agent. The software level for the CIM agent is not displayed. This occurs for storage subsystems or switches that are not products of IBM.

# Action

No action is required. For non-IBM storage subsystems or switches, the software level for the CIM agent is not displayed.

# Error message: HWNPM2132W

You receive this message when you are try to collect performance data from a Data ONTAP file system.

# Problem

The Data ONTAP SMI-S 3.0 agent has the following limitation: If a volume is offline, the performance monitor might fail with the message: PM HWNPM2132W Performance data could not be collected for device <device>.

# Action

Check your vendor's documentation for any current information in this area.

# Miscellaneous troubleshooting

Use this section to troubleshoot and resolve miscellaneous problems.

# Traditional Chinese characters not displayed correctly in GUI help panels

This problem occurs when you are displaying Traditional Chinese characters in the IBM Tivoli Storage Productivity Center GUI help panels.

#### Problem

The Traditional Chinese characters are not displayed correctly in the Tivoli Storage Productivity Center GUI help panels.

# Action

To work around this problem, follow these steps:

- Download the file mtsans\_t.zip from the following Web site:ftp:// submit.boulder.ibm.com/download/typography/fonts/worldtype/archive/ wts\_/2002-02-26/.
- 2. Unzip the file mtsans\_t.zip to access the unicode font file mtsans\_t.ttf (Monotype Sans WT TC).
- 3. Install the font file mtsans\_t.ttf on the Traditional Chinese Windows system.
- 4. Modify the file:

<TPC\_install\_dir>\jre\lib\fontproperties.zh\_TW

Add the line: filename.Monotype Sans WT TC=MTSANS T.TTF

Modify the fontproperties.zh\_TW file with the following lines in bold highlight:

```
======= fontproperties.zh_TW ========
serif.0=Times New Roman
serif.1=Monotype Sans WT TC,CHINESEBIG5 CHARSET
serif.2=Lucida Sans Regular
serif.3=Times New Roman WT TC
serif.4=EUDC
serif.italic.0=Times New Roman Italic
serif.italic.1=Monotype Sans WT TC,CHINESEBIG5_CHARSET
serif.italic.2=Lucida Sans Oblique
serif.italic.3=Times New Roman WT TC
serif.italic.4=EUDC
serif.bold.0=Times New Roman Bold
serif.bold.1=Monotype Sans WT TC,CHINESEBIG5 CHARSET
serif.bold.2=Lucida Sans Regular
serif.bold.3=Times New Roman WT TC
serif.bold.4=EUDC
serif.bolditalic.0=Times New Roman Bold Italic
serif.bolditalic.1=Monotype Sans WT TC,CHINESEBIG5 CHARSET
serif.bolditalic.2=Lucida Sans Oblique
serif.bolditalic.3=Times New Roman WT TC
serif.bolditalic.4=EUDC
```

sansserif.0=Arial
sansserif.1=Monotype Sans WT TC,CHINESEBIG5\_CHARSET
sansserif.2=Lucida Sans Regular
sansserif.3=Arial Unicode MS

sansserif.4=EUDC

```
sansserif.italic.0=Arial Italic
sansserif.italic.1=Monotype Sans WT TC,CHINESEBIG5_CHARSET
sansserif.italic.2=Lucida Sans Oblique
sansserif.italic.3=Arial Unicode MS
sansserif.italic.4=EUDC
```

sansserif.bold.0=Arial Bold
sansserif.bold.1=Monotype Sans WT TC,CHINESEBIG5\_CHARSET
sansserif.bold.2=Lucida Sans Regular
sansserif.bold.3=Arial Unicode MS
sansserif.bold.4=EUDC

sansserif.bolditalic.0=Arial Bold Italic
sansserif.bolditalic.1=Monotype Sans WT TC,CHINESEBIG5\_CHARSET
sansserif.bolditalic.2=Lucida Sans Oblique
sansserif.bolditalic.3=Arial Unicode MS
sansserif.bolditalic.4=EUDC

monospaced.0=Courier New
monospaced.1=Monotype Sans WT TC,CHINESEBIG5\_CHARSET
monospaced.2=Lucida Sans Typewriter Regular
monospaced.3=Lucida Sans Regular
monospaced.4=Monotype Sans Duospace WT TC
monospaced.5=EUDC

monospaced.italic.0=Courier New Italic
monospaced.italic.1=Monotype Sans WT TC,CHINESEBIG5\_CHARSET
monospaced.italic.2=Lucida Sans Typewriter Oblique
monospaced.italic.3=Lucida Sans Oblique
monospaced.italic.4=Monotype Sans Duospace WT TC
monospaced.italic.5=EUDC

monospaced.bold.0=Courier New Bold
monospaced.bold.1=Monotype Sans WT TC,CHINESEBIG5\_CHARSET
monospaced.bold.2=Lucida Sans Typewriter Regular
monospaced.bold.3=Lucida Sans Regular
monospaced.bold.4=Monotype Sans Duospace WT TC
monospaced.bold.5=EUDC

monospaced.bolditalic.0=Courier New Bold Italic
monospaced.bolditalic.1=Monotype Sans WT TC,CHINESEBIG5\_CHARSET
monospaced.bolditalic.2=Lucida Sans Typewriter Oblique
monospaced.bolditalic.3=Lucida Sans Oblique
monospaced.bolditalic.4=Monotype Sans Duospace WT TC
monospaced.bolditalic.5=EUDC

```
#
# Define dialog and dialoginput to match the above definitions
#
alias.dialog=sansserif
alias.dialoginput=monospaced
#
# Exclusion Ranges
#
# exclusion.dialog.0=0500-20ab,20ad-ffff
#exclusion.dialoginput.1=0500-20ab,20ad-ffff
#exclusion.serif.0=0500-20ab,20ad-ffff
#exclusion.sansserif.0=0500-20ab,20ad-ffff
#exclusion.monospaced.1=0500-20ab,20ad-ffff
#
# To enable helvetica, courier and timesroman as real fonts
# remove aliases, and define them as real terminal fonts.
```

# (i.e. timesroman.0=TimesRoman) # timesroman.0=TimesRoman alias.timesroman=serif # helvetica.0=Helvetica alias.helvetica=sansserif # courier.0=Courier alias.courier=monospaced # font filenames filename.Arial=arial.ttf filename.Arial Bold=arialbd.ttf filename.Arial\_Bold\_Italic=arialbi.ttf filename.Arial Italic=ariali.ttf filename.Arial Unicode MS=arialuni.ttf filename.Courier\_New=cour.ttf filename.Courier\_New\_Bold=courbd.ttf filename.Courier\_New\_Bold\_Italic=courbi.ttf filename.Courier\_New\_Italic=couri.ttf filename.EUDC=eudc.tte filename.Lucida Sans Oblique=LucidaSansOblique.ttf filename.Lucida Sans Regular=LucidaSansRegular.ttf filename.Lucida Sans Typewriter Oblique=LucidaTypewriterOblique.ttf filename.Lucida Sans Typewriter Regular=LucidaTypewriterRegular.ttf filename.Monotype\_Sans\_Duospace\_WT\_T=mtsansdt.ttf filename.Times\_New\_Roman=times.ttf filename.Times New Roman Bold=timesbd.ttf filename.Times New Roman Bold Italic=timesbi.ttf filename.Times\_New\_Roman\_Italic=timesi.ttf filename.Times New Roman WT TC=tnrwt t.ttf filename.Monotype\_Sans\_WT\_TC=mtsans\_t.ttf filename.\u65b0\u7d30\u660e\u9ad4=mingliu.ttc filename.MingLiU=mingliu.ttc filename.PMingLiU=mingliu.ttc # default char definition default.char=02ff # charset for text input inputtextcharset=CHINESEBIG5 CHARSET # font substitution substitute.0=\u7d30\u660e\u9ad4=MingLiU substitute.1=\ub5b0\u7d30\u660e\u9ad4=PMingLiu substitute.2=Arial Unicode MS=Times New Roman WT TC substitute.3=Arial Unicode MS=Monotype Sans Duospace WT TC substitute.4=Monotype Sans Duospace WT=Arial Unicode MS substitute.5=Monotype Sans Duospace WT=Times New Roman WT TC substitute.6=Times New Roman WT=Arial Unicode MS substitute.7=Times New Roman WT=Monotype Sans Duospace WT TC substitute.8=Times New Roman=Times New Roman substitute.9=Courier New=Courier New substitute.10=Arial=Arial substitute.11=Times New Roman=Times New Roman substitute.12=Courier New=Courier New substitute.13=Arial=Arial register.0=MingLiU register.1=PMingLiU ====== end of fontproperties.zh TW ========

**5**. Save the file and redisplay the help panels in Tivoli Storage Productivity Center GUI.

# Cannot read Korean language logs from GUI

This problem occurs in Korean language environments.

# Problem

You will not be able to view the log files from the IBM Tivoli Storage Productivity Center GUI because of a DB2 JDBC driver problem.

# Action

You will have to read the files using another text viewer like Notepad.

# **Chapter 8. Reference information**

This reference information describes configuration files, log files, silent installation files, and other files.

# Agent Manager toolkit for administrators

In addition to the commands in <Agent\_Manager\_install\_dir>, the Agent Manager provides a toolkit of "as-is" administration tools. The toolkit commands are in the following directory: <Agent\_Manager\_install\_dir>/toolkit/bin. Use caution when using these tools because they have not been translated and the output of the commands are not translated. They are also subject to change in the future.

The commands provided are:

#### HealthCheck

**HealthCheck** is a command to verify the state of the basic functions of the Agent Manager. This command indicates if the Agent Manager is or is not operational. This command must be run from the machine on which the Agent Manager is installed. This command requires certain parameters depending on if you used the installation defaults and if you are using generated or demonstration certificates. The files are:

#### HealthCheck.sh

The script that runs the **HealthCheck** command on UNIX and Linux systems.

#### HealthCheck.bat

The script that runs the **HealthCheck** command on Windows systems.

#### HealthCheck.jar

The JAR file that contains the Java code for the command.

An example of using the **HealthCheck** command is to verify that the Common agent password you are using is still valid:

For Windows:

HealthCheck -registrationPw changeMe

```
For UNIX:
```

./HealthCheck.sh -registrationPw changeMe

Where changeMe is the password you are checking for.

# LogCollector

**LogCollector** gathers logs and other information needed to debug problems with the Agent Manager. **LogCollector** creates the **LogCollector.zip** file, which is located in the root directory of where the Agent Manager is installed. This command must be run from the machine on which the Agent Manager is installed. Review the **LogCollector** README file for instructions on running the commands and the parameters required for this command. The **LogCollector** README file also lists known issues and limitations. The files are:

#### LogCollector.sh

The script that runs the **LogCollector** command on UNIX and Linux systems.

#### LogCollector.bat

The script that runs the **LogCollector** command on Windows systems.

#### LogCollector.jar

The JAR file that contains the Java code for the command.

# Estimating tablespace allocation

This topic describes how you can use the IBM Tivoli Storage Productivity Center to estimate the tablespace size in the repository database.

When you install Tivoli Storage Productivity Center, you can specify the tablespace size in the repository database. The space needed for the Tivoli Storage Productivity Center database schema varies significantly with storage network configuration, data collection, data retention period, and other factors. Unless you are an experienced administrator, you should use the default values for tablespace allocation that Tivoli Storage Productivity Center provides.

Table 51 provides space estimations for a storage configuration containing 5000 volumes with some general assumptions.

Table 51.	Tablespace	allocation	for the	Tivoli	Storage	Productivitv	Center	database	schema

Tablespace	Description of tablespace usage	Recommended size for a 5000 volume configuration	Assumptions
KEY	This tablespace is used for configuration data which is constantly used. For example, the key entity and relationships data (T_RES_STORAGE_ SUBSYSTEM, T_RES_STORAGE_VOLUME, and the normalization tables, and so forth)	500 MB	A table that uses significant space is T_RES_DATA_PATH. This table uses about 300 bytes for each record for the relationship between the storage volumes and host ports. There could be dozens to hundreds of data paths for a volume.
NORMAL	This tablespace is used for snapshots and miscellaneous data	500 MB	A table that uses significant space is T_RES_STORAGE_VOLUME_ SNAPSHOT. This table uses about 2500 bytes for each record. The number of snapshots depends on the data collection activities.
BIG	This tablespace is used for performance statistics	2 to 3 GB or 400 MB per day of performance data	The data collected for performance data for storage volumes can use a significant amount of space (about 200 bytes for each record). For 5000 volumes, if performance data is collected every 5 minutes, the data for one day would be 300 MB. If the data is kept for 7 days, the data collected would take about 2 to 3 GBs. If the data is kept longer, the storage must be scaled up accordingly.
TEMP	This tablespace is used for temporary data for query processing and other temporary tables	1 GB	

# DB2 user names and passwords

This topic lists rules for DB2 user names and passwords.

DB2 user names and passwords must follow these rules. Names cannot be any of the following:

- UNIX user names and passwords cannot be more than eight characters long. They cannot start with a numeric digit or end with \$.
- Windows 32-bit user names and passwords can contain 1 to 20 characters.
- Group and instance names can contain 1 to 8 characters.
- Names cannot be any of the following:
  - USERS
  - ADMINS
  - GUESTS
  - PUBLIC
  - LOCAL
- Names cannot begin with:
  - IBM
  - SQL
  - SYS
- Names cannot include accented characters.
- UNIX users, groups, and instance names must be lowercase.
- Windows 32-bit users, groups, or instance names can be any case.

# Valid characters for user IDs and passwords

This section provides information about valid user IDs and passwords for IBM Tivoli Storage Productivity Center.

If you are performing a typical installation, the valid characters for the common user ID and password are as follows. This includes the user IDs and passwords for the DB2 administrator, DB2 user, WebSphere administrator, host authentication password, Common agent Windows service, and NAS filer.

- A through Z (uppercase characters)
- a through z (lowercase characters)
- 0 through 9 (numeric characters)
- Special characters: \_ .

**Important:** For Tivoli Storage Productivity Center, do not use a password that begins with a dash character.

The valid characters for the Common agent registration password or resource manager registration user ID and password as follows:

- A through Z (uppercase characters)
- a through z (lowercase characters)
- 0 through 9 (numeric characters)
- Special characters: ` ~ @ # % ^ & \* ( ) \_ = + [ ] { } \ \ ; : ' " , . < > / ?

For custom installation, the valid characters are shown in the following table.

User ID and password for	Valid characters
DB2 administrator, DB2 user	<ul> <li>A through Z (uppercase characters)</li> <li>a through z (lowercase characters)</li> <li>0 through 9 (numeric characters)</li> <li>Special characters: ~ @ # % ^ &amp; ( ) { }.</li> </ul>
WebSphere administrator or host authentication password	<ul> <li>A through Z (uppercase characters)</li> <li>a through z (lowercase characters)</li> <li>0 through 9 (numeric characters)</li> <li>Special characters:</li> </ul>
Common agent Windows Service user ID or NAS Filer user ID	<ul> <li>A through Z (uppercase characters)</li> <li>a through z (lowercase characters)</li> <li>0 through 9 (numeric characters)</li> <li>Special characters: `~ # % ^ &amp; ( ) { } '.</li> </ul>
Common agent Windows Service password or NAS Filer password	<ul> <li>A through Z (uppercase characters)</li> <li>a through z (lowercase characters)</li> <li>0 through 9 (numeric characters)</li> <li>Special characters: `~ @ # % ^ &amp; * () = + [] { } \   ;: ' " , . &lt; &gt; / ?</li> </ul>
Common agent registration password or resource manager registration user ID and password	<ul> <li>A through Z (uppercase characters)</li> <li>a through z (lowercase characters)</li> <li>0 through 9 (numeric characters)</li> <li>Special characters: `~ @ # % ^ &amp; * ( ) = + [ ] { } \   ;: ' " , . &lt;&gt; / ?</li> </ul>

Table 52. Valid characters for user IDs and passwords

# Interop namespaces for CIM agents for switches and storage subsystems

This section describes the namespaces for switches and storage subsystem CIM agents that are used in IBM Tivoli Storage Productivity Center.

If you specify an incorrect namespace the following issues might occur:

- The connection test fails when the CIMOM is added.
- The discovery does not discover all information of the system that is managed by the CIMOM.
- The probe fails.
- The function that you want to perform on the system might fail (for example, collecting performance data).

See the following table contains the interop namespaces.

Table 53. Interop Namespaces for CIM Agents for switches and storage subsystems

Switch or subsystem	Namespace
IBM	/root/ibm
Brocade	/interop

Switch or subsystem	Namespace
Cisco	/root/cimv2
	For version 3.2.1 or later: /root/pg_interop
Engenio	/interop
EMC	/root/emc
HDS	For HiCommand 5.6 or later, use: /root/smis/current For a HiCommand version that supports SMI-S 1.2, use following namespace to traverse the model as SMI-S 1.1:
	/root/smis/smis11 For HiCommand versions earlier than HiCommand 5.6, use: /root/hitachi/dmxx, where xx is represents the level of HiCommand.
HP	/root
McData	/interop
SUN	/root/sun3510 or /interop
	Note: This namespace is for a subsystem and not a switch.
XYRATEX	/root/PG_interop

Table 53. Interop Namespaces for CIM Agents for switches and storage subsystems (continued)

# agent.config file

The **agent.config** file contains configuration parameters for the Data agent. These parameters are set when the Data agent is installed; they can also be changed manually by modifying the file.

The following table contains the parameters for the **agent.config** file. If the Data agent is installed in the default location, this file is located at either /opt/IBM/TPC/ca/subagents/TPC/Data/config or C:\Program Files\IBM\TPC\ca\subagents\TPC\Data\config.

Table 54. Para	ameters for	the age	ent.config	file
----------------	-------------	---------	------------	------

Parameter	Description
agentPort	Port on which the Data agent listens for requests. By default, this is set to 9510.
serverHost	Fully qualified host name of the system on which the Data server is installed.
serverPort	Port on which the Data server listens for requests. By default, this is set to 9549.
logFilesKept	Maximum number of Data agent logs that are retained. When this number is reached, the oldest log file is overwritten. By default, this is set to five.
messagesPerLog	Maximum number of messages in a Data agent log file. When this number is reached, the a new log file is created. By default, this is set to 100,000.
maxBacklog	Maximum number of uncompleted jobs that are permitted. When this number is reached, if additional job requests are made, any error is generated. By default, this is set to 500.

Parameter	Description
sendFailWait	Number of seconds to wait before the Data agent attempts to resend a message to the Data server. By default, this is set to 30.
maxIdleThreads	Maximum number of idle threads to retain for use by future jobs. By default, this is set to 10.
uptimePoll	How often (in seconds) should agent check to ensure it is up (20).
hostAlias	This parameter appears if the HOST_ALIAS is not specific and represents the name of the server. This value for this parameter is used when multiple computers have the same name or the name cannot be determined.
honorSentScripts	If this parameter is set to '1', 't', 'T', 'y', or 'Y', the Data agent can run scripts sent from the Data server. Otherwise, only scripts that are exist in the <b>scripts</b> directory on the system where the Data agent is installed can be run.
TPCInstallLocation	Directory where the Data agent is installed.

Table 54. Parameters for the agent.config file (continued)

# server.config file

This topic lists the parameters that are set in the server.config file. These parameters include Controller, Logging, Repository, and Service.

Table 55. Falameters for server coming me	Table 55.	Parameters	for	server.	config	file
-------------------------------------------	-----------	------------	-----	---------	--------	------

Parameter	Description
Controller parameters:	
name	Data Manager Server Name (host computer name)
port	Port on which the server listens for requests (9549)
maxConnections	Maximum number of concurrent sockets that the server will open (500)
routerThreads	Number of threads redirect incoming requests to the appropriate service provider (1)
serviceThreads	Number of threads to allocate for the Server internal service provider (2)
agentErrorLimit	Number of consecutive attempts to reach an agent before the agent is displayed as DOWN. When an agent is in this state, no attempts to connect are made until either the agent contacts the Server or the agent status is manually changed to UP (3)
adminGroup	Name of the group a user must be a member of in order to perform administrative functions from the Graphic User Interface (adm)
commEncrypted	Switch that secures communication between the Server/Agent and the Server/GUI by encrypting the data stream.
	• $\theta$ = Off. Do not encrypt the data stream.
	• 1 = On. Encrypt the data steam.

Parameter	Description
hostAlias	This parameter appears if the HOST_ALIAS is not specific and represents the name of the server. This value for this parameter is used when multiple computers have the same name or the name cannot be determined.
Logging parameters:	
logsKept	Number of server logs to keep (5)
messagesPerLog	Maximum number of messages in a log, when this number is reached the log is closed and a new log is created. (100,000)
Repository parameters:	
driver	<ul> <li>Name of the JDBC driver to use, normally:</li> <li>Oracle: oracle.jdbc.driver.OracleDriver</li> <li>MS SQL: com.inet.tds.TdsDriver</li> <li>Sybase: com.sybase.jdbc2.jdbc.SybDriver</li> <li>UDB/DB2: COM.ibm.db2.jdbc.app.DB2Driver</li> <li>Cloudscape: com.ibm.db2j.jdbc.DB2jDriver</li> </ul>
url	<pre>The URL used to connect to the database, normally:    Oracle: jdbc:oracle:thin:@<host_name>:<port>:<sid>    MS SQL: jdbc:inetdae:<host_name>    Sybase: jdbc:sybase:Tds:host_name:port    UDB: jdbc:db2:database_name</host_name></sid></port></host_name></pre>
user	User name that IBM Tivoli Storage Productivity Center uses to connect to the repository
connectionPool	Number of database connections in a pool of reusable open connections (10)
Service parameters	
name	Repeating section that indicates the service providers to start. REQUIRED: • TStorm.server.svp.GuiSvp • TStorm.server.svp.AgentSvp • scheduler.Scheduler

Table 55. Parameters for server.config file (continued)

# scheduler.config file

This topic lists the parameters that are set in the scheduler.config file. These parameters include Concurrency parameters and Jobs parameters.

Table 56. Parameters for scheduler.config file

Parameter	Description	
Concurrency para	meters:	

Description	
Number of threads to create that handle the submission of jobs (3)	
Maximum Number of threads to create to handle job completions. Initially will create a pool of 1/2 the number that can grow to the maximum (3)	
Number of minutes in advance of scheduled time to begin the scheduling process. This allows for the overhead time involved in scheduling a job so that the job will actually start close to the scheduled time (1)	

Table 56. Parameters for scheduler.config file (continued)

# **TPCD.config file**

This topic lists parameters that are set in the TPCD.config file. These include Server parameters and GUI parameters.

Parameter	Description	
Server parameters:		
threadPoolSize	Number of initial threads to create for handling requests (3)	
abbreviatedProbe	Only Small Computer Systems Interface (SCSI) commands are sent to disk drives for inquiry and disk capacity information (1).	
maxThreads	Maximum number of threads allowed for handling requests (8)	
pingReceiveTimeout	Number of seconds to wait before indicating that a ping has failed (10)	
skipAutoFS=1	Set to 1 for discovery on the Solaris Data agent to skip the automounts process. By default, discovery always processes automounts on the Solaris Data agent.	
GUI parameters:		
threadPoolSize	Number of initial threads to create for handling user interface requests (3)	
maxThreads	Maximum number of threads allowed for handling user interface requests (10)	
reportRowLimit	Maximum number of rows that will be sent at a time to the user interface. If this number is exceeded, a <b>More</b> button will be displayed above the table, along with a warning message (5000)	
keepCachedReport	Number of minutes to retain incomplete reports in the server's <i>tmp</i> directory (120)	

# Information gathered by the agents

This section provides information about what data is collected by the agents.

Event which triggers discovery	In-band fabric agent	Out-of-band fabric agents	CIMOM fabric agents (Brocade or McData)	CIMOM fabric agents (QLogic or Cisco)
Administrative Services- >Discovery->Out- of-band fabric		<ol> <li>Finds switches within an IP address range</li> <li>Gets fabric, switch, and topology information</li> <li>Gets Cisco VSANs</li> <li>Gets Brocade zoning data<sup>1</sup></li> </ol>		
Administrative Services- >Discovery- >CIMOM			<ol> <li>Discovers CIMOMs through SLP</li> <li>Gets switches</li> <li>Gets fabrics</li> </ol>	<ol> <li>Discovers CIMOMs through SLP</li> <li>Gets switches</li> <li>Gets fabrics</li> </ol>
IBM Tivoli Storage Productivity Center ->Probe (including fabric)	<ol> <li>Gets zoning information, excluding zone aliases<sup>3</sup></li> <li>Gets fabric, switch, and topology information</li> <li>Hosts, endpoint devices, device- centric, and host-centric information collected</li> </ol>	<ol> <li>Gets fabric, switch, and topology information</li> <li>Gets Cisco VSANs</li> <li>Gets Brocade zoning data<sup>1</sup></li> </ol>	<ol> <li>Gets zoning data, including zone aliases for Brocade</li> <li>Gets fabric, switch, and switch port information, including blades<sup>2</sup></li> <li>Gets fabric topology connectivity data</li> <li>Subscribes to CIM indications</li> </ol>	1. Gets fabric, switch, and switch port information

Table 57. Information gathered by IBM Tivoli Storage Productivity Center for Fabric

Event which triggers discovery	In-band fabric agent	Out-of-band fabric agents	CIMOM fabric agents (Brocade or McData)	CIMOM fabric agents (QLogic or Cisco)
In-band fabric agent starts, or in-band agent connectivity changes, or in-band fabric change event detected	<ol> <li>Gets zoning information, excluding zone aliases<sup>3</sup></li> <li>Gets fabric, switch, and topology information</li> <li>Hosts, endpoint devices, device- centric and host-centric information collected</li> </ol>	<ol> <li>Gets fabric, switch, and topology information</li> <li>Gets Cisco VSANs</li> <li>Gets Brocade zoning data<sup>1</sup></li> </ol>		
SNMP trap received from switch	<ol> <li>Gets zoning information, excluding zone aliases<sup>3</sup></li> <li>Gets fabric, switch, and topology information</li> <li>Hosts, endpoint devices, device- centric and host-centric information collected</li> </ol>	<ol> <li>Gets switch and topology information</li> <li>Gets Cisco VSANs</li> <li>Gets Brocade zoning data<sup>1</sup></li> </ol>		

Table 57. Information gathered by IBM Tivoli Storage Productivity Center for Fabric (continued)

Event which triggers discovery	In-band fabric agent	Out-of-band fabric agents	CIMOM fabric agents (Brocade or McData)	CIMOM fabric agents (QLogic or Cisco)
CIM indication received from fabric CIMOM			<ul> <li>Performs</li> <li>"mini-probe" to collect</li> <li>information</li> <li>relevant to the indication</li> <li>received, or sets</li> <li>entities as</li> <li>missing. Can do one of the following:</li> <li>Get switches and fabrics</li> <li>Gets zoning data</li> <li>Gets switch port status and connection to node</li> <li>Gets switch blade status and all associated port connections</li> <li>Sets fabric, switch, blades, connections, and/or nodes</li> </ul>	
			<ul> <li>Sets fabric, switch, blades, connections, and/or nodes as missing</li> </ul>	

Table 57. Information gathered by IBM Tivoli Storage Productivity Center for Fabric (continued)

- 1. Brocade zoning data is only retrieved from out-of-band fabric agents if no CIMOM is configured for this fabric. If an out-of-band fabric agent is used, Zone Aliases changes cannot be made through Tivoli Storage Productivity Center
- 2. Physical switch and blades information is not collected for McDATA i10000 switches (and same switch models from OEM partners). Virtual switches are collected.
- **3**. Zoning data is only retrieved from in-band fabric agents for non-Brocade switches. For McDATA, if a CIMOM is configured for this fabric, zoning data is collected from the CIMOM.

# **Zone configuration**

When you configure zones, you can use Fabric Manager or the management application for the devices. The advantages to using Fabric Manager rather than the management applications of the devices are that Fabric Manager lets you perform zoning from a single interface, and you can use consistent, familiar methods to work with devices from multiple vendors.

Consider the following guidelines if you use Fabric Manager with zones:

- For Brocade and McDATA fabrics, topology information is collected through CIM agents. If no CIM agents are configured, or if the fabric is a QLogic or Cisco fabric, have at least one managed host per zone for the complete topology display. In this way, you can manage your switches and a string is returned, provided by the vendor, that can be the worldwide name (WWN) or a vendor, model, and level type designation.
- If CIM agents cannot be used to collect zoning, the Fabric Manager can retrieve the zone information from IBM 2005 and 2109 switches and from Brocade Silkworm Fibre Channel Switches. SNMP agents must log into the switch with administrative rights. To see zone information, specify the login ID for the agents you define.

For zone discovery and zone control for any fabrics with Brocade switches or vendor Brocade switches, you must have a SMI-S agent configured for the fabric. If a SMI-S agent is not configured, you must enable advanced Brocade discovery. To do this, enter the administrator user ID and password for at least one switch in a fabric. However, you should not enable advanced discovery for all Brocade switches that have been configured as SNMP agents. The enabled switch acts as a proxy and gathers zone information for the entire fabric. You can enable a second switch for redundancy. Enabling all Brocade switches puts an unnecessary load on the switches and fabric. You should enable newer, more powerful switches (such as director class) and those running the highest level of firmware.

- A zone set can be deleted while it contains zones. With QLogic switches, those zones are put into an orphan zone set. The zones can later be moved from an orphan set into other zone sets. The Fabric Manager zone configuration panels cannot display zones in an orphan zone set. However, the zones exist on the switch, and they can be configured using the switch vendor's tool.
- For McData switches, you can add empty zones to inactive zone sets. You cannot add empty zones to inactive zone sets for other vendors' switches.

**Note:** Activating an inactive zone set that contains empty zones will fail if a switch does not support empty zones in active zone definitions.

**Note:** In-band discovery does not detect orphan zones (that is, zones that do not belong to any zone set). These zones are not listed in the Zone Configuration window. However, the zones exist on the switch, and they can be configured using the switch vendor's tool. However, Brocade orphan zones, which are discovered through SMI-S agents and out-of-band discovery, are listed in the Zone Configuration window and can be configured by the Fabric Manager. Brocade orphan zone aliases, which are discovered through SMI-S agents, are listed in the Zone Configuration window and can be configured by the Fabric Manager. Similarly, for McDATA fabrics managed where a CIM agent is configured, orphan zones are listed in the Zone Configuration window and can be configuration window and can be configured by the Fabric Manager.

# SQL access to IBM Tivoli Storage Productivity Center's views

IBM Tivoli Storage Productivity Center stores the information collected by data collection jobs in its DB2 database repository. This information is organized into a set of accessible views. You can use Structured Query Language (SQL) to retrieve the information from these views to create custom reports or for use within other applications.

**Prerequisite:** See "Planning for SQL access to IBM Tivoli Storage Productivity Center's views" on page 114 for information about the requirements when retrieving data from views in the database repository.

A view is a logical table that consists of data that is generated by a query. A view is based on an underlying set of base tables in the database repository, and the data in a view is determined by a SELECT statement that is run on those base tables. The data collected Tivoli Storage Productivity Center is organized into the following sets of views that you can access in the database repository:

#### Storage entity views

These views include detailed information about the properties of storage entities. For example, the name, disk space, and available disk space for a storage subsystem. Information about the following storage entities are available in views in the database repository:

- Storage entity views: Hosts, volume groups, disks, virtual disks, external storage volumes, disk paths, virtual disk paths, controllers, logical volumes, file systems, clusters, cluster resource groups, hypervisors, virtual machines, virtual machine disks, hypervisor volumes, host virtual files, hypervisor partitions, MAC addresses, files, file types, directories, exports, OS users, OS user groups, IP addresses, Windows domains, and Storage Resource agents.
- Host relationship views:
  - Logical volume to host disk
  - Logical volume to logical volume (Parent and child logical volume relationships)
  - Computer to storage entity (disk or logical volume)
  - Filesystem to logical volume

(for example, the relationship between a logical volume and a host disk)

- Database views: Database instances, database containers, database archive logs, database control files, database datafiles, database devices, database log files, database log groups, database segments, database tables, database tablespaces
- Storage subsystem views: Storage subsystems, storage virtualizers, storage pools, extents, volumes, disk drives, disk groups, element managers, nodes, backend disks, storage virtualizer I/O groups, volume paths, array sites, ranks
- Storage subsystem relationship views:
  - Disk drive to storage extent
  - Storage volume to storage extent
  - Volume to disk drive
  - Storage volume to backend disk
- NAS Filers
- Tape library views: Tape libraries, tape cartridges, tape drives, tape frames, tape I/O ports, tape media changers, tape media locations
- Fabric views: Fabrics, nodes, peripheral entities, port to port connections, switches, switch blades, zones, zone members, zone sets, zone aliases, FC ports, host bus adapters
- Fabric relationship views:
  - Blade to FC port
  - Node to HBA, Node to port

- Peripheral entity to node
- Switch to port
- Zone to alias, Zone to zone member, Zone to node, Zone to member
- Zone set to zone
- Zone alias to node
- Alias to member
- Fabric to switch, Fabric to zoneset, Fabric to zone, Fabric to zone alias
- Performance management views (for example, metrics and threshold violations)

#### Entities defined by Tivoli Storage Productivity Center

These views include information about entities that are defined by Tivoli Storage Productivity Center. These entities include Data agents, Fabric agents, the alert log, the Tivoli Storage Productivity Center servers, scan profiles, external tools, monitoring groups, reporting groups, and storage resource groups.

#### Data sources

These views include information about the data sources that are associated with Tivoli Storage Productivity Center. These data sources include Data agents, Storage Resource agents, Fabric agents, Tivoli Storage Productivity Center servers, CIMOM agents, Out of Band agents, and VMWare Virtual Infrastructure.

#### Aggregated views

These views provide summary information for the database history, data in a database instance, and the Data agent file system.

#### **Reporting views**

These views combine several different entities into one view, such as aggregate database and file system summary views, file size, time, and age distribution views, enterprise-wide statistics views, directory size views, and historical views of statistics for database summaries, ping jobs, user space usage, and files in user groups.

#### **Rollup views**

These views include rollup report information from the master and subordinate Tivoli Storage Productivity Center servers, Data agents, Fabric agents, Storage Resource agents, host cluster data, computer group, host, database computer groups, fabric SAN assets, switch assets, storage subsystem group, storage subsystems, and Data Manager for Databases.

See the Tivoli Storage Productivity Center's support Web site for detailed descriptions of the views provided with Tivoli Storage Productivity Center: http://www.ibm.com/systems/support/storage/software/tpc

This Web page contains the following additional documentation:

- Information about the TPCREPORT schema, including:
  - A list of the views that exist in the schema and descriptions of the columns with the views.
  - A list of the views that contain performance data and descriptions of the performance metrics within those views.
  - Diagrams that show the relationships between views.

• A diagram that traces the relationship between a computer and a storage subsystem disk and shows the views that contain information about the storage entities within that relationship.

# Accessing views in the database repository

Use SQL to access the views in IBM Tivoli Storage Productivity Center database repository. You can do this using an SQL command line or an application capable of using SQL to retrieve information from views. This topic provides an example of how to create and view a report based on those views.

To retrieve information from the database repository you must have the proper authority to access the views. You must also collect information about your storage assets to populate those views with information. See "Planning for SQL access to IBM Tivoli Storage Productivity Center's views" on page 114 for more information.

To perform the steps described in this topic, you must install the correct version BIRT. You can download BIRT v2.2.1 from the following Web page: http://www-01.ibm.com/software/brandcatalog/portal/opal/ details?catalog.label=1TW10OT02. You must use this version of BIRT when working with IBM Tivoli Storage Productivity Center and Tivoli Common Reporting.

You can use a number of SQL and reporting tools for accessing and viewing the content of IBM Tivoli Storage Productivity Center's exposed views. For example, you can use the DB2 Command Line Processor to run SQL commands against the views.

This topic describes how to use BIRT to create a report package based on the views and how to import that package into Tivoli Common Reporting for viewing. Tivoli Common Reporting is installed with IBM Tivoli Storage Productivity Center.

See the following Web sites for more information about BIRT and Tivoli Common Reporting:

- BIRT overview information: http://www.eclipse.org/birt/phoenix/intro/
- Tivoli Common Reporting overview information: http://www.ibm.com/ developerworks/spaces/tcr

Complete these steps to use BIRT and Tivoli Common Reporting to work with Tivoli Storage Productivity Center's views:

- 1. Install BIRT on a computer that has access to Tivoli Storage Productivity Center's database repository. The database repository is located on the computer where the Tivoli Storage Productivity Center server is installed.
- 2. Start the BIRT Designer tool.
- **3**. Set the connection information for the Tivoli Storage Productivity Center database repository in Data Source section of the user interface.
- 4. Use the **Data Sets** section of the user interface to create a report based on SQL queries to the exposed views that are in the TPCREPORT schema. See http://www.eclipse.org/birt/phoenix/intro/ for information on how to use BIRT to create a report. When writing queries against the views make sure to qualify the view names with the TPCREPORT schema (for example, TPCREPORT.STORAGESUBSYSTEM).

**Note:** BIRT limits the amount of views that are displayed to 100 by default. To change this, access the **Preferences** window for the Data Set Editor and enter a value greater than **275** in the **Maximum number of tables in each schema to display** field.

- 5. Define the layout of the report. Use BIRT to customize the appearance of a report, including customizing column names and creating charts, graphics, and aggregated totals for the data in the report. Use the preview function to view a snapshot of the report that you defined.
- 6. Create a report package (archive file) for the reports to import into Tivoli Common Reporting.
- 7. Import the report package into Tivoli Common Reporting.
  - a. Start Tivoli Integrated Portal. See "Starting the Tivoli Storage Productivity Center GUI from Tivoli Integrated Portal" on page 467 for information on how to start Tivoli Integrated Portal.
  - b. Expand **Reporting** in the navigation tree and click **Common Reporting**.
  - c. Right-click **Report Sets** and select **Import Report Package**.
  - d. Select the report package you want to import and click **Import**. Click **Overwrite** in the **Advanced Options** section if the report package was previously imported. The name of the report package appears in the **Reports** section of the panel.
  - e. Right-click the report package and select **Views As** > *output\_type*, where *output\_type* represents the format of the generated report.
  - f. View the report.

# Options files for installing or uninstalling IBM Tivoli Storage Productivity Center in silent mode

This topic describes the installation and uninstallation options files for Tivoli Storage Productivity Center. Use these files to install or uninstall Tivoli Storage Productivity Center in silent mode.

These options are found in the installation directory. By default this is C:\Program Files\IBM\TPC or /opt/IBM/TPC.

Options file	Description
setup_agents.iss	Provides installation options for the Data agent and the Fabric agent.
uninstall.iss	Provides options used during an uninstall of the Data agent and Fabric agent. This can also uninstall the database schema if you have installed the database on a remote system.

Table 58. Options files for installing or uninstalling in silent mode

# setup\_agents.iss options file

The setup\_agents.iss file is an options file that allows you to install the Data agent and the Fabric agent on the local computer. Use the setup\_agents.iss file to provide options for installation in silent mode.

The setup\_agents.iss options file is found on the installation DVD or electronic image in the root directory. Copy this file to a directory. Before you can install IBM Tivoli Storage Productivity Center, you must change the appropriate parameters in the options file and save the file.
Follow these guidelines when using the setup\_agents.iss file:

- All variables are required unless commented out (meaning, a pound symbol (#) precedes it).
- Removing or commenting out the variables (for example, lines that start with -P or -V) from the setup\_agents.iss file can cause the installation to fail.
- If you are not familiar with the installation variables, then you should use the interactive installation wizard for Tivoli Storage Productivity Center.
- You cannot remotely deploy an agent in silent mode.
- Data agents and Fabric agents support only IPv4, but not IPv6. The Data agent connects to the Data server, and the Fabric agent connects to the Device server. Therefore, the Data server and the Device server addresses used for the agents can be only IPv4 addresses or names.

See the following example of the file used to install the agents in silent mode. All variables are required unless commented out (meaning, a pound symbol (#) precedes it).

Figure 91. An example of setup\_agents.iss file

```
# (C) Copyright Tivoli Systems, Inc. 2005, 2008
# 5608-VC0
# All Rights Reserved
# Licensed Material - Property of Tivoli Systems, Inc,
# an IBM company.
# This option file is used to do silent installation of TPC agents.
# Data and Device Agents will be supported through this
# silent installation options file.
# NOTE! All variables are required unless they are commented out
# (a '#' in front of the variable). Removal or commenting out variables can
# cause the install to fail.
# Variables set to "" e.g. -V varCASvcUsrID="" should be left as is when not
# using.
# If you are not familiar with the install variables it is suggested that you
# do an interactive install.
# IBM Tivoli Storage Productivity Center Install Location
# The install location of the product. Specify a valid directory into which the
# product should be installed. If the directory contains spaces, enclose it in
# double-quotes.
#
# Example:
# -P installLocation="/opt/IBM/TPC"
# -P installLocation="C:\Program Files\IBM\TPC"
```

```
-P installLocation="C:\Program Files\IBM\TPC"
******************
# Install Data Agent. Default is true
#
**********************
-V varInstallDataAgt="true"
# Install Fabric Agent. Default is true
********************
-V varInstallDevAgt="true"
**********
# Agent Manager Hostname. Required when installing TPC Servers or Agents.
# Example:
# -V varAMHostname="amserver.yourdomain.com"
********************
-V varAMHostname=""
# Agent Manager Secured Port Number <-- Default is 9511</pre>
*****************
-V varAMRegPort="9511"
# Agent Manager Public Port <-- Default is 9513</pre>
-V varAMPubPort="9513"
# Common Agent Port <-- Default is 9510</pre>
-V varCAPort="9510"
*****************
# Common Agent Registration Password. Required when installing TPC Agents.
# changeMe is the default id for Demo certs on Agent Manager.
******************
-V varCAPassword="changeMe"
# CA Installation Location
# Common Agent installation location. (Provide this location in old or
  or new install location)
#
Examples:
  -V varCAInstallLoc="C:\\Program Files\\IBM\\TPC\\ca" <-- Default Location
#
  -V varCAInstallLoc=/opt/IBM/TPC/ca
#
                             <-- Default Location
#
***************
-V varCAInstallLoc="C:\\Program Files\\IBM\\TPC\\ca"
```

```
# Common Agent Port. Required when installing TPC Agents. Default port is 9510
-V varCAPort="9510"
**********
# Common Agent Service Name (For Windows only). Default is "". If service name
# not provided the default name is IBMTivoliCommonAgent(#)
*******************
-V varCASvcName=""
# Common Agent Service User ID (For Windows only). Default is ""
# If you don't supply a user, user itcauser(#) will be created with a random
# password.
***************
-V varCASvcUsrID=""
**********
# Common Agent Service User Password (For Windows only). Default is ""
#
-V varCASvcUsrPW=""
# Whether to install New Common Agent if it does not exist. Default is
# -V varInstallNewCA="true" and -V varUseOldCA="false".
# When using an existing Common Agent -V varInstallNewCA="false" and
# -V varUseOldCA="true"
-V varInstallNewCA="true"
-V varUseOldCA="false"
#
# Data Server Host Name. Both Required when installing tpc agents.
#
# Data and Device Server addresses used for the Agents can be only IPv4
# addresses or names. The TPC GUI can connect to the Data Server over IPv4
# and IPv6, and the Data Server can connect to Device Server over IPv4 and IPv6.
# For this reason we have two separate variables used for Data servers.
# Example:
#
 -V varDataSrvName=tpcserver.yourdomain.com
                              <-- IPV6 or IPV4
     -V varDataSrvNameForAgent=tpcserver.domain.com <-- IPV4 onlv
#
#
             ****
-V varDataSrvName=""
-V varDataSrvNameForAgent=""
#
# Data Server Port Number. Default is 9549
#
***************
-V varDataSrvPort="9549"
```

```
# Device Server Host Name. Both Required when installing tpc fabric agent.
# Data and Device Server addresses used for the Agents can be only IPv4
# addresses or names. The TPC GUI can connect to the Data Server over IPv4
# and IPv6, and the Data Server can connect to Device Server over IPv4 and IPv6.
# For this reason we have two separate variables used for Device server.
# Example:
# -V varDevSrvName=tpcserver.yourdomain.com
                             <-- IPV6 or IPV4
     -V varDevSrvNameForAgent=tpcserver.domain.com <-- IPV4 only
#
#
-V varDevSrvName=""
-V varDevSrvNameForAgent=""
******************
# Device Server Port Number. Default is 9550
-V varDevSrvPort="9550"
******************
# Host Authentication password. Required when installing fabric agent.
******************
-V varHostAuthUsrPW=""
# Do Scan by Data Agent after the install. Default is false.
******************
-V varDataAgtScan="false"
******************
# Data agent able to run scripts or not. Default is true
#
-V varDataAgtScripts="true"
# REQUIRED VARIABLES: DO NOT REMOVE OR MODIFY
-V LICENSE ACCEPT BUTTON="true"
-V LICENSE REJECT BUTTON="false"
-V varCreateDBSchm="false"
-V varInstallDataSrv="false"
-V varInstallDevSrv="false"
-V varInstallGUI="false"
-V varInstallCLI="false"
-V varInstallTIP="false"
-V varSkipTIPInstall="true"
#
***************
# REQUIRED VARIABLES: DO NOT REMOVE OR MODIFY
******
```

### uninstall.iss file

The uninstall.iss file provides options used during an uninstallation of the Data agent and Fabric agent from the local computer. You can also uninstall the CLI, GUI, and a database schema with this file. Use the uninstall.iss file to provide options for uninstallation in silent mode.

The uninstall.iss options file is found in the following default installation directory:

Windows: C:\Program Files\IBM\TPC UNIX or Linux: <usr or opt>/IBM/TPC

Before you can uninstall the Data agents or Fabric agents, you must change the appropriate parameters in the options file and save the file. See Figure 92 on page 627.

```
# (C) Copyright Tivoli Systems, Inc. 2005, 2009.
# 5608-VC0
# All Rights Reserved
# Licensed Material - Property of Tivoli Systems, Inc,
# an IBM company.
************
# This option file is used to do silent uninstall of TPC components.
# Creation date: 11/29/2005
**************************
*************
# Uninstall and drop the database
-V varDropDBSchm="false"
*******
# Uninstall Data Agent
-V varUninstallDataAgt="false"
***************
# Uninstall Device Agent
-V varUninstallDevAgt="false"
*******
***************
#
# Uninstall the Common Agent
-V varForceUninstallCA="false"
***************
#
# Uninstall GUI
-V varUninstallGUI="false"
***************
# Uninstall CLI
-V varUninstallCLI="false"
*****
Figure 92. uninstall.iss file
```

# Appendix A. General information for Storage Resource agents and Data agents

This section provides general information about installing Storage Resource agents and Data agents.

#### Windows systems

If you want to install a Storage Resource agent or Data agent on Windows targets, the Enable NetBIOS over TCP/IP option must be selected in the Control Panel settings for the machine's network connections properties. To set this option, click Start > Settings > Control Panel > Network and Dial-Up Connections > <some\_connection> > Properties > Internet Protocol (TCP/IP) > Advanced > WINS > Enable NetBIOS over TCP/IP.

See the documentation for your firewall to determine if these ports are not blocked for inbound requests.

To determine if security policies are blocking the connection ports, click **Start > Settings > Control Panel > Administrative Tools**.

Depending on whether your policies are stored locally or in Active Directory, follow these directions:

Locally stored policies

For locally stored policies, click **Start > Settings > Control Panel > Administrative Tools > Local Security Policy > IP Security Policies on Local Computer**.

Policies stored in Active Directory

For policies stored in Active Directory, examine the IP security policies and edit or remove filters that block the ports:

- Click Administrative Tools > Default Domain Security Settings > IP Security Policies on Active Directory.
- Click Administrative Tools > Default Domain Controller Security Settings > IP Security Policies on Active Directory.

For all Windows systems, the Server service must be running to connect to a Windows system using the Windows protocol.

The following table lists the ports reserved for NetBIOS. Ensure that these ports are not blocked.

Port	Description
135	NetBIOS Remote procedure call. (Not currently used.)
137	NetBIOS name service.
138	NetBIOS datagram. (Not currently used.)
139	NetBIOS session (for file and print sharing).
445	CIFS (on Windows XP).

For Windows Server 2008, shares must be shared for the Guest or Everyone accounts, and password protected sharing must be disabled. To disable password protected sharing, follow these steps:

- 1. Click Control Panel > Networking and Sharing Centre.
- 2. Click the down arrow next to **Password protected sharing**.
- 3. Click Turn off password protected sharing.
- 4. Click Apply. Exit from the Control Panel.

#### **UNIX systems using RSH protocol**

If RSH is configured to use a user ID and password, the connection will fail. To successfully connect to a system using RSH, you must set up the .rhosts file (in the account's home directory). RSH must be configured to accept a login from the system that is running your application.

### Appendix B. Accessibility features for IBM Tivoli Storage Productivity Center

IBM strives to provide products with usable access for everyone, regardless of age or ability.

#### Accessibility features

The following list includes the major accessibility features in IBM Tivoli Storage Productivity Center:

- IBM Tivoli Storage Productivity Center functions are available using the keyboard for navigation instead of the mouse. You can use keys or key combinations to perform operations that can also be done using a mouse. However, you must use the mouse to navigate the Topology Viewer and report graphs. Standard operating system keystrokes are used for standard operating system operations.
- You can use screen readers to read the user interface.
- The user interface communicates all information independently of color.
- The *IBM Tivoli Storage Productivity Center Information Center*, and its related publications, are accessibility-enabled and include the following accessibility features:
  - The information center is provided in XHTML 1.0 format, which is viewable in most Web browsers. XHTML allows you to view documentation according to the display preferences set in your browser. It also allows you to use screen readers and other assistive technologies.
  - All documentation is available in PDF format.
  - All images are provided with alternative text, so that users with vision impairments can understand the contents of the images.

#### **Keyboard navigation**

This product uses standard Microsoft Windows navigation keys that are supported through the native Windows manager.

#### Interface information

Use the options available in the **Preferences** > **Look and Feel** menu to select how to display the IBM Tivoli Storage Productivity Center user interface. To do this, complete the following steps:

- 1. Start the IBM Tivoli Storage Productivity Center user interface.
- Select one of the following options from the Preferences > Look and Feel menu to change the visual appearance of the user interface to best suit your visual needs:
  - Windows Classic
  - Windows
  - CDE/Motif
  - Metal

#### **Related accessibility information**

You can view the publications for IBM Tivoli Storage Productivity Center in Adobe Portable Document Format (PDF) using the Adobe Acrobat Reader. The PDFs are provided on a CD that is packaged with the product, or you can access them from the Printable documentation topic in the information center at http://publib.boulder.ibm.com/infocenter/tivihelp/v4r1/index.jsp.

#### IBM and accessibility

See the IBM Human Ability and Accessibility Center website for more information about the commitment that IBM has to accessibility.

### Appendix C. TCP/IP ports used by the IBM Tivoli Storage Productivity Center family

This topic lists the default ports that should be opened through the firewall when you install the IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication servers. You must disable the firewall program or open the ports to allow incoming requests to the IBM Tivoli Storage Productivity Center ports. Review these ports before installing the IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication.

#### TCP/IP ports used by IBM Tivoli Storage Productivity Center

See Table 9 on page 19 for the IBM Tivoli Storage Productivity Center ports.

Component	Session initiator (server perspective)	Inbound/ outbound (server perspective)	Port	Inbound/ outbound (agent perspective)	Session initiator (agent perspective)
Data server		Both	Default: 9549 (see note 1)		
Device server		Both	9550		
Common agent	Yes	Outbound	9510	Inbound	No
Agent Manager	No	Inbound	9511	Outbound	Yes
Agent Manager	Yes	Both	9512	Both	Yes
Agent Manager	No	Inbound	9513	Outbound	Yes
Common agent (no access needed)			9514	Local to server	
Common agent(no access needed)			9515	Local to server	
Agent Manager	No	Inbound	80	Outbound	Yes
Remote installation of UNIX agent	Yes	Outbound	SSH (22)	Both	No
Remote installation of Windows agent	Yes	Outbound	NetBIOS Sessions Service (139)		

Table 59. TCP/IP ports used by IBM Tivoli Storage Productivity Center

Component	Session initiator (server perspective)	Inbound/ outbound (server perspective)	Port	Inbound/ outbound (agent perspective)	Session initiator (agent perspective)
Remote installation of UNIX agent	Yes	Outbound	RSH (514)	Both	No
Remote installation of UNIX agent	Yes	Outbound	REXEC (512)	Both	No
Remote installation of UNIX agent	Yes	Inbound	601		
Remote installation of all agents	Yes	Inbound	Data Server 9549		
Device server to CIM agent	Yes	Outbound	Default: HTTP: 5988 HTTPS: 5989		
VMware VI Data Source to VirtualCenter or ESX server	Yes	Outbound	Default: HTTP: 80 HTTPS: 443		
Tivoli Integrated Portal server. See note 5.	Yes	Outbound	389		
Device server. See note 5.	Yes	Outbound	389		
IBM Tivoli Storage Productivity Center for Replication server. See note 5.	Yes	Outbound	389		

Table 59. TCP/IP ports used by IBM Tivoli Storage Productivity Center (continued)

Table 59. TCP/IP ports used by IBM Tivoli Storage Productivity Center (continued)

	Session	Inbound/		Inbound/	Session
	initiator	outbound		outbound	initiator
	(server	(server		(agent	(agent
Component	perspective)	perspective)	Port	perspective)	perspective)

- 1. Data server inbound server port plus another port that is 10 greater than the Data server port (9549). For example, if the Data server port is 9549, than another port would be 9549+10 or 9559.
- 2. If you choose to use a port other than the default port (9510) for the Common agent, make sure that the port you choose, and the ports above it, are available for use. For example, if N represents the open port you want to use, ensure that ports N+4 and N+5 are open as well.
- **3**. When you install the Data agent, you can specify a listener port for a remote probe. This is the port that the program uses to communicate back to the installation program.
- 4. You can find the port numbers used on your system by running the following command:

netstat -an

5. If you intend to install IBM Tivoli Storage Productivity Center so that it authenticates users against an LDAP-compliant repository, then the Embedded WebSphere Application Servers for Tivoli Integrated Portal, IBM Tivoli Storage Productivity Center Device server, and IBM Tivoli Storage Productivity Center for Replication need to be able to initiate an outbound connection to the LDAP-compliant repository, which typically listens on port 389.

# Other TCP/IP ports used by IBM Tivoli Storage Productivity Center

Port	Default
DB2	50000
CIM agent for SAN Volume Controller	For proxy CIM agent: 5988 (http) 5989 (https)
CIM agent for IBM TotalStorage Enterprise Storage Server (ESS)	5989
CIM agent for DS8000	<pre>6989 (for embedded CIM agent,</pre>
IBM Tivoli Storage Productivity Center with DS8000 GUI	8451 8452
IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for Replication	162 (default SNMP listening port)

Table 60. Other TCP/IP ports used by IBM Tivoli Storage Productivity Center

# TCP/IP ports used by IBM Tivoli Storage Productivity Center for Replication

Table 11 on page 21 shows the ports used for incoming communication. Table 12 on page 21 shows the ports used for outgoing communication.

Table 61. TCP/IP ports used by IBM Tivoli Storage Productivity Center for Replication for incoming communication

Port	Description
3080 and 3443	A Web browser typically communicates with the IBM Tivoli Storage Productivity Center for Replication GUI using HTTP ports 3080 and 3443. These ports are configurable from the IBM Tivoli Storage Productivity Center for Replication installer during installation.
5110	The IBM Tivoli Storage Productivity Center for Replication command line and GUI typically communicate with the IBM Tivoli Storage Productivity Center for Replication server using port 5110.
5120	IBM Tivoli Storage Productivity Center for Replication uses port 5120 for communication with other IBM Tivoli Storage Productivity Center for Replication servers for high-availability purposes.
Note: If you changed	ports 3080 or 3443 during the installation or made changes to the

other port settings, note the values to which these settings were changed.

Table 62. TCP/IP ports used by IBM Tivoli Storage Productivity Center for Replication for outgoing communication

Port	Description
2433	For communication with ESS.
1750	For communication with DS Storage Systems.
22	For communication with SAN Volume Controller devices.

Note:

- If you changed the port configuration of your storage controller, the ports would be different.
- Your network configuration should allow for IBM Tivoli Storage Productivity Center for Replication to send outgoing TCP/IP packets to the storage controllers. It is possible when adding the storage controllers to IBM Tivoli Storage Productivity Center for Replication to set a specific port number for your storage controller.
- Since there are typically multiple applications running on a server, it is possible that port conflicts might arise if other applications attempt to use the same ports that IBM Tivoli Storage Productivity Center for Replication is using. You can find the port numbers used on your system by running the following command:

netstat -an

- If firewalls are being used in your configuration, make sure that none of these ports are being blocked. Ensure that not only is the IBM Tivoli Storage Productivity Center for Replication server granted access to reach the other components, but that the other components are granted access to reach the IBM Tivoli Storage Productivity Center for Replication server.
- If you are running Windows Server 2008, you need to configure the inbound and outbound rules for IBM Tivoli Storage Productivity Center for Replication. To create a new outbound rule, launch the New Outbound Rule Wizard from the Windows Firewall with Advanced Security menu.

# Appendix D. Work sheet for user IDs and passwords

This section provides a work sheet to help you keep track of user IDs and passwords during the planning and installation of IBM Tivoli Storage Productivity Center.

Item	Description	Your input
DB2 administrator user ID and password	This user ID and password is required to install Tivoli Storage Productivity Center. On Windows, this user ID must be a member of the DB2ADMNS group and Administrators group. On UNIX, the user ID must be the instance owner of the instance you wish to use. This user ID and password is created when you install DB2.	
Certificate authority password	This password allows you to look at the certificate files if you have problems. Specified when you install the Agent Manager.	
Common agent registration password	This is the password required by the Common agent to register with the Agent Manager. Specified when you install the Agent Manager. You must specify this password when you install the Common agent. To change the Common agent registration password, see "Changing the agent registration password" on page 481.	
Common agent service logon user ID and password	This is for Windows only and is optional. This creates a new service account for the Common agent to run under. If your enterprise has a security policy that requires long passwords, the installation can fail. This user ID and password allows you to run under a local account user name and password that meets your enterprise's security policy. This user ID and password will be created if you do not have one.	No default. If this user ID and password does not exist, these will be created at installation time.

Table 63. User IDs and passwords for Tivoli Storage Productivity Center installation

Item	Description	Your input
Host authentication password	<ul><li>This password is required for:</li><li>the Fabric agent to communicate with the Device server</li></ul>	This password is created when you install the Device serverr.
	• the subordinate server when added to the master server (for enterprise-wide reporting)	
	Specified when you install the Device server. You must specify this password when you install the Fabric agent.	
NAS filer login user ID and password	This is for Windows only. This is the default user name and password used by Data agents during NAS discovery.	
Resource manager registration user ID and password	This is the user ID and password required by the Device server and Data server to register with the Agent Manager. You must specify this user ID and password when you install the Device server or Data server. For information on how to change the user ID and password, see "Changing the registration password for a resource manager" on page 483.	The default user ID is <b>manager</b> . The default password is <b>password</b> .
WebSphere administrator user ID and password	This is the user ID and password required by the Device server to communicate with embedded WebSphere. Embedded WebSphere runs as a Windows Service. The Windows Service runs under the authority of this user ID and password. This user ID and password is only used when you install the Device server.	If this user ID and password does not exist, these will be created at installation time.
Windows Service account and password	This account and password is valid for Windows only and lets the agent run under this service account.	When you install the Tivoli Storage Productivity Center agent, you will be able to specify a domain name which validates the account and password.

Table 63. User IDs and passwords for Tivoli Storage Productivity Center installation (continued)

Item	Description	Your input
LDAP Tivoli Storage Productivity Center Administrator username and password and LDAP Tivoli Storage Productivity Center Administrator group	These values are relevant if you install Tivoli Storage Productivity Center so that it authenticates users against an LDAP-compliant repository. The username, password, and group must already exist in your LDAP-compliant repository in the "branches" specified by the "Relative Distinguished Name for usernames" and the "Relative Distinguished Name for groups" values. The user must also be a member of the group.	During the Tivoli Storage Productivity Center installation, the LDAP Tivoli Storage Productivity Center Administrator username value is used to set the WebSphere Administrative ID value for the Tivoli Integrated Portal server, the Tivoli Storage Productivity Center Device server, and the Tivoli Storage Productivity Center for Replication server. Also during the Tivoli Storage Productivity Center installation, the LDAP Tivoli Storage Productivity Center Administrator group value is mapped to the "superuser" role in Tivoli Integrated Portal, Tivoli Storage Productivity Center, and Tivoli Storage Productivity Center for Replication to allow initial access to the applications once the installation is complete.

Table 63. User IDs and passwords for Tivoli Storage Productivity Center installation (continued)

For information about valid user IDs and passwords, see "Valid characters for user IDs and passwords" on page 607

### Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing IBM Corporation North Castle Drive Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation Licensing 2-31 Roppongi 3-chome, Minato-ku Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk. IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation Software Interoperability Coordinator, Department YBWA 3605 Highway 52 N 11400 Burnet Road Rochester, MN 55901 U.S.A

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

### **Trademarks**

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (<sup>®</sup> or <sup>™</sup>), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Adobe and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Intel is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Red Hat and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

### Glossary

This glossary includes terms and definitions for IBM Tivoli Storage Productivity Center.

The following cross-references are used in this glossary:

- *See* refers the reader from a term to a preferred synonym, or from an acronym or abbreviation to the defined full form.
- *See also* refers the reader to a related or contrasting term.

To view glossaries for other IBM products, go to: http://www.ibm.com/software/globalization/ terminology/.

**agent** An entity that represents one or more managed objects by sending notifications regarding the objects and by handling requests from servers for management operations to modify or query the objects.

#### Basic HyperSwap<sup>™</sup>

In System *z*, a replication feature that performs the following actions:

- Monitoring for events that indicate a storage device has failed
- Determining whether the failing storage device is part of a Peer-to-Peer Remote Copy (PPRC) pair
- Determining from policy, the action to be taken
- Ensuring that data consistency is not violated
- Swapping the I/O between the primary logical devices in the consistency group with the secondary logical devices in the consistency group.
- Allowing only CKD volumes to be added to the HyperSwap session.
- CIM See Common Information Model.

#### CIM agent

The code that consists of common building blocks that can be used instead of proprietary software or device-specific programming interfaces to manage CIM-compliant devices.

#### CIM object manager (CIMOM)

The common conceptual framework for data management that receives, validates,

and authenticates the CIM requests from the client application. It then directs the requests to the appropriate component or service provider.

#### CIMOM

See CIM object manager

CKD Count key data

#### cluster

1. In SAN Volume Controller, a pair of nodes that provides a single configuration and service interface. 2. In IBM System Storage DS8000, a partition capable of performing all DS8000 series functions. With two clusters in the DS8000 storage unit, any operational cluster can take over the processing of a failing cluster.

#### **Common Information Model (CIM)**

An implementation-neutral, object-oriented schema for describing network management information. The Distributed Management Task Force (DMTF) develops and maintains CIM specifications.

#### comma-separated value file

A text file, created in a spreadsheet program such as Microsoft Excel. A CSV file includes each of the copy sets you want to add to the session separated by a comma.

#### community name

The part of an SNMP message that represents a password-like name and that is used to authenticate the SNMP message.

#### consistency group

The set of target volumes in a session that have been updated to preserve write ordering and are therefore, recoverable.

#### copy set

A set of volumes that contain copies of the same data. All the volumes in a copy set are the same format (count key data [CKD] or fixed block) and size.

CSV See comma-separated value file

#### data collection

See discovery.

#### data exposure

The time between the point at which the data is written to primary storage, and when it is replicated to secondary storage. Data exposure includes factors such as:

- Requested consistency-group interval time
- Type of storage systems
- Physical distance between the storage systems
- Available bandwidth of the data link
- I/O load on the storage systems

#### discovery

The process of finding resources within an enterprise, including finding the new location of monitored resources that were moved. Discovery includes the detection of changes in network topology, such as new and deleted nodes or new and deleted interfaces. See also *discovery interval*.

#### discovery interval

The frequency at which topology and attribute information is gathered. The discovery interval is set by a schedule to occur either periodically or at specific times. Discovery can also occur at other times, such as when triggered by an event from a SAN switch.

#### discovery job

A job that enables you to find new Windows machines that have been introduced into your environment, identify the servers and volumes within NetWare trees (NDS trees), discover the file systems within NAS filers, and discover the CIMOMs in your environment and the storage subsystems managed by those CIM/OMs.

#### enterprise repository

A component of the Data server that records and stores all information about the monitored computers' storage assets and their usage over time. The repository is organized into relational database tables and is accessed by Data server using Java Database Connectivity (JDBC).

event Any significant change in the state of a system resource, network resource, or network application. An event can be generated for a problem, for the

resolution of a problem, or for the successful completion of a task. Examples of events are: the normal starting and stopping of a process, the abnormal termination of a process, or the malfunctioning of a server.

**fabric** A complex network using hubs, switches, and gateways. Fibre channel uses a fabric to connect devices.

#### failover and failback

The implementation of a complex local or remote disaster-recovery solution with the capability of a two-way site switch.

#### fibre channel

A technology for transmitting data between computer devices. It is especially suited for attaching computer servers to shared storage devices and for interconnecting storage controllers and drives.

#### FlashCopy

An optional feature of the DS8000 series that can make an instant copy of data; that is, a point-in-time copy of a volume.

#### global copy

An optional capability of the DS8000 remote mirror and copy feature that maintains a fuzzy copy of a logical volume on the same DS8000 storage unit or on another DS8000 storage unit. In other words, all modifications that any attached host performs on the primary logical volume are also performed on the secondary logical volume at a later point in time. The original order of update is not strictly maintained. See also *remote mirror* and *copy* and *metro mirror*.

#### global mirror

An optional capability of the remote mirror and copy feature that provides a 2-site extended distance remote copy. Data that is written by the host to the storage unit at the local site is automatically maintained at the remote site. See also Metro Mirror and Remote Mirror and Copy.

#### globally unique identifier (GUID)

An algorithmically determined number that uniquely identifies an entity within a system.

#### heat map

A color-coded data chart where colors are used to differentiate values in a data set.

**host** A computer that is connected to a network (such as the Internet or a SAN) and provides a point of access to that network. Also, depending on the environment, the host can provide centralized control of the network. The host can be a client, a server, both a client and a server, a manager, or a managed host.

#### host volume

A volume that represents the volume functional role from an application point of view. The host volume can be connected to a host or server, and receives read, write, and update application I/Os, depending on the site that the application is writing to.

#### in-band discovery

The process of discovering information about the SAN, including topology and attribute data, through the fibre-channel data paths. Contrast with *out-of-band discovery*.

#### intermediate volume

The target of the remote copy relationship, and the source of a FlashCopy relationship in which the target of the FlashCopy is the H2 volume.

#### job scheduler

A component of the Data server that deploys all monitoring activities. The job scheduler controls when monitoring jobs are run by agents.

#### journal volume

A volume that functions like a journal and holds the required data to reconstruct consistent data at the Global Mirror remote site. When a session must be recovered at the remote site, the journal volume is used to restore data to the last consistency point.

#### logical unit number (LUN)

An identifier used on a SCSI bus to distinguish among devices (logical units) with the same SCSI ID. For a SCSI bus, a LUN represents a storage volume.

LUN See logical unit number.

#### managed disk (MDisk)

A SCSI logical unit that a Redundant Array of Independent Disks (RAID) controller provides and a cluster manages. The MDisk is not visible to host systems on the SAN.

#### managed host

A host that is managed by Tivoli Storage Productivity Center and one or more active in-band fabric agents. Install in-band fabric agents on host systems with host bus adapters (HBAs) that are connected to the SAN fabrics that you want to manage.

#### **Management Servers**

Increased availability of the replication management software with the implementation of a high-availability configuration such that one management workstation runs as standby, ready to take over in case of a failure of the active workstation.

**Note:** The takeover is not automatic and requires you to issue a takeover command.

#### metro mirror

A function of a storage server that maintains a consistent copy of a logical volume on the same storage server or on another storage server. All modifications that any attached host performs on the primary logical volume are also performed on the secondary logical volume. See also *Remote Mirror* and *Copy* and *Global Copy*.

#### Metro Global Mirror

The three-site remote mirroring solution.

#### out-of-band discovery

The process of discovering SAN information, including topology and device data, without using the fibre-channel data paths. A common mechanism for out-of-band discovery is the use of SNMP MIB queries, which are invoked over a TCP/IP network. Contrast with *in-band discovery*.

#### ping job

A job that tracks the availability of assets and that is performed by an agent. Several ping jobs can be used to monitor the availability of any computer or subset of computers in the network. **pool** A named set of storage volumes that is the destination for storing client data.

#### primordial pool

Unallocated storage capacity on a storage device. Storage capacity can be allocated from primordial pools to create storage pools.

#### probe job

A job that itemizes and creates an inventory of assets, such as computers, controllers, disk drives, file systems, and logical units, and that is performed by an agent. Several probe jobs can be used on any computer or subset of computer

**RAID** See Redundant Array of Independent Disks.

#### Recovery point objective (RPO)

The maximum amount of data that you can tolerate losing in the case of a disaster.

#### remote console

A console that is installed on a machine other than the one on which the server is installed. A remote console lets you access Tivoli Storage Productivity Center from any location.

#### remote mirror and copy

A feature of a storage server that constantly updates a secondary copy of a logical volume to match changes made to a primary logical volume. The primary and secondary volumes can be on the same storage server or on separate storage servers.

role A function that a volume assumes is the copy set. The role is is composed of the intended use and, for Global Mirror and Metro Mirror, the volume's site location. Every volume in a copy set is assigned a role. A role can assume the functions of a host volume, journal volume, or target volume. For example, a host volume at the primary site might have the role of Host1, while a journal volume at the secondary site has the role of Journal2.

#### role pair

The association of two roles in a session that take part in a copy relationship. For example, in a metro mirror session, the role pair could be the association between the volume roles of Host1 and Host2. In another example, a Host1 volume could be a host volume on the primary site, and a Host2 volume could be a host volume on the secondary site.

#### **SAN** See storage area network.

#### scan job

A job that monitors the usage and consumption of your storage and the constraints and that is performed by an agent. Several scan jobs can be used to monitor the file systems on any computer or subset of computers.

**SCSI** See Small Computer Systems Interface.

#### session

A collection of multiple copy sets that comprise a consistency group.

#### site switching

See also failover and failback.

**SMI-S** See Storage Management Initiative -Specification.

#### SMI-S agent

See CIM Object Manager (CIMOM). See also Storage Management Initiative -Specification (SMI-S).

- **SNIA** See Storage Networking Industry Association.
- **source** The site where production applications run while in normal operation. The meaning is extended to the disk subsystem that holds the data as well as to its components: volumes and LSS.

#### storage area network

A dedicated storage network tailored to a specific environment, combining servers, storage products, networking products, software, and services.

#### storage group

A collection of storage units that jointly contain all the data for a specified set of storage units, such as volumes. The storage units in a group must be from storage devices of the same type.

# Storage Management Initiative - Specification (SMI-S)

The standard that defines the protocol used for communication with SMI-S agents.

# Storage Networking Industry Association (SNIA)

An alliance of computer vendors and

universities that focus on developing and promoting industry standards for storage networks.

#### storage pool

An aggregation of storage resources on a SAN that have been set aside for a particular purpose.

#### System z Global Mirror

See also Global Mirror.

target The site to where the data is replicated, the copy of the application data. The meaning is extended to the disk subsystem that holds the data as well as to its components: volumes and logical subsystem (LSS).

#### target volume

A volume that receives data from a host volume or another intermediate volume. It is used only in FlashCopy sessions.

#### topology

The physical and logical arrangement of devices in a SAN. Topology can be displayed graphically, showing devices and their interconnections.

#### **VDisk** See *virtual disk*.

#### virtual disk (VDisk)

A device that host systems attached to the storage area network (SAN) recognize as a Small Computer System Interface (SCSI) disk.

#### virtualization

A concept in which a pool of storage is created that contains several disk subsystems. The subsystems can be from various vendors. The pool can be split into virtual disks that are visible to the host systems that use them.

#### virtual storage area network (VSAN)

A Cisco technology that allows independent logical fabrics to be defined from a set of one or more physical switches. A given switch port is assigned to only one VSAN. Each VSAN is completely isolated from the other VSANs and functions as a separate and independent fabric with its own set of fabric services (for example, Name Services, zoning, routing, and so on).

#### volume

The basic entity of data storage as defined by the SCSI protocol. A volume is a logical address space, having its data content stored on the systems disk drives.

- **VSAN** See virtual storage area network.
- **zone** A segment of a SAN fabric composed of selected storage devices nodes and server nodes. Only the members of a zone have access to one another.

#### zone set

A group of zones that function together on the fabric. Each zone set can accommodate up to 256 zones. All devices in a zone see only devices assigned to that zone, but any device in that zone can be a member of other zones in the zone set.

### Index

### Numerics

64-bit environment supported 15

### Α

accessibility features for this product 631 accessing the Tivoli Storage Productivity Center for Replication server 463 adding installation license 240 Agent Manager administering 424 backing up certificates 420 certificate authority password 56 changing agent registration password 481 changing DB2 password 477 changing DB2 password on UNIX 479 changing password encryption key 484 changing resource manager registration password 483 changing resource manager registration properties 424 changing the maximum heap size 428 checking version 132 configuration file properties file 482 configuring how long information is saved 427 configuring login threshold 427 configuring to use different port numbers 415 controlling access to agents 56 controlling resource manager access 56 correcting registration failures 537 determining version of 420 duplicate agent registration 424 estimating size of registry 56 hardware requirements 54 installation log files 503 installing 132, 143, 149, 158 log files, packaging for support 419 manually encrypting a password 484 overview 412 port conflicts 535 recovering agents 421 registering 294 reusing an existing manager 429 security considerations 56 software requirements 55 starting 414 stopping 415 TCP/IP ports used 59 toolkit 605 uninstallation log files 504

Agent Manager (continued) uninstalling 394 upgrading 360 using a 32-bit DB2 instance 132, 143 using a 64-bit DB2 instance 158 using a 64-bit DB2 instance on UNIX 149 using multiple managers 429 agent recovery service 412 port conflicts 535 agent registration password changing 481 agent.config 500, 609 agents 424 assigning agents for scan and probe jobs 289 changing the Windows service logon 430 checking the health 430 CIM agents 430 configuration file 293 configuration updates 427 configuring for Data agent upgrade 311 configuring for Storage Resource agent upgrade 311 controlling access to 56 correcting registration failures 537 deploying Storage Resource agents 295 disabling automatic upgrade 447 duplicate registration 424 enabling automatic upgrade 447 hardware requirements 3 in-band Fabric agents 450, 451 increasing memory allocation 474 information collected 613 installing 246 installing Data agents using custom installation 206 installing Fabric agents remotely 259 installing on Virtual I/O Server 259 installing remotely 253 listing on a Virtual I/O Server 461 migrating Storage Resource agent to Data agent 374 out-of-band agents 451 overview 267, 412, 413 planning for CIM agents 64 planning for Data agents 61 planning for Storage Resource agents 32 planning for TagmaStore CIM agents 66 preparing Storage Resource agents for installation 167 recovery 421 registering with a different server 449 removing data 453 removing from registry 424

agents (continued) starting 461, 462 uninstalling 392 uninstalling common agents 392 uninstalling locally 390 uninstalling on Virtual I/O Server 393 uninstalling remotely 391, 392 universal agents 109 using version 1.2.2 Common agents 60 viewing and managing 451 agentTrust.jks file re-encrypting 482 unlocking 481 alerts, overview 269 authorization for users 18 Authorization.xml file 424 controlling resource manager access 56 AuthXMLAddUser command 424 AuthXMLRemoveAuthType command 426 AuthXMLRemoveUser command 425

### В

backup Tivoli Storage Productivity Center 399 Tivoli Storage Productivity Center for Replication 463 batch reports configuring Linux for 331 configuring UNIX for 331 Brocade switches advanced discovery 615 configuring 84 discovery 615 browsers supported 13

### С

certificate authority password 56 certificates backing up 420 creating for Storage Resource agents 302 importing SSL certificates for VMware 490 replacing for Storage Resource agents 307 changing properties 424 CIM agents 430 adding 430 collecting logs 436 collecting XIV logs for 436 discover automatically 432 planning for 64

CIM agents (continued) planning for TagmaStore 66 removing 435 show managed devices 436 testing a connection 435 updating user identification 434 using Service Location Protocol 432 verify they are running 437 viewing information 433 Cisco switches configuring 85 CLI installing 239 Cloudscape database for registry 412 cluster resource group for HACMP 94 cluster resource groups 93 CNT switches configuring 87 commands AuthXMLAddUser 424 AuthXMLRemoveAuthType 426 AuthXMLRemoveUser 425 EncryptAMProps 482 EncryptPW 484 GETAMInfo 420 HealthCheck 605 HealthCheck.bat 605 HealthCheck.sh 605 LogCollector 605 LogCollector.bat 605 LogCollector.sh 605 repocopy 490 common agents overview 412, 413 recovery 421 removing from registry 424 supported 55 uninstalling 392 configuration authorizing users 279 collecting information 613 editing nas.config file 294 for Device server 317 for NetWare 290 for Network Attached Storage 290 for switches 314 guidelines 17 History Aggregator 295 NetApp 100 overview 267 planning for Fabric Manager 81 planning for HBAs 83 planning for rollup reports 47 planning for VMware 105 Removed Resource Retention 312 Resource History Retention 311 role-to-group mapping 279 the Device server 314 Configuration Analysis tool planning 48 configuration files agent..config file 293 agent.config 500, 609 default locations 497 encryption 498, 610

configuration files (continued) for IBM Tivoli Storage Productivity Center 497 scheduler.config 499, 611 server.config 498, 610 server.config file 293 TPCD.config 500, 612 configuration history settings 314 Configuration History tool planning 49 configuration utility how to access Tivoli Storage Productivity Center for Replication 276 how to collect statistics on usage and trending 273 how to create alert definitions 275 how to create alert definitions for storage-related events 273 how to display availability reports 273 how to enable a storage subsystem for provisioning 274 how to manage tape library reports 275 how to manage your fabrics 274 how to monitor storage assets, storage subsystems and fabrics 273 how to monitor storage subsystem performance 274 learn how to manage element managers and external tools 275 learn how to manage servers and agents 272 show managed devices 273 tasks 272 configuring Brocade switches 84 Cisco switches 85 CNT switches 87 Data agent for upgrade 311 Data server for Windows domain 320 DB2 JDBC driver 329 for IBM System Storage N Series Gateway servers 377 for RDBMS logon 285 how long information is saved 427 inactive zonesets for fabric data source 316 Java Web Start 323 McDATA switches 86 QLogic switches 86, 87 Storage Resource agent for upgrade 311 custom installation 198

### D

Data agents configuring for upgrade 311 increasing memory allocation 474 installing locally 246 installing remotely 253 installing using custom installation 206

Data agents (continued) installing using typical installation 244 planning for 61 planning for Solaris 61 protocol support 33 registering with a different server 449 uninstalling 392 uninstalling locally 390 uninstalling remotely 391, 392 uninstalling using GUI 389, 447 Data Manager agent..config file 293 databases that can be monitored 28 Data Path Explorer view 53 Data server increasing memory 472 increasing memory on AIX 472 increasing memory on Linux 473 increasing memory on UNIX 473 increasing memory on Windows 473 installing using local database 219 installing using remote database 231 Data Server changing DB2 password 476 checking status 471 preparing for using remote database 231 database connection alerts 271 database migration tool 112, 346 database repository accessing views 619 planning to retrieve information from DB2 views 114, 115 software requirements 11 views overview 617 database schema installing 217 upgrading 112, 346 databases histories, specifying how long to keep 313 specifying how long to keep information 313 that Data Manager can monitor 28 troubleshooting 529 DB2 command line 400 db2cc command 400 Health Center 116 health monitor 116 installing on AIX 126 installing on Linux 124 installing on UNIX 124 installing on Windows 122 migrating repository database 349 migrating repository database on AIX 355 migrating repository database on Linux 357 migrating repository database on Windows 350 monitoring 401 preparing to install on UNIX 122 preparing to install on Windows 121 troubleshooting 529

DB2 (continued) uninstalling 395 upgrading 349 user names and passwords 607 verifying installation 129 verifying installation using CLP 129, 289 verifying installation using First Steps 129 DB2 database for registry 412 DB2 password changing for Agent Manager 477 changing for Agent Manager on UNIX 479 changing for Data server 476 changing for Device server 475 DB2 publications xiv Device server changing DB2 password 475 changing host authentication password 481 changing WebSphere password 476 checking status 471 configuration 314, 317 increasing memory 474 installing using local database 219 installing using remote database 231 preparing for using remote database 231 setting timeout values 318 Disk Manager user rights required 22 DNS server for Agent Manager 412 domain account how to grant local administrative privileges 321, 489 DS3000 list of publications xi DS4000 list of publications xi DS5000 list of publications xi DS6000 list of publications xii DS8000 how to manage DS8000 element managers 275 planning for performance 69 duplicate registration 424

### E

editing configuration files 293 element manager XIV troubleshooting 588 EMC PowerPath Multipathing 31 EncryptAMProps command 482 encryption 498, 610 EncryptPW command 484

### F

Fabric agents changing host authentication password 481 Fabric agents (continued) increasing memory allocation 474 installing locally 246 installing remotely 253, 259 installing using typical installation 244 removing data 453 uninstalling 392 uninstalling locally 390 uninstalling remotely 391 fabric management planning for 75 Fabric Manager configure zones 615 directors 82 planning for 73 planning for configuration 81 planning for HBAs 83 switches 82 user rights required 22 file systems supported 29 fully qualified host name checking for on AIX 487 checking for on Linux 488 checking for on Solaris 488 checking for on Windows 487 fully-qualified host names host names fully-qualified host names required 110 required 110, 120

## G

GetAMInfo 420 glossary 645 GUI installing 239 installing Tivoli Integrated Portal 172 starting from Tivoli Integrated Portal 467 stand-alone 468 GUI8347E error message 523

### Η

HACMP planning for 94 HACMP cluster upgrading agents 97 HACMP support 97 hardware requirements 2 for Agent Manager 54 IBM Tivoli Storage Productivity Center for Replication 2 Tivoli Storage Productivity Center GUI 4 HBAs planning for Fabric Manager 83 Health Center for DB2 116 health monitor for DB2 116 HealthCheck command 605 checking version of Agent Manager 132 HealthCheck.bat command 605

HealthCheck.sh command 605 heap size changing for Agent Manager 428 HiCommand for Hitachi Data Systems 595 History Aggregator, configuring 295 Hitachi Data Systems troubleshooting 595 host authentication password changing for Fabric agents 481 changing for the Device server 481

### 

IBM 2005 switches 615 IBM 2109 switches 615 IBM System Storage N Series Gateway servers configuring 377 planning for 102 IBM Tivoli Storage Productivity Center hardware requirements 2 installing 165 installing overview 119 log files 501 migrating 111, 345 silent installation 625 software requirements 5 uninstalling 383 uninstalling the agents 389 upgrading 111, 345 IBM Tivoli Storage Productivity Center family hardware requirements 2 IBM Tivoli Storage Productivity Center for Replication browser support 14 installing 165 installing overview 119 installing Two Site or Three Site BC license 197 installing using custom installation 216 installing using typical installation 182, 195 migrating 111, 345, 348 planning for 1 software requirements 5 uninstalling 383 upgrading 111, 345 iKeyman utility 482 installation files setup\_agents.iss 620 uninstall.iss 625 installing Agent Manager 132 Agent Manager using 32-bit DB2 instance, console install 143 Agent Manager using 64-bit DB2 instance 149, 158 Agent Manager, using 32-bit DB2 instance 132 agents 241, 246 agents on Virtual I/O Server 259 agents remotely 253 CLI 239

installing (continued) Data agent using custom installation 206 Data agents using typical installation 244 database schema 217 DB2 on AIX 126 DB2 on Linux 124 DB2 on UNIX 124 DB2 on Windows 122 DB2, preparing for installation on UNIX 122 DB2, preparing for installation on Windows 121 Device server using local database 219 Fabric agents remotely 259 Fabric agents using typical installation 244 GUI 239 TIP 110, 184 IBM Tivoli Storage Productivity Center for Replication using custom installation 216 IBM Tivoli Storage Productivity Center for Replication using typical installation 182, 195 Language Pack 263 new installation 110 overview 119 preparing for 165 starting installation 168 Storage Resource agents 295 Storage Resource agents locally 242 Storage Resource agents remotely 167 TIP installing 110 Tivoli Integrated Portal using typical installation 176, 190 Two Site or Three Site Business Continuity license 197 using customized installation all components 198 using typical mode 171 using typical mode with Agent Manager registration 184 using typical mode without Agent Manager registration 172 InstallShield limitations 113, 121, 347 interop namesapces 608 IPv6 configuring AIX for IPv6 130 DB2 on AIX for IPv6 130 DB2 on Linux for IPv6 131 configuring DB2 on Linux 131 configuring for AIX 130 configuring for DB2 on AIX 130 limitations 37 planning for 34

### J

Java Web Start configuring 323 JDBC driver configuring 329 jobs, overview 268

### Κ

key management utility 482

Language Pack installing 263 uninstalling 263, 393 launch in context starting from Tivoli Integrated Portal 467 LDAP planning for 41 LDAP servers software requirements 14 LDAP user authentication configuring in Tivoli Integrated Portal 403 license adding 240 log files Agent Manager 503, 504 Agent Manager-specific WebSphere 504 Agent Managerpackaging for support 419 for IBM Tivoli Storage Productivity Center 501 installation 503 run-time for Agent Manager 504 setting retention period 288 uninstallation 504 LogCollector command 605 LogCollector.bat command 605 LogCollector.sh command 605

### Μ

McDATA Intrepid 10000 removing data 453 McDATA switches configuring 86 memory increasing allocation for Data server on AIX 472 increasing allocation for Data server on Linux 473 increasing allocation for Data server on Windows 473 memory allocation Data server 472 increasing allocation for Device server 474 migrating IBM Tivoli Storage Productivity Center for Replication 348 overview 111, 345 Tivoli Storage Productivity Center 111, 345 TotalStorage Productivity Center 3.x 347

monitoring databases 28 file systems 29 HACMP clustered nodes and cluster resource groups 97 MSCS clustered nodes and cluster resource groups 92 networked file systems 29 volume managers 30 MSCS support 91, 92

### Ν

namespaces, interop 608 NAS support of 98 NAS configuration file, editing 294 nas.config file, editing 294 NetApp configuration 100 identifying in user interface 102 limitations 101 planning for 100 removing a device 101 NetWare configuring for 290 logging into NDS tree 311 support of 98 Network Attached Storage configuring for 290 networked file systems supported 29 Novell Directory Services logging into 311

## 0

operating system user authentication configuring in Tivoli Integrated Portal 409 operating systems supported 5 orphan zones 615

### Ρ

packages 15 partitiontables.bat file 112, 346 partitiontables.sh file 112, 346 passwords changing 475 changing agent registration 481 changing DB2 password for Agent Manager 477 changing DB2 password for Agent Manager on UNIX 479 changing DB2 password for Data server 476 changing DB2 password for Device server 475 changing encryption key for Agent Manager 484 changing for resource managers 483 changing host authentication password for Fabric agents 481 changing host authentication password for the Device server 481 passwords (continued) changing using password tool 485 changing WebSphere password for the Device server 476 encrypting for Agent Manager 484 valid characters 607 work sheet 23, 637 Path Planner 49 performance configuration 89 planning for DS8000 69 performance metrics 88 planning 18 for an MSCS environment 92 for CIM agents 64 for Configuration Analysis 48 for Configuration History tool 49 for Data agents 61 for Data Path Explorer view 53 for IBM System Storage N Series Gateway servers 102 for MSCS support 91 for NAS system support 98 for NetWare system support 98 for retrieving information from DB2 views 114, 115 for rollup reports 46 for rollup reports configuration 47 for SAN configuration tools 47 for Solaris Data agents 61 for TagmaStore CIM agents 66 for tape library support 27 for Tivoli Storage Productivity Center for Replication 1 for universal agents 109 for user IDs and user rights for installing 22 for VMware configuration 105 for VMware support 103 for volume manager support 30 for XIV Storage System 71 IPv6 support 34, 37 NetApp support 100 overview 1 storage subsystem support 26 switches 27 Virtual I/O Server support 106 ports changing port 80 416 configuring Agent Manager to use different port numbers 415 port conflicts with Agent Manager 535 used by Agent Manager 59 PROBE\_ME file 449

### Q

QLogic switches configuring 86, 87

### R

RDBMS logon 285

recovery Tivoli Storage Productivity Center for Replication 463 registering the Data agent with a different server 449 registration reregistering 424 registry configuring retention period 427 estimating size of for Agent Manager 56 overview 412 removing agents from 424 repocopy command 490 exporting data 491 importing data 492 reports configuring for batch reports on Linux 331 configuring for batch reports on UNIX 331 configuring for data aggregation 295 specifying how long to keep information 313 VMware capacity 106 Repository Copy tool 490 exporting data 491 importing data 492 resource histories setting retention periods 311 resource managers 412 changing registration password 483 changing registration properties 424 controlling access to 56 resources specifying how long to keep 312 rollup reports planning for 46 planning for configuration 47 run-time log files 504 run-time log files for Agent Manager 504 location 503

### S

SAN configuration tools planning 47 SAN Volume Controller publications xiii scheduler.config 499, 611 Secure Socket Layer (SSL) disabling 408 enabling 406 security duplicate agent registration 424 for Agent Manager 56 server.config 498, 610 Service Location Protocol using to discover CIM agents 432 Service tool for agents 494 for servers 494 services Device server displaying information 474

services (continued) Device server (continued) viewing log 475 starting 465 stopping 464 setup\_agents.iss 620 silent installation for IBM Tivoli Storage Productivity Center 620, 625 single sign-on planning for 42 user authentication method used with 42 SMI-S planning for fabric management 75 **SNMP** sending traps 287 software requirements database repository 11 for Agent Manager 55 for LDAP servers 14 operating systems 5 SSH protocol creating a certificate 302 SSL certificates how to import for VMware 490 replacing a certificate 307 starting from Tivoli Integrated Portal Tivoli Storage Productivity Center 467 stand-alone Tivoli Storage Productivity Center 468 starting services 465 Tivoli Integrated Portal server 466 stopping services 464 storage capacity of volumes 73 Storage Optimizer planning for 51 troubleshooting 585, 586 Storage Resource agents changing authentication 442 configuring for upgrade 311 creating certificates for 302 Data agents general information 628 deploying 295 general information 628 importing authentication information 336 installing 295 installing locally 242 migrating to Data agent 374 planning for 32 preparing for 167 protocol support 33 replacing SSL certificates 307 uninstalling manually 390 uninstalling using GUI 389, 447 upgrading manually 369 storage subsystem supported 26 subsystem device drivers planning for 30 support collect data about Virtual I/O Servers 108

support (continued) in an HACMP environment 97 switches configuring 314 configuring Brocade 84 configuring Cisco 85 configuring CNT 87 configuring McDATA 86 configuring QLogic 86, 87 planning for 82 supported 27 using private networks 84 SYSMAINT authority checking and setting 401 system maintenance authority checking and setting 401

### T

tape library support 27 TCP/IP ports planning for 19, 21, 633, 635 used by Agent Manager 59 used by IBM Tivoli Storage Productivity Center for Replication 21, 636 TEC events sending 287 timeout values setting for Device server 318 TIP installing 184 Tivoli Common Agent Services Agent Manager 412 software requirements 13 Tivoli Integrated Portal installing using customized installation 210 installing using typical installation 176, 190 starting 467 starting server 466 troubleshooting 590 Tivoli Storage Productivity Center configuration files 497 disabling 341 silent installation 620 uninstalling 383 upgrading 111, 345 Tivoli Storage Productivity Center for Replication backing up 463 disabling 341 how to access through Tivoli Storage Productivity Center 276 recovering 463 server, accessing 463 troubleshooting 528 uninstalling with InstallShield 387 Tivoli Storage Productivity Center servers overview 453 toolkit for Agent Manager 605 tools repository copy 490 TotalStorage Productivity Center migrating 347

TPCD.config 500, 612 trademarks 643 translations browser locale requirement xv troubleshooting 497 database 529 DB2 529 Tivoli Integrated Portal 590 Tivoli Storage Productivity Center for Replication 528 XIV 588 truststore file re-encrypting 482

# U

uninstall.iss 625 uninstalling Agent Manager 394 agents 392 agents from Virtual I/O Server 393 AIX 388 common agents 392 Data agent 389, 447 Data agents locally 390 Data agents remotely 392 DB2 395 Fabric agents locally 390 IBM Tivoli Storage Productivity Center 383, 389 IBM Tivoli Storage Productivity Center for Replication 383 Language Pack 263, 393 Linux 388 Storage Resource agent 389, 447 Storage Resource agent manually 390 Tivoli Storage Productivity Center 383 Tivoli Storage Productivity Center for Replication 388 on Windows 388 with InstallShield 387 universal agents planning for 109 upgrading Agent Manager 360 database schema 112, 346 overview 111, 345 Storage Resource agents manually 369 upgrading agents 447 user authentication configuring in Tivoli Integrated Portal LDAP 403 operating system 409 Secure Socket Layer (SSL) disabling 408 enabling 406 user group name adding to Tivoli Storage Productivity Center for Replication 462 user IDs planning for 22 valid characters 607 work sheet 23, 637 user interface installing Tivoli Integrated Portal 172 user interface *(continued)* installing Tivoli Integrated Portal using custom installation 210 starting using Tivoli Integrated Portal 466, 467 user rights required for Disk Manager 22 required for Fabric Manager 22 required for installing 22 required for WebSphere 22

### V

views overview 617 planning to retrieve information 114, retrieving information 617, 619 Virtual I/O Server collecting data 108 installing agents on 259 listing agents 461 planning for 106 uninstalling agents from 393 VMware capacity reports 106 VMware data source viewing and managing 458 VMware support 103 configuration 105 how to import SSL certificates 490 volume managers supported 30 Volume Planner 49

### W

WebSphere user rights required 22 WebSphere password changing for the Device server 476 Windows domain configuring Data server for 320 work sheets 23, 637

### X

XIV collecting CIM agent logs for 436 troubleshooting 588 XIV Information xiv XIV Storage System planning for 71

# Ζ

zone configure 615 orphan 615 Zone Planner 49 zone set delete while contains zones 615 zonesets configuring for inactive zonesets 316
## 

Program Number: 5608-WB1, 5608-WC0, 5608-WC3, 5608-WC4 5608-WB2, 5608-WB3

Printed in USA

SC27-2337-00

