IBM Spectrum Control Version 5.3.7

Installation Guide



SC27-8767-07

Note:

Before using this information and the product it supports, read the information in <u>"Legal notices" on</u> page 223.

This edition applies to version 5, release 3, modification 7 of IBM Spectrum Control (product numbers 5725-F93, 5725-G33, 5725-Y23, and 5725-Y24) and to all subsequent releases and modifications until otherwise indicated in new editions.

This edition replaces SC27-8767-06.

[©] Copyright International Business Machines Corporation 2001, 2020.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this guide	vii
Who should read this guide	vii
Publications	vii
Accessing publications online	vii
IBM Redbooks	ix
Translation	ix
Providing feedback about publications	ix
IBM Spectrum Control technical community	ix
Contacting IBM Software Support	x
Reporting a problem	x
Conventions used in this guide	x
Chapter 1. Planning	1
Planning for installation	1
Product licenses	
Planning to install IBM Spectrum Control in a Windows domain	8
Required user privileges in installation scenarios	12
Planning for configuration	
Planning for capacity	
Planning for IBM Spectrum Control authentication and authorization	
User names and passwords	
Ports used by IBM Spectrum Control	
Planning for multipath subsystem device drivers	
Planning for Storage Resource agents	
Planning for Internet Protocol Version 6	
Planning to use LDAP	35
Planning for storage management	
Sudo command privileges	
Chapter 2. Installing	37
IBM Spectrum Control components	37
Hardware requirements	37
Software requirements	
Software requirements for operating systems	38
Software requirements for Storage Resource agents	38
Software requirements for the database repository	38
Web browser support	38
Software requirements for LDAP servers	
Software requirements for CIM agents	
Installing IBM Spectrum Control	39
Installation checklists for IBM Spectrum Control	40
Db2	43
Starting the installation programs	51
Installing IBM Spectrum Control in a single-server environment	54
Installing IBM Spectrum Control in a multiple-server environment	62
Accessing IBM Spectrum Control server from a remote computer using Command Line	
Interface	69
Installing IBM Spectrum Control on a Windows domain	71
Verifying the connection to the domain controller computer by using the Dcdiag tool	73

Installing IBM Spectrum Control and associated products using minimal space on the	
Windows C: drive	74
Verifying the installation	75
Reviewing the log files to resolve installation issues	77
Changing languages	77
Adding an installation license	79
Installing Storage Resource agents	81
Installing IBM Cognos Analyti	84
Installing Cognos Analytics in a single Windows environment	85
Installing Cognos Analytics in a single Linux environment	85
Installing Cognos Analytics in a single AIX environment	87
Configuring IBM Cognos Analytics	88
Copying JDBC files for Db2 on Windows	88
Copying Db2 files and linking the Db2 library on Linux and AIX	89
Creating a content store and starting Cognos Analytics on Windows	89
Creating a content store and starting Cognos Analytics on Linux or AIX	90
Creating Cognos Analytics data source for the IBM Spectrum Control database	91
Importing IBM Spectrum Control pre-defined reports package	96
Configuring access to the Cognos Analytics reporting tool	97
Reinstalling the software if a failure occurs	98
Taking the first steps after installation	99
Chapter 3. Upgrading and migrating	101
Preparing for an upgrade	.101
Backups	. 105
Backing up a replication environment	. 106
Example of upgrading Db2	.106
Migrating reports to IBM Cognos Analytics during upgrade	.108
Migrating Cognos BI reports to IBM Cognos Analytics in a single windows environment	.110
Migrating Cognos BI reports to IBM Cognos Analytics in a multiple-server windows	440
environment with a remote database	. 118
Migrating Cognos BI reports to IBM Cognos Analytics in a multiple server windows	100
environment with remote Jazz for Service Management	. 125
Migrating Cognos BI reports to IBM Cognos Analytics in a single Linux environment.	. 133
with a remote database	1 1 1
With a remote database	.141
with remote Jazz for Service Management	150
Miditating Cognes PI reports to IPM Cognes Applytics in a single AIX environment	150. 150
Migrating Cognos BI reports to IBM Cognos Analytics in a single AIX environment	.150
with a remote database	167
Migrating Cognos BI reports to IBM Cognos Analytics in a multiple server AIX environment	. 107
with remote Jazz for Service Management	175
Ungrading IBM Spectrum Control in a single-server environment	18/
Ungrading IBM Spectrum Control in a single-server Windows environment by using the	. 104
installation program	18/
Ungrading IBM Spectrum Control in a single-server AIX or Linux environment by using the	.104
installation program	185
Ungrading IBM Spectrum Control in a single-server environment by using silent mode	187
Editing the ungrade response file	188
Upgrading IBM Spectrum Control in a multiple-server environment	189
Upgrading from Tivoli Storage Productivity Center Version 5.2.0 and later with a remote	. 10 /
database by using the installation program.	.189
Upgrading from Tivoli Storage Productivity Center Version 5.2.0 and later with remote Jazz for	0 /
Service Management by using the installation program	
Upgrading IBM Spectrum Control with a remote database by using silent mode	.192
Upgrading Storage Resource agents	.195

	Starting agent upgrades	195
	Scheduling agent upgrades	196
	Upgrading Storage Resource agents by using a command	196
	Upgrading Windows Storage Resource agents from previous versions to 5.2.13 or later	197
U	lpgrading SMI-S providers for storage systems	197
	Upgrading CIM agents	198
Μ	ligrating alert definitions from Tivoli Storage Productivity Center 5.2.7	198
Μ	ligrating alert definitions to alert policies	201
Μ	ligrating groups	201
S	cenario: Changing from LDAP and Local OS authentication to only LDAP or Local OS	
	authentication after an upgrade	202
~		
Cna	pter 4. Uninstalling	205
U	Ininstalling IBM Spectrum Control in a single-server environment	205
U	Ininstalling IBM Spectrum Control in a multiple-server environment	206
U	Ininstalling IBM Spectrum Control by using silent mode	207
Μ	1anually uninstalling IBM Spectrum Control components on AIX or Linux	208
Μ	1anually uninstalling IBM Spectrum Control components on Windows	209
U	Ininstalling Storage Resource agents	210
	Uninstalling Storage Resource agents manually	210
	Deleting Storage Resource agent registry entries after a failed installation or uninstallation	211
	Removing servers	212
U	Ininstalling Db2	213
	Uninstalling Db2 on AIX or Linux	213
U	Ininstalling Tivoli Common Reporting and Jazz for Service Management	215
Cha	ntor E. Deference	217
	pter 5. Reference	
a	gent.sh command	217
a	gent.sh command	217
a; App	gent.sh command bendix A. Accessibility features for IBM Spectrum Control	217 219
a; App	gent.sh command	217 219
a; App Lega	gent.sh command pendix A. Accessibility features for IBM Spectrum Controlal notices.	217 219 223
a; App Lega P	gent.sh command pendix A. Accessibility features for IBM Spectrum Control al notices	217 219 223
a; App Lega P T	gent.sh command pendix A. Accessibility features for IBM Spectrum Control al notices rivacy policy considerations	217 219 223 224 225
a; App Lega P T Glos	gent.sh command pendix A. Accessibility features for IBM Spectrum Control al notices rivacy policy considerations rademarks	217 219 223 224 225 227
a; App Lega P T Glos	gent.sh command pendix A. Accessibility features for IBM Spectrum Control al notices rivacy policy considerations rademarks ssary.	217 219 223 224 225 227 227
App Lega P T Glos	gent.sh command pendix A. Accessibility features for IBM Spectrum Control al notices rivacy policy considerations rademarks	217 219 223 224 225 227 227
App Lega P T Glos	gent.sh command pendix A. Accessibility features for IBM Spectrum Control al notices rivacy policy considerations rademarks	217 219 223 224 225 227 227 228
App Lega P T Glos B C	gent.sh command pendix A. Accessibility features for IBM Spectrum Control al notices rivacy policy considerations rademarks	217 219 223 224 225 227 227 228 228 228
App Lega P T Glos C D	gent.sh command pendix A. Accessibility features for IBM Spectrum Control al notices rivacy policy considerations rademarks	217 219 223 224 225 227 227 228 228 230
App Lega P T Glos A B C D	gent.sh command pendix A. Accessibility features for IBM Spectrum Control al notices rivacy policy considerations rademarks	217 219 223 224 225 227 227 228 228 230 231
App Lega P T Glos C D E F	gent.sh command pendix A. Accessibility features for IBM Spectrum Control al notices rivacy policy considerations rademarks	217 219 223 224 225 227 227 228 228 230 231 232
App Lega P T Glos C D E G	gent.sh command	217 219 223 224 225 227 227 227 228 228 230 231 232 234
App Legi P T Glos C D E F G H	gent.sh command	217 219 223 224 225 227 227 228 228 228 230 231 232 234 234
App Legi P T Glos C D E F G H I.	gent.sh command	217 219 223 224 225 227 227 228 227 228 227 228 230 231 232 234 234 235
App Legi P T Glos C D E F G H I. J	gent.sh command	217 219 223 224 225 227 227 227 227 228 228 230 231 234 234 234 235 236
App Legi P T Glos C D E F G H I. J K	gent.sh command	217 219 223 224 225 225 227 227 228 228 230 231 232 234 234 235 236 236
App Legi P T Glos C D E G H I. J K	gent.sh command	217 219 223 224 225 227 227 227 228 228 228 230 231 231 234 234 234 236 236 236 236
App Legi P T Glos C D E G H I. J K L M	gent.sh command	217 219 223 224 225 227 227 228 228 228 230 231 231 234 234 234 234 236 236 236 236 236
App Legi PT Glos CDEF GH I.J KL N	gent.sh command	217 219 223 224 225 227 227 228 228 230 231 231 234 235 236 236 236 236 236 236 236 237
App Legi PT Glos ABCDEF GHIJKLMNO	gent.sh command	217 219 223 224 225 227 227 228 228 230 231 231 232 234 235 236 236 236 236 236 237 237 237
App Legi PT Glos BCDEF GHIJKLM NOP	gent.sh command	217 219 223 224 225 227 227 227 227 228 230 230 231 234 234 236 236 236 236 237 237 237 237 237 238
App Legi P T Glos B C D E F G H I.J.K L N O P D	gent.sh command	217 219 223 224 225 227 227 227 228 226 230 230 231 232 234 236 236 236 236 237 237 237 238 238 238 237 237 238 238 237
App Legi P T Glos B C D E F G H I.J.K L M N O P R S	gent.sh command	217 219 223 224 225 227 227 227 227 228 228 230 230 231 232 234 236 236 236 236 237 237 238 239 239 239
App Legi P T Glos A B C D E F G H I.J.K L M N O P R S T	gent.sh command	217 219 223 224 225 227 227 227 227 228 227 228 230 230 231 234 234 236 236 236 236 236 236 236 237 238 237 238 237 238 237 236 236 236 236 236 237 236 236 236 236 236 237 236 236 236 236 237 236 236 237 236 237 236 236 237 236 236
App Legi PT Glos ABCDEFGHI.J.KLMNOPRST	gent.sh command	217 219 223 224 225 227 227 227 228 228 228 230 231 232 234 234 236 236 236 236 236 236 236 236 237 238 239 239 239 240 243
App Legi PT Glos ABCDEFGHIJKLMNOPRSTU	gent.sh command	217 219 223 224 225 227 227 227 227 228 230 231 231 232 234 234 236 236 236 236 237 237 237 237 237 237 237 237 237 237 237 237 237 237 237 236 236 236 236 237 237 236 236 236 236 237 237 236 236 236 237 236 236 237 236 237 236 236 237 237 236 236 236 237 237 236 236 236 237 237 236 236 236 236 237 237 236 236 236 236 236 236 237 237 237 237 237 236 236 236 237
App Legi PT Glos ABCDEFGHIJKLMNOPRSTUV	gent.sh command	217 219 223 224 225 227 227 227 227 227 228 230 230 231 232 234 234 236 236 236 236 236 236 237 237 237 237 237 237 238 236 236 236 236 236 236 236 237 237 237 237 236 236 236 236 236 236 236 237 237 236 236 236 236 237 237 237 236 236 236 236 236 237 237 237 236 236 236 236 236 237 237 237 236 236 236 236 236 236 236 237 237 237 237 236 236 236 236 236 237

Ζ	
Index	

About this guide

IBM Spectrum Control manages storage infrastructure by centralizing, automating, and simplifying the management of complex and heterogeneous storage environments. Use this guide to complete the steps that are required to install these products, including planning for installation and configuration.

Who should read this guide

This publication is intended for administrators or users who are installing IBM Spectrum Control. It also describes the hardware and software requirements for installing the product 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 Windows, AIX®, Linux®, HP-UX, and Oracle Solaris.
- Storage area network (SAN) concepts
- IBM Spectrum Control concepts
- IBM[®] Db2[®] Database concepts
- Simple Network Management Protocol (SNMP) concepts
- IBM® Tivoli® Enterprise Console concepts

Publications

A number of publications are provided with IBM Spectrum Control.

IBM Tivoli Storage Productivity Center for Replication is no longer installed with IBM Spectrum Control. For current Tivoli Storage Productivity Center for Replication users who upgrade to IBM Spectrum Control,

Tivoli Storage Productivity Center for Replication will get uninstalled. See 🖻 https://ibm.co/2ut9z0n.

The following section describes how to access these publications online.

Accessing publications online

Information about installing, configuring, using, upgrading, and uninstalling IBM Spectrum Control and related products is available online.

Use Table 1 on page vii to view and download these publications. Translated documents are available for some products.

Table 1. Locations of publications for IBM Spectrum Control and related products		
Product	Online location	
IBM Cognos [®] Analytics	https://www.ibm.com/support/knowledgecenter/SSEP7J	
IBM Copy Services Manager	http://www.ibm.com/support/knowledgecenter/SSESK4	
IBM [®] Db2 [®] Database	https://www.ibm.com/support/knowledgecenter/SSEPGG	
IBM FlashSystem [®] 5000, IBM FlashSystem 5100, and IBM Storwize [®] V5000E	https://www.ibm.com/support/knowledgecenter/STHGUJ	
IBM FlashSystem 7200 and IBM Storwize V7000	https://www.ibm.com/support/knowledgecenter/ST3FR7	

_

Table 1. Locations of publications for IBM Spectrum Control and related products (continued)			
Product	Online location		
IBM FlashSystem V840 Enterprise Performance Solution	http://www.ibm.com/support/knowledgecenter/ST2HTZ/		
IBM FlashSystem 840 and IBM FlashSystem 900	http://www.ibm.com/support/knowledgecenter/STKMQB_1.6.1		
IBM FlashSystem 9200 and IBM FlashSystem 9100	http://www.ibm.com/support/knowledgecenter/STSLR9/		
IBM FlashSystem V9000	http://www.ibm.com/support/knowledgecenter/STKMQV		
IBM FlashSystem A9000	http://www.ibm.com/support/knowledgecenter/STJKMM		
IBM FlashSystem A9000R	http://www.ibm.com/support/knowledgecenter/STJKN5		
IBM Spectrum Accelerate	http://www.ibm.com/support/knowledgecenter/STZSWD/ welcome		
IBM Spectrum Control	http://www.ibm.com/support/knowledgecenter/SS5R93		
IBM Spectrum Virtualize as Software Only	https://www.ibm.com/support/knowledgecenter/STVLF4/		
IBM Spectrum Virtualize for Public Cloud	https://www.ibm.com/support/knowledgecenter/STHLEK/		
IBM Spectrum Scale (General Parallel File System)	https://www.ibm.com/support/knowledgecenter/SSFKCN/ gpfs_welcome.html		
IBM Storwize V3500	https://www.ibm.com/support/knowledgecenter/STLM6B		
IBM Storwize V3700	https://www.ibm.com/support/knowledgecenter/STLM5A		
IBM Storwize V5000, IBM Storwize V5100, and IBM Storwize V5000E	https://www.ibm.com/support/knowledgecenter/STHGUJ		
IBM Storwize V7000	https://www.ibm.com/support/knowledgecenter/ST3FR7		
IBM Storwize V7000 Unified	https://www.ibm.com/support/knowledgecenter/ST5Q4U		
IBM System Storage [®] DS3500	http://www.ibm.com/support/pages/node/655429		
IBM System Storage DS3700	http://www.ibm.com/support/pages/node/655889		
IBM System Storage DS6000™	http://www.redbooks.ibm.com/abstracts/sg246781.html		
	The DS6000 series is no longer supported. For information, see the preceding publication.		
IBM System Storage DS8000®	http://www.ibm.com/support/knowledgecenter/		
	Go to the preceding website and search for the DS8000 series system that you want.		
IBM System Storage DS [®] Open Application Programming Interface publications	http://www.ibm.com/support/knowledgecenter/HW213_7.3.0/ com.ibm.storage.ssic.help.doc/f2c_dsopenapi_1v2fvp.html Use these publications for information about how to install,		
	configure, and use the CIM agent.		
IBM System Storage N series	http://www.ibm.com/support/knowledgecenter/nseries/ kc_welcome_nseries.html		
IBM SAN Volume Controller	http://www.ibm.com/support/knowledgecenter/STPVGU		

Table 1. Locations of publications for IBM Spectrum Control and related products (continued)		
Product	Online location	
IBM XIV [®] Storage System	http://www.ibm.com/support/knowledgecenter/STJTAG	
IBM WebSphere [®] Application Server	https://www.ibm.com/support/knowledgecenter/SSEQTP/ mapfiles/product_welcome_was.html	
IBM WebSphere Application Server Liberty	https://www.ibm.com/support/knowledgecenter/ SSEQTP_liberty/as_ditamaps/was900_welcome_liberty.html	
Jazz® for Service Management	http://www.ibm.com/support/knowledgecenter/SSEKCU	

IBM Redbooks

The IBM Redbooks® are publications about 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.

Languages

Non-English publications are available from IBM Knowledge Center, which is available in certain non-English languages. It is displayed in the language that is appropriate for the browser locale setting.

When a locale does not have a non-English version, the information is displayed in English, which is the default language. Non-English PDFs are available when the information is translated.

Providing feedback about publications

Your feedback is important to help IBM provide the highest quality information.

To provide comments or suggestions about the product documentation, go to the IBM Knowledge Center

for IBM Spectrum Control: ^{http://www.ibm.com/support/knowledgecenter/SS5R93. Click **Feedback** at the bottom of any page and complete the form.}

IBM Spectrum Control technical community

Connect, learn, and share with storage professionals: product support technical experts who provide their perspectives and expertise.

Access the IBM Spectrum Control technical community at <u>https://www.ibm.com/developerworks/</u> servicemanagement/.

Use IBM Spectrum Control technical community in the following ways:

- Become involved with transparent development, an ongoing, open engagement between other users and developers of IBM products.
- Connect one-on-one with the experts to collaborate and network about IBM and the Storage Management community.
- Read blogs to benefit from the expertise and experience of others.
- Use forums to collaborate with the broader user community.

Contacting IBM Software Support

You can contact IBM Software Support by phone, and you can register for support notifications at the technical support website.

• Go to the IBM Spectrum Control technical support website at http://www.ibm.com/support/entry/ portal/product/tivoli/ibm_spectrum_control/ibm_spectrum_control_standard_edition.

To receive future support notifications, sign in under **Subscribe to support notifications**. You are required to enter your IBM ID and password. After you are authenticated, you can configure your subscription for IBM Spectrum Control technical support website updates.

- Customers in the United States can call 1-800-IBM-SERV (1-800-426-7378).
- For international customers, go to https://www.ibm.com/planetwide/.

You can also review the *IBM Software Support Handbook*, which is available at <u>http://</u>www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html.

The support website 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 IBM Software Support, 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 website. See <u>"Reporting a problem" on page x.</u>

Reporting a problem

Provide IBM Software Support with information about the problems that you report.

Have the following information ready when you report a problem:

- The IBM Spectrum Control 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

Information is given about the conventions that are used in this publication.

This publication uses several conventions for special terms and actions, and for operating systemdependent commands and paths.

The following typeface conventions are used in this publication:

Bold

- · Flags that display with text
- Graphical user interface (GUI) elements (except for titles of windows and dialogs)
- Names of keys

Italic

- Variables
- · Values that you must provide
- New terms

- Words and phrases that are emphasized
- Titles of documents

monospace

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

For syntax notations, remember the following details.

- In AIX, the prompt for the root user is #.
- In AIX and Linux, the commands are case-sensitive, so you must type commands exactly as they are shown.

Chapter 1. Planning

The following sections provide information to help plan your IBM Spectrum Control 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.

Planning for installation

You can install IBM Spectrum Control by using the installation program or the command line in silent mode. Installing IBM Spectrum Control by using console mode is not supported. Also, upgrading the operating system of a server where IBM Spectrum Control is installed is not supported. If you must upgrade the server, contact the IBM Support team for IBM Spectrum Control Support to discuss your options.

Antivirus software considerations

Installing IBM Spectrum Control involves making use of your operating system in manners typical for installing new application software. If your antivirus software is set on the maximum mode, it might prevent some of your changes from being accepted.

To verify that your installation completes correctly, enable your antivirus software product to allow the following instances:

- The /etc/hosts file can be edited
- Files can be created in the /temp directory
- New executable files can be created in the C:\Program Files directory

Recommended skills and knowledge

Administrators and users of IBM Spectrum Control should be familiar with the following skills and topics:

- General procedures for installing software on Microsoft Windows, IBM AIX, and Linux operating systems
- Storage Area Network (SAN) concepts
- IBM Spectrum Control concepts
- IBM Db2 Database
- Simple Network Management Protocol (SNMP) concepts

Required user privileges for installation

Ensure that you have the required privileges to install Db2 and IBM Spectrum Control. If you are installing on a Windows operating system, you must install as a user with administrator privileges. If you are installing on an AIX or Linux operating system, you must install as a root user or as a non-root user who has sudo privileges.

Fully qualified host names

Some systems might be configured to return a short host name such as server22, instead of a fully qualified host name such as server22.myorg.mycompany.com. IBM Spectrum Control requires fully qualified host names, so you must install the product on a computer that has a fully qualified host name.

For more information about determining whether you have a fully qualified domain name, see <u>http://</u>www.ibm.com/support/knowledgecenter/SS5R93_5.3.7/com.ibm.spectrum.sc.doc/ fqz0_t_checking_fully_qualified_host_name.html.

Hardware and software requirements

The IBM Spectrum Control server can require a large amount of memory, disk space, network bandwidth, and processor resources. To promote consistent availability and performance, install IBM Spectrum Control on a dedicated server where no other critical business applications, including IBM Copy Services Manager, are installed. IBM Software Support is not responsible for availability, performance, and functional problems that are caused by other business applications that are deployed on the same server as IBM Spectrum Control.

For information about hardware requirements, see "Hardware requirements " on page 37.

For information about software requirements, see Software requirements.

For information about updates to product and operating system support, see Find the Supported

Hardware, Products and Platforms Interoperability Matrix Links at ^{http://www.ibm.com/support/docview.wss?uid=swg21386446.}

Installation methods

You can install Db2 and IBM Spectrum Control by using the GUI or silent mode. In silent mode, a command is provided with the values in a response file.

Use the silent-mode installation to install on a server that cannot display graphics. For example, if you are installing on an AIX or Linux server that does not have the X Window System installed.

On a server that does not have the X Window System installed, you cannot change the Db2 and IBM Spectrum Control passwords within IBM Spectrum Control by using the change password tool. For

information on how to change the passwords, see <a href="http://www.ibm.com/support/knowledgecenter/supports.com/support/knowledgecenter/supports.com/supports.co

Installation images

Compressed installation images are available electronically. Download and extract these images to a location with adequate disk space. For disk space requirements by operating system, see *IBM Spectrum*

Control 5.2.x - Hardware Support: Memory, Processor and Disk Space at Emission IBM Spectrum Control 5.3.x - Hardware Support: Memory, Processor and Disk Space.

Download the installation images for each product into a separate directory. The following list provides sample download directory paths:

- c:\downloads\DB2
- c:\downloads\SC

Extract the image files into a separate temporary directory for each product. For example:

- c:\temp\DB2
- c:\temp\SC



Attention: If you do not extract the files into separate directories for each product, the common paths or path structures might overwrite each other, and you cannot install the products.

Follow these rules for naming the directories:

- Do not include spaces in the directory name.
- Keep the directory name short.
- For Linux or AIX operating systems, do not include a period (.) at the end of the directory name.

During the extraction of multi-part images, if you are prompted to merge or replace folders or files with the same name, click **Merge/Replace**.

Installation files for the following components are provided with IBM Spectrum Control:

Db2

- Db2 for Windows (64-bit)
- Db2 for Linux (64-bit)
- Db2 for AIX (64-bit)

IBM Spectrum Control

- IBM Spectrum Control for AIX
- IBM Spectrum Control for Linux
- IBM Spectrum Control for Windows

In addition, installation files for the following optional agents are available with IBM Spectrum Control:

- IBM Spectrum Control Storage Resource agent for Windows
- IBM Spectrum Control Storage Resource agent for UNIX
- IBM Spectrum Control Monitoring Agent for IBM Tivoli Monitoring on Windows
- IBM Spectrum Control Monitoring Agent for IBM Tivoli Monitoring on UNIX

On Windows operating systems, assign the appropriate security settings for the Db2 and IBM Spectrum Control compressed files by completing the following steps:

- 1. Right-click one of the compressed installation files.
- 2. Examine the General tab and determine whether the Unblock button is displayed.
- 3. If the **Unblock** button is displayed:
 - a. Right-click the compressed file and click **Properties**.
 - b. On the **General** tab, next to **Security**, click **Unblock**.
- 4. Verify that the compressed installation files no longer have the **Unblock** button displayed.

IBM Spectrum Control GUI

After IBM Spectrum Control is installed, use the GUI to complete your storage management tasks. The GUI runs in a web browser and includes the ability to monitor, manage, and troubleshoot storage resources. You can access this interface from anywhere that you have a web browser and connectivity to a network. You can also use the IBM Cognos Analytics reporting tool to generate, save, and view reports about the condition, capacity, and performance resources.

Installation language

When you install IBM Spectrum Control, you must select one of the following languages:

- English
- Czech
- French
- German
- Hungarian
- Italian
- Japanese
- Korean
- Polish
- Brazilian Portuguese
- Russian
- Spanish

- Chinese (Simplified)
- Chinese (Traditional)

For more information about changing the operating system for the user interface, see <u>"Changing</u> languages" on page 77.

Messages, online help, and text are displayed in the language that you select. You are not required to install a language pack after installation. When you use IBM Spectrum Control, the language that is displayed is the language setting of the operating system.

To install IBM Spectrum Control on a Windows domain, see <u>"Planning to install IBM Spectrum Control in a</u> <u>Windows domain" on page 8</u> and <u>"Installing IBM Spectrum Control on a Windows domain" on page</u> 71.

Installation images on AIX

When you extract installation images, use the GNU tape archive (tar) program instead of the AIX tape archive program. The AIX tape archive program might truncate long file names, which can cause installation errors in IBM Spectrum Control.

To get the GNU tape archive program, go to <a>http://www.ibm.com/systems/power/software/aix/linux/ toolbox/alpha.html#T. Find tar in the Package column, and click RPM to download the program. You must specify this program as the default tape archive program in the PATH environment variable.

For more information on using the correct program to extract the IBM Spectrum Control installation media, see How to install GNU tar on AIX operating system .

Product licenses

Multiple product licenses are available for IBM Spectrum Control. Each license determines the features that you can access from the IBM Spectrum Control GUI, command prompt, command-line interface, and the API.

Compare the features of these four offerings:

Table 2. Features of the IBM Spectrum Control licenses		
Feature	IBM Spectrum Control Standard Edition and IBM Spectrum Control Standard Select Edition	IBM Spectrum Control Advanced Edition and IBM Spectrum Control Advanced Select Edition
	Understanding the environment	
Support for a single dashboard view of the environment to manage storage systems, hypervisors, servers, and Fibre Channel fabrics.	~	*
Capacity monitoring of storage systems, pools, volumes, file systems, and file sets.	~	~
Performance monitoring of storage systems, Fibre Channel networks, applications, and departments.	~	*
Defining groups of resources that represent applications or departments.	~	~
Defining tiers of storage for planning and reporting.	~	~
Health and alerting		

Table 2. Features of the IBM Spectrum Control licenses (continued)			
Feature	IBM Spectrum Control Standard Edition and IBM Spectrum Control Standard Select Edition	IBM Spectrum Control Advanced Edition and IBM Spectrum Control Advanced Select Edition	
Show health status of hypervisors, networks, servers, and storage systems, and selected internal entities.	*	*	
Alerting on status changes and thresholds of capacity, performance and error metrics.	*	~	
	Reporting		
Web GUI reports: Reports that you can create from the information in the user-interface tables. You can configure, schedule, and save this information to your file systems. Or you can specify to send it to another user or person by mail.	*	*	
Web GUI reports: Capacity and inventory reports.	~	~	
Web GUI reports: Chargeback reports for showing the capacity and the cost of the storage that is used by applications, departments, hypervisors, and physical servers.		~	
Web GUI reports: Consumer reports for showing the capacity and the cost of the block storage that is used by an application, department, hypervisor, and physical server.		*	
Web GUI reports: Roll up reports in which capacity data is combined from multiple instances of IBM Spectrum Control for reporting purposes.		*	
External reports: Reports that use REST API and Cognos.	*	*	
Transforming			
For storage systems that run IBM Spectrum Virtualize, the transform storage feature moves volumes, and configures compression and the properties of the volumes.		~	
Analyzing			
Analytics-driven tiering to automatically move volumes to the most cost-effective tier.		~	

Table 2. Features of the IBM Spectrum Control licenses (continued)		
Feature	IBM Spectrum Control Standard Edition and IBM Spectrum Control Standard Select Edition	IBM Spectrum Control Advanced Edition and IBM Spectrum Control Advanced Select Edition
Analysis of storage-pool balancing to generate recommendations to help you optimize storage resources.		~
Storage reclamation that you can realize when the block storage systems in your data center are analyzed, and you determine and reclaim volumes that aren't used for storing data. You can replace the existing storage space instead of purchasing new storage media.		~
	Provisioning	
File provisioning for IBM Storwize V7000 Unified.	*	~
	Other	
Inclusion of the license for IBM Copy Services Manager to manage 2-site replication, 3-site replication, and advanced copy services. Learn more about how to download and install Copy Services Manager at http://www.ibm.com/support/ knowledgecenter/SSESK4.	~	~
Snapshot-based protection that is provided by IBM Spectrum Protect [™] Snapshot for the applications and databases that IBM Spectrum Control uses.		~

For more information about the product licenses, see the following topics in the IBM Spectrum Control IBM Knowledge Center, or see the *IBM Spectrum Control User's Guide*:

- Experimental Functions that are available based on role and license at http://www.ibm.com/support/ knowledgecenter/SS5R93_5.3.7/com.ibm.spectrum.sc.doc/fqz0_r_wg_functions_available.html
- License compliance at http://www.ibm.com/support/knowledgecenter/SS5R93_5.3.7/ com.ibm.spectrum.sc.doc/tpch_r_managed_capacity_breakdown.html

To view a complete list of devices that can be used with IBM Spectrum Control, go to <u>http://</u>www.ibm.com/support/docview.wss?uid=swg21386446.

IBM Storage Insights for IBM Spectrum Control: IBM Storage Insights for IBM Spectrum Control is an IBM Cloud service that can help you predict and prevent storage problems before they impact your business. It is complementary to IBM Spectrum Control and is available at no additional cost if you have an active license with a current subscription and support agreement for IBM Virtual Storage Center, IBM Spectrum Storage Suite, or any edition of IBM Spectrum Control.

For more information and to view a list of features in the service, see <u>IBM Storage Insights for IBM</u> Spectrum Control.

Definitions of licensing metrics

Use these steps to access definitions of licensing metrics for Storage Capacity Units (SCUs) and for the Select Edition storage device or enclosure metrics. Examples are provided.

Two different license metrics are available for IBM Spectrum Control:

SCUs

Licenses are priced by the number of SCUs that are needed to cover the total usable capacity that they manage. Total usable capacity is measured in tebibytes (2^40 bytes). This metric is available for IBM Spectrum Control Standard Edition, IBM Spectrum Control Advanced Edition, and IBM Virtual Storage Center.

Storage devices or enclosures

Licenses are priced by the number of slots and capacity in the storage enclosures that they manage. One license is required for every 25 slots or 500 TB (decimal), whichever is reached first. This metric is available for IBM Spectrum Control Standard Select Edition and IBM Spectrum Control Advanced Select Edition.

These examples illustrate how licensing is determined:

- Example 1: A storage system has 92 slots and 300 TB of storage. It requires four licenses:
 - <u>Calculation by slot:</u> 25 slots + 25 slots + 25 slots + 17 slots requires four licenses. This limit is reached first.
 - <u>Calculation by TB:</u> 300 TB requires one license.
- Example 2: A storage system has 25 slots and 600 TB. It requires two licenses.
 - Calculation by slot: 25 slots require one license.
 - Calculation by TB: 500 TB + 100 TB require two licenses. This limit is reached first.

To learn about the licensing of IBM Spectrum Control, click the Announcement in Table 3 on page 7. Information about licenses is available in the section *Charge Metrics*.

Table 3. Product announcements for IBM Spectrum Control licenses			
License	Announcement	Revised Announcement	
IBM Spectrum Control Standard Edition	5.3.0.0	5.3.6.0	
IBM Spectrum Control Standard Select Edition	5.3.0.0	5.3.7.0	
IBM Spectrum Control Advanced Edition	<u>5.3.0.0</u>	5.3.6.0	
IBM Spectrum Control Advanced Select Edition	5.3.0.0	<u>5.3.7.0</u>	

Names of equivalent licenses in previous releases

The IBM Spectrum Control licenses were known by different names in previous releases. Use this table to determine the names.

Table 4. IBM Spectrum Control licenses and their previous names			
Name of IBM Spectrum Control license	Name of Tivoli Storage Productivity Center Version 5.1 license	Name of Tivoli Storage Productivity Center Version 5.2.1 through 5.2.7 license	
IBM Spectrum Control Standard Edition	Tivoli Storage Productivity Center	Tivoli Storage Productivity Center	
IBM Spectrum Control Standard Select Edition	Tivoli Storage Productivity Center Select	Tivoli Storage Productivity Center Select	

Table 4. IBM Spectrum Control licenses and their previous names (continued)			
Name of Tivoli Storage Name of IBM Spectrum Control license Name of Tivoli Storage Productivity Center Version 5.1 license		Name of Tivoli Storage Productivity Center Version 5.2.1 through 5.2.7 license	
IBM Spectrum Control Advanced Edition	Tivoli Storage Productivity Center Advanced or IBM SmartCloud® Virtual Storage Center	IBM SmartCloud Virtual Storage Center Storage Analytics Engine	
IBM Spectrum Control Advanced Select Edition	Tivoli Storage Productivity Center Advanced or IBM SmartCloud Virtual Storage Center	IBM SmartCloud Virtual Storage Center Storage Analytics Engine	

Planning to install IBM Spectrum Control in a Windows domain

Before you can install IBM Spectrum Control on a Windows domain, you must determine which installation method is appropriate, based on your environment.

Installation methods

Install Db2 and IBM Spectrum Control in one of the following ways:

- Use local user accounts to install both Db2 and IBM Spectrum Control.
- Use a local user account to install Db2 and a domain user account to install IBM Spectrum Control.
- Use domain user accounts to install both Db2 and IBM Spectrum Control.

Windows domain and local user accounts

When a computer is a member of a Windows domain, you can install IBM Db2 on the local computer or on a computer that is a member of a Windows domain. The installation process creates a local Db2 user account or a domain Db2 user account.

User accounts

Windows domain user accounts are used to manage multiple computers, and local user accounts can be used to manage one computer.

Restriction: Before you install IBM Spectrum Control by using a Windows domain or a local user account as the common user name, you must add the Windows domain user account or local user account to the local administrators group. The IBM Spectrum Control installation software recognizes only Windows domain or local user accounts (and not Windows domain or local groups) that are added to the local administrators group.

domain Db2 user account is an example of a Windows domain user account, and *local Db2 user account* is an example of a local user account.

Naming conventions for user accounts

You can install IBM Spectrum Control by using the same user account that is defined in both the local and Windows domain registries. The Windows operating system resolves this naming collision on computers that belong to a Windows domain by prefixing the user name with the host name or domain name. This user name is also called a *fully qualified user name*.

You must use the following naming conventions for each user account:

- domain_name\administrator
- domain_name\user 1, domain_name\user2, domain_name\userN.
- host_name\administrator
- host_name\user1, host_name\user2, host_name\userN.

For example, if the domain name is TPC51, and the user name is db2admin, the Windows domain user account is TPC51\db2admin. The naming convention for a local user account is *host_name*\user name.

For example, if the host name is machine2, and the user name is db2admin, the user account is machine2\db2admin. You must enter the fully qualified user names in the common user name field when you install IBM Spectrum Control on computers that are members of a Windows domain.

Installation considerations

As part of your planning process, you must determine which user accounts to use when you install IBM Spectrum Control and Db2, consider the environment and security requirements.

IBM Spectrum Control uses WebSphere Application Server Liberty to authenticate the users for local and domain user accounts. When the computer that hosts the WebSphere Application Server Liberty process is a member of a Windows domain, by default local and domain user registries are used, but the Windows domain user registry takes precedence.

Related reference

<u>"Adding a computer to the Windows domain" on page 9</u> Before you can install IBM Spectrum Control in a Windows domain, you must first add the computer on which you plan to install IBM Spectrum Control to the domain.

"Installing Db2 by using a Windows domain user account" on page 10 Before you install IBM Spectrum Control in a Windows domain, you must install Db2 and register the Db2 license key.

"Creating a Windows domain common user account for IBM Spectrum Control" on page 11 You must create a Windows domain common user account before you can install IBM Spectrum Control in a Windows domain.

"Granting Db2 SYSADM authority to a Windows domain user account" on page 12 If a Windows domain user account is used to install IBM Spectrum Control, the user account may not have the Db2 SYSADM authority, because Db2 goes to the domain controller computer to list the groups. Before you install IBM Spectrum Control, you must grant the Windows domain user accounts the Db2 SYSADM authority.

"Installing IBM Spectrum Control on a Windows domain" on page 71 You can install IBM Spectrum Control and Db2 by using a Windows domain or a local user account.

Adding a computer to the Windows domain

Before you can install IBM Spectrum Control in a Windows domain, you must first add the computer on which you plan to install IBM Spectrum Control to the domain.

You can log on to a computer that is a member of a Windows domain by entering a user name that is prefixed with the domain name. For example, you can enter TPC52\Administrator if you are the domain administrator of the TPC52 domain.

To add a computer to a Windows domain, complete the following steps:

- 1. Click Start > Control Panel > Network and Internet > Network and Sharing Center.
- 2. On the **Network and Sharing Center** window, click the left mouse button on your local area connection and click **Properties**.
- 3. Select the Internet Protocol Version 4 (TPC/IP4) check box, and click Properties.

Tip: If you are using Windows Server 2012, ensure that the **Client for Microsoft Networks** check box is selected.

- 4. On the General tab, select Use the following DNS server addresses.
- 5. In the **Preferred DNS server** field, enter the IP address of the domain controller computer.
- 6. In the **Alternate DNS server** field, enter the IP address of the alternate DNS server.
- 7. Click Advanced.
- 8. On the **DNS** tab, review the list of IP addresses.
- 9. In **DNS suffix for this connection** field, enter the fully qualified domain name.
- 10. Click **OK**.

- 11. Right-click **Computer** and select **Properties**.
- 12. In the Computer name, domain, and workgroup settings section, click **Change settings**.
- 13. Click Change.
- 14. On the Computer Name/Domain Changes window, select **Domain**, enter the fully qualified domain name, and click **OK**.
- 15. Enter the user name and password for the domain controller computer.

Important: The user name and password that you enter must be a domain administrator user name and password.

16. Click **OK** for the changes to take effect and to start the computer again.

Verifying that the Netlogon service is running

IBM Spectrum Control uses WebSphere Application Server Liberty to authenticate domain users. WebSphere Application Server Liberty requires that the Microsoft Netlogon service is enabled and running to authenticate these users.

To verify that the **Netlogon** service is running on the domain controller computer and the computer that is a member of a domain, complete the following steps:

- 1. Right-click **Computer** and select **Manage**.
- 2. In the navigation tree view, click **Server Manager** > **Configuration** > **Services**.
- 3. Verify that the **Netlogon** service is started.

If the service has a **Stopped/Disabled** status on the domain controller computer, you must also restart the computer that is a member of a Windows domain after you start the service on the domain controller computer.

Installing Db2 by using a Windows domain user account

Before you install IBM Spectrum Control in a Windows domain, you must install Db2 and register the Db2 license key.

The following table shows the privileges that are required for users associated with installing and running Db2 in a Windows domain environment:

Table 5. User privileges related to Db2 in a Windows domain environment			
User role	Required privileges		
Installing Db2 on the target Windows domain member machine such that the Db2 instance owner (typically db2admin) is a domain user and the Db2 groups (typically DB2ADMNS and DB2USERS) are domain groups	Local Administrator and Domain Administrator The Db2 installation needs to access and update the Db2 user and group information in the Active Directory that is running on the Windows Domain Controller machine.		
Db2 instance owner (typically db2admin) that runs Db2 after Db2 is installed	Local Administrator		

Tip: It is recommended that you manually create the Db2 user (the user who will own the Db2 instance that gets created when Db2 is installed, typically *db2admin*), and the Db2 groups (typically *DB2ADMNS* and *DB2USERS*) in the Active Directory on the Domain Controller before you install Db2 on the Windows domain member machine. The Db2 user *must* be a member of both Db2 groups in the Active Directory and a member of the local Administrators group on the Windows domain member machine.

To install Db2 by using a Windows domain user account, complete the following steps:

- 1. Log on to Windows as a user that has the correct privileges.
- 2. In Windows Explorer, go to the directory where Db2 installation image is located.
- 3. Right-click setup.exe and select **Run as administrator**.
- 4. Complete the DB2 Setup program.

- 5. On the Set user information for the DB2 Administration Server page, in the User Information panel, select your domain.
- 6. Enter the name of the Db2 user (the user who will own the Db2 instance, typically *db2admin*) that you manually created in the Active Directory on the Domain Controller then enter and confirm the corresponding password.
- 7. On the Enable operating system security for DB2 objects page, complete the following steps:
 - a. Verify that Enable operating system security check box is selected.
 - b. In the DB2 administrators group and DB2 users group sections, select your domain and then enter the names of the Db2 groups that you manually created in the Active Directory on the Domain Controller.
 - c. Click **OK** in the dialog warning you that these groups already exist.

Creating a Windows domain common user account for IBM Spectrum Control

You must create a Windows domain common user account before you can install IBM Spectrum Control in a Windows domain.

To create a domain common user account for IBM Spectrum Control, complete the following steps:

- 1. Log on to the domain controller computer by using a domain administrator user account.
- 2. Click Start > Administrative Tools > Active Directory Users and Computers.
- 3. Right-click on the Users folder and select **New** > **User**.
- 4. On the domain controller computer, click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Users and Computers**.
- 5. Right-click on the domain user you created and click **Properties > Member Of**.
- 6. On the Member of tab, click **Add** and add DB2ADMNS.
- 7. Click Check Names.
- 8. If the name you entered is located, click **OK**.
- 9. Repeat steps 4 8 and add the DB2USERS group.

Tip: The Domain Users group exists.

- 10. Follow the prompts to create the domain common user account for IBM Spectrum Control.
- 11. Log on to the domain client computer on which you want to install IBM Spectrum Control by using a domain administrator user account.

When you log in to computer that is a member of a Windows domain by using the domain administrator user account, and you encounter the 'DB2 UDB SQL5005C System Error' message, complete the following steps:

- a. Log in to the computer that is a member of a domain by using the local user name.
- b. Click Server Manager > Configuration > Local Users and Groups > Groups > DB2ADMNS > Properties > Add.
- c. Add domain\domain user name.
- d. Click Check Names.
- e. If the user name that you checked for is underlined, click **Apply**.
- 12. Open Server Manager.
- 13. In the navigation tree, click **Server Manager** > **Configuration** > **Local Users and Groups** > **Groups**.
- 14. Add the domain common user name that you created in step 3 (commonid) to the local administrator group.

Restriction: When you install IBM Spectrum Control by using a Windows domain user account, the *sAMAccountName* and *userPrincipalName* (the User login name) Active Directory attributes in the Windows domain user account cannot contain spaces. The *sAMAccountName* must have the same value as the part of the *userPrincipalName* Active Directory attribute that precedes the @ character.

Granting Db2 SYSADM authority to a Windows domain user account

If a Windows domain user account is used to install IBM Spectrum Control, the user account may not have the Db2 SYSADM authority, because Db2 goes to the domain controller computer to list the groups. Before you install IBM Spectrum Control, you must grant the Windows domain user accounts the Db2 SYSADM authority.

To enter the commands, and Db2 SYSADM authority, complete the following steps:

- 1. Click Start > Command Prompt.
- 2. Right-click Command Prompt and select Run as administrator.
- 3. Enter these commands:

```
db2cmd
db2set -g DB2_GRP_LOOKUP=local,TOKENLOCAL
db2 force application all
db2stop
db2start
db2set -all
```

After you run the commands, you can log in to IBM Spectrum Control by using a user account that has Db2 SYSADM authority.

If you are logged in by using your Windows domain user account, you may not have the authorization to run the db2 force application all command.

Important: When you grant Db2 SYSADM authority, and the **db2 force application all** command does not work, you can enter the **db2stop** command instead of the **db2 force application all** command.

For more information about acquiring user group information in the Windows operating system, see <u>Using</u> an access token to acquire users' group information (Windows).

For more information about the **sysadmin_group** parameter, see <u>System administration authority</u> (SYSADM) .

Related reference

"Installing IBM Spectrum Control on a Windows domain" on page 71 You can install IBM Spectrum Control and Db2 by using a Windows domain or a local user account.

Required user privileges in installation scenarios

When you are planning to install IBM Spectrum Control, there are users to consider for the installation.

These are the users to consider:

Application administrator

The user who logs in to the operating system and does the installation of IBM Spectrum Control.

Common user

The user that you set during the installation of IBM Spectrum Control. The user name that is used to run IBM Spectrum Control.

Db2[®] user

The user that you set during the installation of IBM Spectrum Control. The user name that is used to install and operate the database repository for IBM Spectrum Control.

There are user privileges that are required in various IBM Spectrum Control installation scenarios.

Important: The required user privileges for Common User and Db2 user *cannot* be changed or removed after you complete the installation of IBM Spectrum Control. You can change the required user privileges for the Application administrator after that user completes the installation of IBM Spectrum Control, but only if the Application administrator is *not* set as the Common User or Db2 user in IBM Spectrum Control.

The following table shows the required user privileges in IBM Spectrum Control installation scenarios:

Table 6. Required user privileges for an IBM Spectrum Control installation		
Installation scenario	Required privilege	
Setting <i>only</i> the Common User, single-server installation, <i>not</i> in a Windows domain environment	Application administrator: Windows operating system: You must be an Administrator and must have the <i>Debug programs</i> privilege and must <i>not</i> have the <i>Deny access to this</i> <i>computer from the network</i> privilege in the Windows operating system security policy. These privileges can be found in Administrative Tools ->	
	Local Security Policy -> Local Policies -> User Rights Assignment	
	Linux operating system: You must be a root user or a non-root user with sudo privileges.	
	AIX operating system: You must be a root user or a non-root user with sudo privileges.	
	Common user:	
	Windows operating system: A member of the local Administrators group, a member of the local DB2 groups (typically DB2ADMNS and DB2USERS).	
	Linux operating system: A member of the root group, a member of the DB2 group (typically db2iadm1).	
	AIX [®] operating system: member of the system group, member of the DB2 group (typically db2iadm1).	

Table 6. Required user privileges for an IBM Spectrum Control installation (continued)			
Installation scenario	Required privilege		
Setting the Common User and Db2 user, single- server installation, <i>not</i> a Windows domain environment	Application administrator:		
	Windows operating system: You must be an Administrator and must have the <i>Debug programs</i> privilege and must <i>not</i> have the <i>Deny access to this</i> <i>computer from the network</i> privilege in the Windows operating system security policy. These privileges can be found in Administrative Tools -> Local Security Policy -> Local Policies -> User Rights Assignment		
	Linux operating system: You must be a root user or a non-root user with sudo privileges.		
	AIX operating system: You must be a root user or a non-root user with sudo privileges.		
	Common User:		
	Windows operating system: A member of the local Administrators group.		
	Linux operating system: A member of the root group.		
	AIX operating system: A member of the system group.		
	Db2 user:		
	Windows operating system: A member of the local DB2 groups (typically DB2ADMNS and DB2USERS).		
	Linux operating system: A member of the DB2 group (typically db2iadm1).		
	AIX operating system: A member of the DB2 group (typically db2iadm1).		
Setting <i>only</i> the Common User, single-server	Application administrator:		
with Db2 installed so the Db2 instance owner (typically db2admin) is a domain user and the Db2 groups (typically DB2ADMNS and DB2USERS) are domain groups.	You must be an Administrator and must have the Debug programs privilege and must not have the Deny access to this computer from the network privilege in the Windows operating system security policy. These privileges can be found in Administrative Tools -> Local Security Policy -> Local Policies -> User Rights Assignment		
	Common user:		
	A member of the local Administrators group, a member of the domain DB2 groups (typically DB2ADMNS and DB2USERS; these groups are stored in the domain Active Directory).		

Table 6. Required user privileges for an IBM Spectrum Control installation (continued)			
Installation scenario	Required privilege		
Setting the Common User and Db2 user, single-	Application administrator:		
environment with Db2 installed so the Db2 instance owner (typically db2admin) is a domain user and the Db2 groups (typically DB2ADMNS and DB2USERS) are domain groups.	You must be an Administrator and must have the Debug programs privilege and must not have the Deny access to this computer from the network privilege in the Windows operating system security policy. These privileges can be found in Administrative Tools -> Local Security Policy -> Local Policies -> User Rights Assignment		
	Common User: A member of the local Administrators group.		
	Db2 user: A member of the domain DB2 groups (typically DB2ADMNS and DB2USERS; these groups are stored in the domain Active Directory).		
Setting <i>only</i> the Db2 user, multiple server	Application administrator:		
Installation (Database repository), <i>not</i> in a Windows domain environment.	Windows operating system:		
	You must be an Administrator and must have the Debug programs privilege and must not have the Deny access to this computer from the network privilege in the Windows operating system security policy. These privileges can be found in Administrative Tools -> Local Security Policy -> Local Policies -> User Rights Assignment		
	Linux operating system: Must be a root user or a non-root user with sudo privileges.		
	AIX operating system: Must be a root user or a non-root user with sudo privileges		
	Db2 user:		
	Windows operating system: A member of the local DB2 groups (typically DB2ADMNS and DB2USERS).		
	Linux operating system: A member of the DB2 group (typically db2iadm1).		
	AIX operating system: A member of the DB2 group (typically db2iadm1).		

Table 6. Required user privileges for an IBM Spectrum Control installation (continued)			
Installation scenario	Required privilege		
Setting <i>only</i> the Common User, multiple server	Application administrator:		
a Windows domain environment.	Windows operating system:		
	You must be an Administrator and must have the Debug programs privilege and must not have the Deny access to this computer from the network privilege in the Windows operating system security policy. These privileges can be found in Administrative Tools -> Local Security Policy -> Local Policies -> User Rights Assignment		
	Linux operating system: Must be a root user or a non-root user with sudo privileges.		
	AIX operating system: Must be a root user or a non-root user with sudo privileges.		
	Common user:		
	Windows operating system: A member of the local Administrators group.		
	Linux operating system: A member of the root group.		
	AIX operating system: A member of the system group.		
Setting <i>only</i> the Db2 user, multiple server	Application administrator:		
domain environment with Db2 installed so the Db2 instance owner (typically db2admin) is a domain user and the Db2 groups (typically DB2ADMNS and DB2USERS) are domain groups.	You must be an Administrator and must have the Debug programs privilege and must not have the Deny access to this computer from the network privilege in the Windows operating system security policy. These privileges can be found in Administrative Tools -> Local Security Policy -> Local Policies -> User Rights Assignment		
	Db2 user:		
	A member of the domain DB2 groups (typically DB2ADMNS and DB2USERS; these groups are stored in the domain Active Directory).		
Setting <i>only</i> the Common User, multiple server	Application administrator:		
Windows domain environment.	You must be an Administrator and must have the Debug programs privilege and must not have the Deny access to this computer from the network privilege in the Windows operating system security policy. These privileges can be found in Administrative Tools -> Local Security Policy -> Local Policies -> User Rights Assignment		
	Common user:		
	A member of the local Administrators group.		

Planning for configuration

Use this information to plan your IBM Spectrum Control environment. The information includes general configuration guidelines, TCP/IP ports, user names and user rights, and SMI-S support.

Planning for capacity

The following guidelines can help you determine the capacity for IBM Spectrum Control.

Consider the following guidelines when you determine your capacity requirements:

Database repository

For best performance, install the database repository across multiple physical disks, either through operating system striping or hardware RAID. You must have a minimum of three disks that are separate from the location of the IBM Spectrum Control host server's operating system and the directory of the IBM Spectrum Control product installation.

IBM Spectrum Control server

The IBM Spectrum Control server must meet the following requirements:

- The IBM Spectrum Control server must have dual 3.2 GHz processors with a minimum of 8 GB of random access memory (RAM).
- The IBM Spectrum Control server must be a dedicated computer for IBM Spectrum Control operations and not shared with other applications.
- Paging space: On AIX operating systems, the paging space must be at least half or, if possible, the same amount as the physical memory. You must periodically monitor paging space usage by running the lsps -s command and increasing the space if the percentage used is higher than 50%.

LSI SMI-S Provider

IBM Spectrum Control supports up to five storage systems with the LSI SMI-S Provider 1.3 or later.

Planning for IBM Spectrum Control authentication and authorization

An operating system user name is required to install and log on to IBM Spectrum Control for the first time. After you install IBM Spectrum Control, you can assign roles to users. Roles determine the product functions that are available to users.

User requirements for installing IBM Spectrum Control

The user name that you use when you run the IBM Spectrum Control installation program must belong to the following operating system groups. The user that you define as the common user during the IBM Spectrum Control installation must also belong to these groups. The IBM Spectrum Control installation program automatically maps these groups to the IBM Spectrum Control Administrator role.

Table 7. Operating system groups that are mapped to the Administrator role			
Operating System Group			
Windows	Administrators		
AIX system			
Linux root			

The user name that is used to install the database repository must belong to one of the following Db2 groups. The user name that is used to install the database repository depends on your installation configuration. For example, if you installed IBM Spectrum Control on a single server and you did not enter separate user information for Db2, the database repository is installed by using the common user name. Therefore, the common user must have these Db2 privileges.

Table 8. Db2 groups that are required to install the database repository		
Operating System Group		
Windows DB2ADMNS		
AIX and Linux db2iadm1		

The IBM Spectrum Control installation program establishes a default authentication configuration by using the federated repositories feature of the WebSphere Application Server Liberty.

If you want to change the user authentication configuration, see <a>http://www.ibm.com/support/knowledgecenter/SS5R93_5.3.7/com.ibm.spectrum.sc.doc/fqz0_c_change_user_auth_method.html.

For more information about installing IBM Spectrum Control on a Windows domain, see <u>"Planning to</u> install IBM Spectrum Control in a Windows domain" on page 8 and <u>"Installing IBM Spectrum Control on a</u> Windows domain" on page 71.

Defining roles for IBM Spectrum Control

After you install IBM Spectrum Control, you can assign roles for IBM Spectrum Control users. These roles are predefined in IBM Spectrum Control and are assigned at the group level. The role determines the authorization level for the users who are in the group. The authorization level determines the functions in IBM Spectrum Control that the user can access.

For example, if a user is in a group that is assigned to the Administrator role, the user has full access to all IBM Spectrum Control functions. However, if a user is in a group that is assigned to the Monitor role, the user has access to only a limited set of functions.

For more information about working with roles and groups, see 🖻 Role-based authorization.

User names and passwords

Several user names and passwords are required to install, configure, and use IBM Spectrum Control. There are also some requirements and limitations that you must understand before you install IBM Spectrum Control.

A worksheet is also provided to help you plan and document the user names and passwords that you use with IBM Spectrum Control. Keep the completed worksheet in a safe, secure place. Before you install IBM Spectrum Control, you must understand your local security policies and requirements. These policies can impose certain standards that you must consider when you create user names and passwords to comply with requirements.

Related reference

"User name and password requirements" on page 18

This information helps you create valid user names and passwords for IBM Spectrum Control and understand any special character restrictions.

"Db2 user names and passwords" on page 21

These are the rules for using Db2 user names and passwords.

"Worksheet for user names and passwords" on page 24

Use this worksheet to document the user names and passwords that you create when you install and administer IBM Spectrum Control. Space is provided for you to list more user names and passwords that you create when you configure more devices in IBM Spectrum Control.

User name and password requirements

This information helps you create valid user names and passwords for IBM Spectrum Control and understand any special character restrictions.

Table 1 lists the user names and passwords that are used with IBM Spectrum Control and specifies the following criteria:

• User names must be local or a Windows domain account or an LDAP account

Restriction: If you use LDAP, IBM Spectrum Control must be configured for LDAP authentication.

- Valid user name characters must comply with the minimum and maximum length requirements
- · Valid password characters must comply with the minimum and maximum length requirements

Restriction: If the IBM Spectrum Control common user name is the same as the IBM Spectrum Control Db2 user name (for example, if you did not use a custom Db2 user name to install IBM Spectrum Control), the corresponding password must be valid as a Db2 password and as a WebSphere Liberty password. For more information about valid Db2 and WebSphere Liberty passwords, see Table 9 on page 19. This restriction applies during a IBM Spectrum Control installation and when you use the IBM Spectrum Control change password tool.

For more information about setting passwords on the Windows operating system, see the see the Microsoft Windows Dev Center - Desktop website at http://msdn.microsoft.com/en-us/library/windows/ desktop/ms675092%28v=vs.85%29.aspx. Search for the SAM-Account-Name attribute.

Table 9. Valla characters for user names and passwords				
User name and password for	Windows domain OK?	LDAP OK?	Valid characters	
IBM Spectrum Control installation	Yes	No	Not applicable	
IBM Spectrum Control common user	<pre>Yes Restriction: You must follow these naming conventions: • Windows domain user name: domain_name \user_name format • Local user name: machine_name \username format</pre>	No	 A through Z (uppercase characters) a through z (lowercase characters) 0 through 9 (numeric characters) Special characters: '_' and '~' Restriction: The user name cannot contain spaces, \$ and ! signs, must have at least 1 character and must not start with a number or underscore. On Windows operating systems, the only valid special characters are `, ~, #, %, ^, (,), -, _, {, }, ', and . 	
IBM Spectrum Control common user passwords	Yes	Yes	 A through Z (uppercase characters) a through z (lowercase characters) 0 through 9 (numeric characters) Special characters: [,], ?, `, ~, ~, !, (,), -, _, *, %, +, and . Restriction: Passwords cannot contain spaces, must have at least 1 character and must not start with a number, dash character {-}, or underscore. 	

Table Q. Valid character fo .

Table 9. Valid characters for user names and passwords (continued)			
User name and password for	Windows domain OK?	LDAP OK?	Valid characters
Db2 administrator, Db2 user	<pre>Yes Restriction: You must follow these naming conventions: • Windows domain user name: domain_name \user_name format • Local user name: machine_name \username format</pre>	Yes	 A through Z (uppercase characters) a through z (lowercase characters) 0 through 9 (numeric characters) Special characters: ~, @, #, %, ^, -, (),_, { }". Restriction: User names and passwords cannot contain spaces and must have at least 1 character. User names also must not start with a number or underscore
Db2 passwords	Yes	Yes	 A through Z (uppercase characters) a through z (lowercase characters) 0 through 9 (numeric characters) Special characters: \$, ~, @, #, (,), -, _, {, }, [,], ?, *, %, +, and . Restriction: Passwords cannot contain spaces, must have at least 1 character and must not start with a number or underscore.
NAS Filer user name	No	No	 A through Z (uppercase characters) a through z (lowercase characters) 0 through 9 (numeric characters) Special characters: ` ~ # % ^ & () { }'. Restriction: User names and passwords cannot contain spaces and must have at least 1 character.

Table 9. Valid characters for user names and passwords (continued)			
User name and password for	Windows domain OK?	LDAP OK?	Valid characters
NAS Filer password	No	No	 A through Z (uppercase characters)
			 a through z (lowercase characters)
			 0 through 9 (numeric characters)
			<pre>• Special characters: ` ~ @ # % ^ & * () = + []{}\ ;:' ",. < >/?</pre>
			Restriction: User names and passwords cannot contain spaces and must have at least 1 character.

Password restrictions for monitored resources:

- Cisco switches: The password that IBM Spectrum Control uses to connect to a Cisco switch can't contain these special characters: < >.
- XIV storage systems: The password that IBM Spectrum Control uses to connect to an XIV storage system can't contain this special character: **&**.

Db2 user names and passwords

These are the rules for using Db2 user names and passwords.

Db2 user names and passwords must follow these rules:

- UNIX user names and passwords cannot be more than eight characters long. They cannot begin with a numeric digit or end with \$.
- 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.

Required user roles for monitoring resources

г

When you add storage systems, switches, and hypervisors for monitoring, you must provide a user name and password for logging in to those resources. The role or user group that is assigned to the user name determines the data collection and provisioning functions that you can use.

The following roles are associated with the user names that IBM Spectrum Control uses to log in to resources. Specify user names when you add a resource for monitoring. These roles are different from IBM Spectrum Control roles, which are assigned to users that log in to IBM Spectrum Control. For more

information about IBM Spectrum Control roles, see 🖙 Role-based authorization.

Any roles that are not listed, but include the privileges of the roles that are listed, can also be used for monitoring resources.

Table 10. Required roles for storage system, switch, and hypervisor users				
Resource	Required role for performance monitors	Required role for probes	Required role for provisioning	
DS6000	Monitor role or higher	Monitor role or higher	Administrator, Physical	
DS8000			operator, or Logical operator	
SAN Volume Controller	Administrator	Monitor	Administrator	
IBM Storwize family				
Storwize V7000 Unified (block storage)				
IBM FlashSystem devices that run IBM Spectrum Virtualize				
IBM Spectrum Virtualize for Public Cloud				
Storwize V7000 Unified (file storage)	Performance monitoring is not available	Monitor	Administrator, or Export Administrator + Storage Administrator.	
XIV	Monitor role or higher	Any role	Storage administrator	
IBM Spectrum Accelerate	Monitor role or higher	Any role	Provisioning is not available	
IBM FlashSystem A9000				
IBM FlashSystem A9000R				
IBM FlashSystem 840	Monitor role or higher	Monitor role or higher	Provisioning is not	
IBM FlashSystem 900			available	
IBM Spectrum Scale (file storage)	Any role	Root or non-root [*]	Provisioning is not available	

Table 10. Required roles for storage system, switch, and hypervisor users (continued)					
Resource	Required role for performance monitors	Required role for probes	Required role for provisioning		
IBM Spectrum Scale (object storage)	Performance monitoring is not available	The Keystone admin role. Information is collected only for the object storage accounts and containers that the user has access to. If you want to monitor all accounts and containers, the user must also be assigned the role that is defined in the reseller_admin_rol e configuration option in the Swift proxy server. The default value for the reseller_admin_rol e option is ResellerAdmin.	Provisioning is not available		
IBM Cloud Object Storage	Performance monitoring is not available	Operator, System Administrator, or Super User role	Provisioning is not available		
Dell EMC storage systems	Operator role or higher	Operator role or higher	Provisioning is not available		
Hitachi storage systems	Operator role or higher	Operator role or higher	Provisioning is not available		
NetApp storage systems	Operator role or higher	Operator role or higher	Provisioning is not available		
Pure storage systems	Role with read-only permission or higher	Role with read-only permission or higher	Provisioning is not available		
Cisco switches	Network-admin	Network-admin	Not applicable		
Brocade switches	Administrator user in Brocade Network Advisor (BNA)	Administrator user in BNA	Not applicable		
Hypervisors (such as ESX, ESXi, and vCenter Servers)	Performance monitoring is not available	A role that has permission to browse through data stores. For example: Administrator role or Virtual Machine Power [®] User role.	Any role		

Table 10. Required roles for storage system, switch, and hypervisor users (continued)					
Resource	Required role for performance monitors	Required role for probes	Required role for provisioning		
Rollup servers	Performance monitoring is not available	Administrator	Provisioning is not available		
Note: * You can add IBM Spectrum Scale and GSS systems as a non-root user, but that user must have privileges to run a set of specified administration commands using the sudo command on the cluster node. For more information, see Monitoring without requiring root privileges.					

Worksheet for user names and passwords

Use this worksheet to document the user names and passwords that you create when you install and administer IBM Spectrum Control. Space is provided for you to list more user names and passwords that you create when you configure more devices in IBM Spectrum Control.

Table 11. User names and passwords for a IBM Spectrum Control installation				
Item	Description	Your input		
IBM Spectrum Control and Db2 installation user				
Windows: local administrator				
• UNIX: root				
Db2 administrator user name and password	The Db2 administrator user name and password are created when you install Db2 and is required to install IBM Spectrum Control.			
	On the Windows operating system, this user name must be a member of the DB2ADMNS group and Administrators group. On UNIX, the user name must be the instance owner of the instance you want to use. This user name and password are created when you install Db2.			
LDAP bind user name	This user name has the authority to log in and connect to the LDAP server for authentication. It is not needed if the LDAP server allows anonymous bind. This user name and password must be provided to you by your LDAP administrator.			
Storage subsystem user name for access from IBM Spectrum Control	This user name is the user name that IBM Spectrum Control uses to log in to a storage device.			
CIMOM or SMI provider login name	This user name has log in access to the CIMOM or SMI provider software that interfaces with a storage device or a switch in a fabric.			
NAS filer user name and password	IBM Spectrum Control uses this user name to log in to a NAS device.			
Related reference

"User name and password requirements" on page 18

This information helps you create valid user names and passwords for IBM Spectrum Control and understand any special character restrictions.

Ports used by IBM Spectrum Control

When you install IBM Spectrum Control, the ports must be opened through the firewall. You must disable the firewall program or open the ports to allow incoming requests to the IBM Spectrum Control ports. Review these ports before you install IBM Spectrum Control.

IBM Spectrum Control ports used for TCP/IP

Table 1 lists the IBM Spectrum Control default ports.

All ports in Table 1 are configured during installation using the installation program. For a silent mode installation, use the **varTPCPortRangeSP** parameter in the installation response file.

Table 12. IBM Spectrum Control ports used by TCP/IP for incoming communication		
Ports	Component and port information	
9549	Data server 9549 listens for communications from the Device server, CLI, and Storage Resource agents.	
9550-9551 9553 9572	Device server 9550-9551 listens for communications from the Data server, Alert server, and Web server. 9553 listens for logging commands. 9572 listens for IBM WebSphere Application Server Liberty administrative commands.	
9556 9570 9571	Alert server 9556 listens for communications from the Device server. 9570 listens for logging commands. 9571 listens for WebSphere Application Server Liberty administrative commands.	

Table 12. IBM Spectrum Control ports used by TCP/IP for incoming communication (continued)		
Ports	Component and port information	
9510	Storage Resource agent	
9567	9510 listens for communications from the Data server if the Storage Resource agent is deployed in daemon mode. The only exception is the Storage Resource agent that is deployed on the IBM Spectrum Control server at installation time, which listens on port 9567 instead.	
	If the Storage Resource agent is deployed in non- daemon mode, the Storage Resource agent does not need any listening ports.	
	The Data server uses RXA to communicate with the Storage Resource agent in non-daemon mode. RXA uses the following default ports for the protocols:	
	SSH	
	512 Remote Execution (REXEC)	
	514 Remote Shell (rsh)	
	445 Windows SMB protocol	
	The Storage Resource agent sends responses back to the Data server on port 9549, in both daemon mode and non-daemon mode.	
9554	Web server	
9568 9569	9554 is used by WebSphere Application Server Liberty.	
	The following ports are used for the GUI:	
	• 9568 (non-secure)	
	• 9569 (secure)	
	9569 is used for the REST API.	
9562	Export server	
	9562 listens for communications from the Web server.	
50000	Db2	
	By default, Db2 listens on port 50000 for communication from IBM Spectrum Control and other clients. This default port can be changed only during the Db2 installation.	

Restrictions: The following restrictions apply to the ports that are listed in Table 12 on page 25:

• The ports apply only to a fresh installation of IBM Spectrum Control. If you upgrade from an earlier version of IBM Spectrum Control that used different ports, those ports are reused for your installation.

• The ports are used for incoming communication and are configured during installation. *Do not* change these ports after your installation is complete.

Table 13. List of IP ports that are used by IBM Spectrum Control		
Resource and ports	Port information	
Resources that run IBM Spectrum Virtualize	For native interface:	
	• 22 listens for SSH communication from IBM Spectrum Control.	
Ports: 22, 5989	• 5989 listens for other communication from IBM Spectrum Control. You can upload the SSH key once at setup time using the 5989 port.	
	By default, the IBM Spectrum Control Device server creates a connection between a IBM Spectrum Virtualize resource and a local port to listen for events from the IBM Spectrum Virtualize resource. The default range is 49152 to 65535. These ports are on the Device server only; you do not need to configure the firewall for them. The ports are used for a SSH tunnel to connect to the event port on the IBM Spectrum Virtualize resource. All communication to the IBM Spectrum Virtualize resource runs through the SSH connection. No other ports need to be open for IBM Spectrum Virtualize events.	
	To change to a custom port range, use the CLI setdscfg command to change the values of the following parameters:	
	• NAPI.SVCEventListenerLPortBase	
	• NAPI.SVCEventListenerLPortMax	
	After resetting the value, restart the Device server.	
	For example, to set the range from 50100 to 65000, run these commands from the <i>installation_dir/</i> cli/ subdirectory:	
	For Windows operating system:	
	<pre>tpctool.bat setdscfg -user <user name=""> -pwd <password></password></user></pre>	
	-property NAPI.SVCEventListenerLPortBase 50100	
	<pre>tpctool.bat setdscfg -user <user name=""> -pwd <password></password></user></pre>	
	-property NAPI.SVCEventListenerLPortMax 65000	
	For AIX and Linux operating systems:	
	./tpctool.sh setdscfg -user <user name=""> -pwd <password></password></user>	
	-property NAPI.SVCEventListenerLPortBase 50100	
	./tpctool.sh setdscfg -user <user name=""> -pwd <password></password></user>	
	-property NAPI.SVCEventListenerLPortMax 65000	

Table 13. List of IP ports that are used by IBM Spectrum Control (continued)		
Resource and ports	Port information	
FlashSystem 840	For native interface:	
FlashSystem 900	• 22 listens for SSH communication from IBM Spectrum Control.	
Ports: 22, 5989, 161 (UDP)	 5989 listens for other communication from IBM Spectrum Control. You can upload the SSH key once at setup time using the 5989 port. 	
	For SNMP:	
	 161 (UDP) listens for SNMP communications from IBM Spectrum Control for performance monitoring. 	
	 The SNMP agent must be enabled for a storage system before IBM Spectrum Control can collect its performance data. 	
DS8000	Native interface:	
Ports: 1751, 1750, 1755, 8451, 8452	1751 (default) listens for communication from IBM Spectrum Control and other clients. If 1751 is unavailable, uses 1750.	
	1751 (default) sends hardware management console (HMC) information and events to IBM Spectrum Control. If 1751 is unavailable, uses 1750.	
	1755 sends and receives data for HTC when logs are being offloaded.	
	8451, 8452 DS8000 listens on these ports for communication with the DS8000 GUI.	
 IBM XIV Storage System IBM Spectrum Accelerate FlashSystem A9000 FlashSystem A9000R Port: 7778 	7778 listens for communication from IBM Spectrum Control and other clients.	
IBM Spectrum Scale	• File storage:	
• File storage ports: 22, 9084	– 22 listens for SSH communication from IBM Spectrum Control.	
 Object storage ports: 5000, 8080, 35357 	 9084 listens for performance data collection on the IBM Spectrum Scale cluster node where the collector component is running. 	
	Important: Ensure that the queryinterface property is set to "0.0.0.0" in the /opt/IBM/zimon/ZIMonCollector.cfg file on the cluster node.	
	Object storage:	
	 5000, 8080, 35357 listen for data about any object storage or OpenStack Swift configurations on the IBM Spectrum Scale cluster node where the collector component is running. 	
IBM Cloud Object Storage Port: 443	443 listens for HTTPS communication from IBM Spectrum Control.	
Dell EMC Unity Port: 443	443 listens for communication from IBM Spectrum Control.	

Table 13. List of IP ports that are used by IBM Spectrum Control (continued)		
Resource and ports	Port information	
Other Dell EMC storage systems Port: 5991	5991 listens for events that are coming from Dell EMC CIMOMs .	
	To change this port, use the CLI setdscfg command and change the value for the Event.ListenerPort parameter. Then, restart the Device server.	
	For example, to set the port to 7200, run this command from the <i>installation_dir</i> /cli/ subdirectory:	
	For Windows operating system:	
	tpctool.bat setdscfg -user <user name=""> -pwd <password></password></user>	
	-property Event.ListenerPort 7200	
	For AIX and Linux operating systems:	
	./tpctool.sh setdscfg -user <user name=""> -pwd <password></password></user>	
	-property Event.ListenerPort 7200	
	You can also modify the protocol for listening to events that are coming from Dell EMC CIMOMs. By default, this protocol is set http.	
	To change this protocol, use the CLI setdscfg command and change the value for the Event.ListenerProtocol parameter. Then, restart the External Process component.	
	For example, to set the protocol to https, run this command from the <i>installation_dir</i> /cli/ subdirectory:	
	For Windows operating system:	
	tpctool.bat setdscfg -user <user name=""> -pwd <password></password></user>	
	-property Event.ListenerProtocol https	
	For AIX and Linux operating systems:	
	./tpctool.sh setdscfg -user <user name=""> -pwd <password></password></user>	
	-property Event.ListenerProtocol https	
Hitachi VSP storage systems Port: 2443	2443 listens for communication from IBM Spectrum Control.	
NetApp ONTAP 9 Port: 22	22 listens for communication from IBM Spectrum Control.	
Other NetApp storage systems Port: 80	80 listens for communication from IBM Spectrum Control using the NetApp Data ONTAP API (NAPI), if the storage system is a file storage system.	
	If the NetApp storage system is a block storage system, the CIM agent ports are used to listen for communication from the Device server.	

Table 13. List of IP ports that are used by IBM Spectrum Control (continued)		
Resource and ports	Port information	
Pure storage systems Port:	443 listens for communication from IBM Spectrum Control.	
SMI-S providers and CIM	5988 listens for non-secure communication from the Device server.	
agents for switches and	5989 listens for secure communication from the Device server.	
Ports: 5988, 5989, 5990	5990 IBM Spectrum Control listens on this port for events coming from CIM agents for managed storage systems.	
	To change the port that IBM Spectrum Control uses to listen for events coming from CIM agents for managed storage systems, use the CLI setdscfg command. Change the value for the Indication.PermanentListenerPort parameter then restart the Device server.	
	For example, to set the port to 7100, run this command from the <i>installation_dir</i> /cli/ subdirectory:	
	For Windows operating system:	
	tpctool.bat setdscfg -user <user name=""> -pwd <password></password></user>	
	-property Indication.PermanentListenerPort 7100	
	For AIX and Linux operating systems:	
	./tpctool.sh setdscfg -user <user name=""> -pwd <password></password></user>	
	-property Indication.PermanentListenerPort 7100	
IBM Spectrum Control Device server	162 (UDP) listens for SNMP traps coming from managed storage systems.	
Ports: 162 (UDP), 5960 (UDP),	5960 (UDP) listens for forwarded SNMP messages.	
49152 (UDP)	49152 (UDP) IBM Spectrum Control uses this port to forward SNMP traps.	
	To change these ports, use these steps:	
	 Log on to IBM Spectrum Control as a user with administrative privileges. 	
	2. Stop the Device server.	
	 Create a backup of the <i>installation_dir</i>/device/conf/ user.properties file. 	
	4. Change the parameter that corresponds to the port to an available port number and save the file.	
	162 SnmpTrapPort	
	5960 SnmpForwardedTrapListeningPort 49152	
	SnmpForwardingPort	
	5. Start the Device server.	

Table 13. List of IP ports that are used by IBM Spectrum Control (continued)

Resource and ports	Port information	
All monitored resources 7 (ECHO port)	Before you can discover resources, ensure that port 7 (ECHO port) is open on the resources, and Internet Control Message Protocol (ICMP) is available.	

Related information

setdscfg command Starting and stopping the IBM Spectrum Control servers

Planning for multipath subsystem device drivers

The subsystem device driver (SDD) is a software solution for multiple configuration environments in supported storage resources.

The subsystem device driver is installed on 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

For the most current support for multipath subsystem device drivers, go to ^[] <u>IBM Spectrum Control</u> 5.3.x - Platform Support: Agents, Servers and Browsers - Multipathing section.

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.
- 3. The SDD driver is no longer supported on HP, starting with HP-UX 11i v3 with Itanium[®].

For more information about multipath subsystem device drivers, see <u>https://www.ibm.com/support/</u>pages/node/651823.

For more information about how to install, configure, and use the subsystem device drivers, see <u>https://</u>www.ibm.com/support/pages/node/651689.

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 IBM Spectrum Control 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.

Dell EMC PowerPath Multipathing

Dell EMC PowerPath Multipathing supports a wide range of servers including cluster servers connected to Dell 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 Dell EMC PowerPath Multipathing, see http://www.dellemc.com. Search for **PowerPath**.

Planning for Storage Resource agents

Use Storage Resource agents to collect asset and configuration information about servers.

You can deploy Storage Resource agents from the IBM Spectrum Control GUI. You must have administrative privileges to deploy Storage Resource agents.

To deploy a Storage Resource agent from the GUI, go to **Servers** > **Servers**. Click **Add Server**, select **Deploy an agent for full server monitoring**, and select a method for adding a server. You can add a single server by manually entering server information or you can add multiple servers by importing configuration information from a file. If you add multiple servers, a time span is calculated during which the agents are deployed. The agents are deployed at regular intervals during the time span to avoid excessive load on the IBM Spectrum Control server.

For more information about deploying a Storage Resource agent, go to the product documentation at http://www.ibm.com/support/knowledgecenter/SS5R93_5.3.7/com.ibm.spectrum.sc.doc/ fqz0_r_native_agents_deployment_considerations.html.

Protocol support for Storage Resource agents

When installing the Storage Resource agent, IBM Spectrum Control uses specific protocols for connectivity between the server and agent.

When installing the Storage Resource agent, IBM Spectrum Control uses the following protocol for connectivity between the server and agent (listed in order):

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

At run time, the connectivity that is used between the server and agent depends on the type of service that 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 by 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 by using the secured socket connection. The server and agent have their respective certificates and no additional information is needed besides the certificates and the security that is provided by the SSH protocol.

Note: Running the Storage Resource agent in daemon mode requires only one socket connection to be open and thus simplifies any firewall rules that might be in place. However, the daemon mode always consumes resources (although a very small amount) when idle. In non-daemon mode, the Storage Resource agent only consumes resources when actively working for the IBM Spectrum Control server. Because the non-daemon mode uses the RXA protocol, additional firewall ports and security configuration are required.

The information required for these protocols is 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 by 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, go to the

documentation at http://www.ibm.com/support/knowledgecenter/SS5R93_5.3.7/ com.ibm.spectrum.sc.doc/fqz0_r_create_certificate_ssh.html. This information 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. The rhosts file 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 is deployed, a probe job is automatically run.

The agent that is 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/TSRM/ registryNA .

For more information about setting up the environment for deploying a Storage Resource agent, go to IBM Knowledge Center at http://www.ibm.com/support/knowledgecenter/SS5R93_5.3.7/ com.ibm.spectrum.sc.doc/fqz0_r_native_agents_deployment_considerations.html.

Planning for the Storage Resource agents on Oracle 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 globally affects all Solaris Storage Resource agents managed by the Data server.

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

- 1. Stop the Data server.
- 2. Modify the TPCD.config file in this directory:

TPC_Data_Server_install_directory/config

The default directory for Windows is:

C:\Program Files\IBM\TPC\data\config

The default directory for UNIX or Linux is:

/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 Storage Resource agent to skip AutoMounts
        process.By default, discovery will always
        process AutoMounts on the Solaris Storage Resource agent.
[gui]
   threadPoolSize=3
   maxThreads=10
   reportRowLimit=5000
   keepCachedReport=120</pre>
```

Save the file.

4. Restart the Data server.

Planning for Internet Protocol Version 6

IBM Spectrum Control 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 IBM Spectrum Control on systems that are enabled for IPv4, IPv6, or dual stack. *Dual stack* indicates that a system has both the IPv4 and IPv6 stacks enabled and both addresses configured.

You can use IPv6 addresses if one of the following conditions are met:

- The system where IBM Spectrum Control is installed is IPv6.
- Dual stack (IPv4 and IPv6) is enabled.

IBM Spectrum Control can communicate with the following external components over IPv6:

- SMI-S CIM agents
- SLP directory agents
- SNMP agents
- Storage resources
- SMTP server

Note: These external components must be IPv6 enabled to communicate with IBM Spectrum Control by using the IPv6 protocol.

Not all components and their related functions of IBM Spectrum Control are enabled for IPv6. Any functions that are not enabled for IPv6 are unavailable through the user interface when you install IBM Spectrum Control on an IPv6-only system.

If you have a system that is configured for dual stack networking, IBM Spectrum Control defaults to IPv4 addressing.

The following examples show an IPv6 address in the long form and in the short form:

Long form: 2001:DB8:0:0:0:0:0:0

Short form: 2001:DB8::

IPv6 and IBM Spectrum Control installation

If you are installing IBM Spectrum Control in an IPv6-only environment, the following requirements apply:

- For Windows operating systems, the IPv4 loopback interface is enabled.
- For AIX or Linux operating systems, the localhost option resolves to the IPv4 address 127.0.0.1, instead of the IPv6 address ::1. This value is specified in the /etc/hosts file.

For Windows operating systems, the localhost option is specified in the C:\Windows \system32\drivers\etc\hosts directory and file.

Table 14. IPv4 and IPv6 configurations in a multiple-servers environment		
If the database repository server is configured for	The IBM Spectrum Control server is configured for	
IPv4	IPv4	
IPv4	Dual stack	
Dual stack	IPv4	
Dual stack	Dual stack	
Dual stack	IPv6	
IPv6	IPv6	

Restriction: When you install the product on servers that are configured for IPv6 only, you cannot use IBM Tivoli Enterprise Console[®] events as triggered actions in alerts.

Planning to use LDAP for IBM Spectrum Control authentication

The Lightweight Directory Access Protocol (LDAP) is an application protocol that you can use to query and modify directory services running over TCP/IP. The IBM Spectrum Control installation program establishes a default authentication configuration using the federated repositories feature of the IBM WebSphere Application Server Liberty. You can configure IBM Spectrum Control for LDAP authentication as a post-installation activity.

A directory is a set of objects with similar attributes that are 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 tree entry (or multiple entries).

In the federated repositories framework, the IBM Spectrum Control installation program creates the following repositories:

File-based user repository

This repository contains the tpcFileRegistryUser user ID. This user password is the same as the common user password that you enter during the IBM Spectrum Control installation.

Operating system repository

This repository contains the users and groups managed by the local operating system.

With this default authentication configuration, you cannot use the IBM Spectrum Control single signon feature. Storage system element managers do not support the operating system repository or the file-based repository for single sign-on, even if the element manager is installed on the same system as IBM Spectrum Control.

To change the user authentication configuration, add or remove an LDAP repository in the federated repositories framework.

To authenticate user names on the IBM Spectrum Control by using an instance of Microsoft Active Directory, complete one of the following options:

Authenticate User names: Method one

- 1. Install IBM Spectrum Control on an AIX, Linux, or Windows operating system.
- 2. Configure IBM Spectrum Control for LDAP authentication.

The target LDAP repository is an instance of Active Directory running on Windows 2003 or later. This method provides the following benefits:

- The IBM Spectrum Control target system does not have to be a Windows system.
- The IBM Spectrum Control target system does not have to be a member of a Windows domain.

- There are fewer configuration steps for IBM Spectrum Control or Windows.
- The IBM Spectrum Control user names and group names do not have to include the Windows Domain Name.
- You can use the single-sign on feature between IBM Spectrum Control and storage system element managers.

Authenticate User names: Method two

- 1. Install IBM Spectrum Control on a Windows system that is a member of a Windows domain or on the Windows Domain Controller.
- 2. Configure IBM Spectrum Control for operating system authentication.

Planning for storage management

Plan for how to use IBM Spectrum Control to manage the storage and storage resources in your environment. In a complex environment, good planning helps you avoid delays and problems in getting your system up and running.

For information about how to plan for storage resources and actions, see the product documentation at

Planning for storage management.

Sudo command privileges

When you install, operate, or uninstall IBM Spectrum Control as a non-root user on AIX or Linux operating systems, you are required to have sudo privileges to multiple commands. Use command aliases in the /etc/sudoers file to configure your sudo privileges for multiple commands.

Example command aliases

The following command aliases are examples that you can create for installing, operating, and uninstalling IBM Spectrum Control:

- Cmnd_Alias IBMSC_INSTALL = /usr/bin/xauth, /Downloads/Db2_11.5_image/server_dec/db2setup, /opt/ibm/db2/V11.5/cfg/db2ln, /Downloads/IBM_Spectrum_Control_image/SC/setup.bin
- Cmnd_Alias IBMSC_OPERATION = /opt/IBM/TPC/scripts/*.sh, /opt/IBM/TPC/scripts/ldap/*.sh, /opt/IBM/TPC/agent/bin/agent.sh, / /opt/IBM/TPC/service/*.sh, /opt/IBM/TPC/service/changepasswords, /opt/IBM/TPC/client_images/*.sh, / /opt/IBM/TPC/cli/*.sh, /opt/IBM/TPC/data/scripts/logCleanup.sh, /opt/IBM/TPC/data/scripts/EncryptPassword.sh, / /opt/IBM/TPC/data/server/tools/repocopy, /opt/IBM/TPC/data/server/tools/runTPCDBMaintenance, / /opt/IBM/TPC/device/bin/linux/setenv.sh, /opt/IBM/TPC/device/bin/linux/disableapialerts.sh, /opt/IBM/TPC/wlp/bin/server, / /opt/IBM/TPC/device/bin/linux/disableapialerts.sh, /opt/IBM/TPC/wlp/bin/server, / /opt/IBM/TPC/dvice/bin/linux/disableapialerts.sh, /opt/IBM/TPC/yire/bin/ikeyman, /opt/IBM/TPC/jre/bin/ikeycmd, /bin/kill
- Cmnd_Alias IBMSC_UNINSTALL = /opt/IBM/TPC/_uninst/uninstall

The following examples show how to use the command aliases to provide non-root users privileges to the various commands:

username1	ALL=(root)	SETENV:	IBMSC_INSTALL
username2	ALL=(root)	SETENV:	IBMSC_OPERATION
username3	ALL=(root)	SETENV:	IBMSC_UNINSTALL

Chapter 2. Installing

Before you install IBM Spectrum Control, you must install IBM Db2 because Db2 is required for the IBM Spectrum Control database repository.

IBM Spectrum Control components

You can install IBM Spectrum Control in single-server or multiple-server environments. In a single-server environment, all components are installed on one server.

In single-server or multiple-server environments, when you install IBM Spectrum Control, the following components are installed:

- Database repository
- IBM Spectrum Control servers, which comprise the following components:
 - Data server
 - Device server
 - Alert server
 - Export server
 - Web server
 - IBM Spectrum Control GUI
 - Command-line interface (CLI)
 - Storage Resource agent

IBM Spectrum Control in an IPv4 or IPv6 environment

IBM Spectrum Control can use both IPv4 and IPv6 addresses for communication between its components.

If you have a system that is configured for dual-stack networking (with both IPv4 and IPv6 addresses), IBM Spectrum Control defaults to IPv4 addressing.

For information about using IPv4 and IPv6, see Planning for Internet Protocol Version 6.

Hardware requirements

The hardware requirements of the IBM Spectrum Control server.

Important: IBM Spectrum Control server can require a large amount of memory, disk space, network bandwidth, and processor resources. To promote consistent availability and performance, install IBM Spectrum Control on a dedicated server where no other critical business applications, including IBM Copy Services Manager, are installed. IBM Software Support is not responsible for availability, performance, and functional problems that are caused by other business applications that are deployed on the same server as IBM Spectrum Control.

For information about the hardware requirements for IBM Spectrum Control, see *Hardware Support: Memory, Processor and Disk Space* at IBM Spectrum Control 5.3.x - Hardware Support: Memory, Processor and Disk Space.

For information about the components that can be used with IBM Spectrum Control, see *Find the Supported Hardware, Products and Platforms Interoperability Matrix Links* at <u>http://www.ibm.com/</u>support/docview.wss?uid=swg21386446.

Restriction: On AIX or Linux operating systems, when you use a Virtual Network Computing (VNC) client that is connected to a VNC server, do not use the following key combinations:

- Alt + H to start the Help page
- Alt + N to proceed to next page
- Alt + P to return to the previous page
- Alt + I to start an installation action on the Summary page

You must press **Tab** and then press **Enter** or the spacebar when the button you want to press is selected. For example, to start the Help, press **Tab** until the **Help** button is highlighted and then press **Enter** or the spacebar.

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

The IBM Spectrum Control family supports a variety of operating systems.

Before you install IBM Spectrum Control, check the IBM Spectrum Control support site at https://www.ibm.com/support/docview.wss?uid=ibm10719187#Server for the latest operating system support.

Software requirements for Storage Resource agents

Storage Resource agents can be used by IBM Spectrum Control in various operating systems.

For a list of the operating systems that are supported for Storage Resource agents, go to <u>https://</u>www.ibm.com/support/docview.wss?uid=ibm10719187#Agents.

Software requirements for the database repository

IBM Spectrum Control uses Db2 as the database repository.

Important: You must use a 64-bit version of Db2 with IBM Spectrum Control. For more information about upgrading Db2 to Db2 11.1 or later, see "Example of upgrading Db2" on page 106.

Supported versions of Db2

For a list of the supported Db2 versions, go to [▶] <u>http://www.ibm.com/support/docview.wss?</u> uid=ibm10719187#DB.

Web browser support

The IBM Spectrum Control GUI runs in a web browser and includes the ability to monitor, manage, and troubleshoot storage resources. You can access this interface from anywhere that you have a web browser and connectivity to a network.

Before you start IBM Spectrum Control, ensure that you are using a supported web browser. For a list of web browsers that you can use with IBM Spectrum Control, see the support matrix at **IBM Spectrum** Control 5.3.x - Platform Support: Servers, Agents, and Browsers - Web Browsers.

Note: The IBM Spectrum Control GUI requires the use of cookies to manage user preferences, such as table customization and frequently viewed charts. Ensure that cookies are enabled to use these features.

Software requirements for LDAP servers

The LDAP repositories that are available on Windows, Linux and AIX operating systems, can be used with IBM Spectrum Control.

For information about the LDAP repositories that are supported, see one of the following WebSphere

Application Server Liberty web pages. On the **Supported Software** tab, click **LDAP Servers**. See 🕩 WebSphere Liberty - Detailed System Requirements.

Software requirements for CIM agents

IBM Spectrum Control requires CIM agents for some IBM storage devices such as the DS3000, DS4000[®], DS5000, DS6000.

CIM agents for DS3000, DS4000, DS5000, DS6000

For information about installing and configuring the CIM agent for the DS3000, DS4000, and DS5000, contact your CIM agent (LSI SMI Provider) at https://signin.netapp.com/oamext/login.html.

The LSI CIM agent must be installed and configured before you can collect data for the DS3000, DS4000, and DS5000 through IBM Spectrum Control. When you configure IBM Spectrum Control to connect to the CIM agent, you must provide the interoperability namespace for the device.

For information about the LSI CIM agent level that is required for each device and the namespace, see http://www.ibm.com/support/docview.wss?uid=swg21386446.

Also, note the following information about the CIM agents from LSI:

- Do not install the CIM agent on the same server as the IBM Spectrum Control server.
- Do not have the CIM agent monitor more than five storage systems.
- Use the LSI SMI-S Provider 10.06.GG.33 or later for the DS4000 and all levels of DS5000 MC 7.60. Otherwise, performance monitoring does not work.
- Do not use the LSI SMI-S agent for the DS4000 and DS5000 with an MC level earlier than 7.50. Lower-level microcode can cause a reboot of the controller device.

CIM agents for switches and directors

CIM agents (SMI-S providers) are also required for switches and directors. For a complete list of switches

and directors that are supported and the level of CIM agents that are required for each device, see http://www.ibm.com/support/docview.wss?uid=swg21386446.

CIM agents for non-IBM storage systems

IBM Spectrum Control also supports some non-IBM storage systems. For example, IBM Spectrum Control supports HP, TagmaStore, CLARiiON, Symmetrix, and other storage systems.

For a complete list of storage systems that are supported and the level of CIM agents that are required for each device, see $\xrightarrow{l=} http://www.ibm.com/support/docview.wss?uid=swg21386446.$

Installing IBM Spectrum Control

IBM Spectrum Control provides an installation program that guides you through the installation process. You can use the installation program or the command line in silent mode.

Installation checklists for IBM Spectrum Control

The installation of IBM Spectrum Control requires you to install a number of components. You can use the following checklists to guide you through the installation procedures for each component. Use separate checklists for multiple server installations.

Prepare your environment for installation

Ensure that your target environment is ready for an installation.

Table 15. Prepare your environment for an installation check list		
Chec k	Required for	Task
	Antivirus software	Installing IBM Spectrum Control involves making use of your operating system in manners typical for installing new application software. If your antivirus software is set on the maximum mode, it might prevent some of your changes from being accepted.
		To verify that your installation completes correctly, enable your antivirus software product to allow the following instances:
		 The /etc/hosts file can be edited
		 Files can be created in the /temp directory
		 New executable files can be created in the C:\Program Files directory
	Fully qualified host names	IBM Spectrum Control requires fully qualified host names, so you must install the product on a computer that has a fully qualified host name. For example, abc.tucson.example.comis a fully qualified host name where abc is the host name and tucson.example.com is the full domain name.
	Hardware prerequisites	For information about the hardware requirements for IBM Spectrum Control, see <i>Hardware Support: Memory, Processor</i> <i>and Disk Space</i> at ^{http://www.ibm.com/support/ docview.wss?uid=swg21386446.}
	Software prerequisites	 The IBM Spectrum Control family supports various operating systems, see <u>"Software requirements for operating systems"</u> on page 38 For the database repository, see <u>"Software requirements for the database repository"</u> on page 38 For LDAP servers, see <u>"Software requirements for LDAP</u>
		servers" on page 39

Table 15. Prepare your environment for an installation check list (continued)		
Chec k	Required for	Task
	Required user privileges	Ensure that you have the required privileges to install Db2 and IBM Spectrum Control.
		If you are installing on a Windows operating system, you must install as a user with administrator privileges. If you are installing on an AIX or Linux operating system, you must install as a root user or as a non-root user who has sudo privileges.
		If you want to install as a non-root user, your system administrator must complete configuration tasks on the target server before you begin the installation. These tasks are listed in <u>"Installing Db2 on AIX or Linux" on page 46 and "Installing IBM Spectrum Control in a single-server AIX or Linux</u> environment" on page 55.
		Ensure that Windows administrators have the Debug programs privilege.
	Download packages	You must download the installation packages or images into a separate directory for each product. The following list provides suggested download directory paths:
		 Windows operating systems:
		<pre>- c:\downloads\DB2</pre>
		<pre>- c:\downloads\TPC</pre>
		 AIX or Linux operating systems:
		– /downloads/DB2
		- /downloads/TPC
		For more information, see <u>"Planning for installation" on page 1</u>
	Language setting	Determine the operating system language that you want to use for IBM Spectrum Control. For optimal support, it's recommended that you use English. The web browser determines the language in which IBM Spectrum Control services and the IBM Spectrum Control GUI are displayed. For more information, see "Changing languages" on page 77.

Windows domain

Before you can install IBM Spectrum Control on a Windows domain, you must determine which installation method is appropriate, based on your environment. For more information, see <u>"Planning to install IBM Spectrum Control in a Windows domain" on page 8</u>

Table 16. Windows domain installation check list		
Chec k	Required for	Task
	Windows domain and local user accounts	When a computer is a member of a Windows domain, you can install IBM® Db2® on the computer such that the Db2® installation process creates a local Db2® user account or a domain Db2 user account. See <u>"Windows domain and local user</u> accounts" on page 8.

Table 16. Windows domain installation check list (continued)			
Chec k	Required for	Task	
	Adding a computer to the Windows domain	Before you can install IBM Spectrum Control in a Windows domain, you must first add the computer on which you plan to install IBM Spectrum Control to the domain, see <u>"Adding a</u> computer to the Windows domain" on page 9.	
	Create Windows domain common user account	You must create a Windows domain common user account before you can install IBM Spectrum Control in a Windows domain, see <u>"Creating a Windows domain common user</u> account for IBM Spectrum Control" on page <u>11</u> .	
	Grant Db2 SYSADM authority to Windows domain user account	If a Windows domain user account is used to install IBM Spectrum Control, the user account might not have the Db2 SYSADM authority, because Db2 goes to the domain controller computer to list the groups. Before you install IBM Spectrum Control, you must grant the Windows domain user accounts the Db2 SYSADM authority, see <u>"Granting Db2 SYSADM authority to</u> a Windows domain user account" on page 12.	

Db2

Install Db2 11.5 on Linux, AIX, or Windows operating systems.

Table 17. Db2 installation check list			
Chec k	Required for	Task	
	Prepare for Db2 installation	 When you install Db2 11.5, a default user name and groups are created. This default user name and password are used to install IBM Spectrum Control. See <u>"Preparing to install Db2"</u> on page 43. 	
	Install on Windows	For information on how to install Db2 on Windows operating systems, see <u>"Installing Db2 on Windows" on page 44</u> .	
	Install Db2 by using a Windows domain user account	 Before you install IBM Spectrum Control in a Windows domain, you must install Db2 and register the Db2 license key. You must have domain administrator access. You do not need to complete this task if you are planning to install Db2 by using a local user account, see <u>"Installing Db2 by using a Windows domain user account" on page 10</u>. 	
	Install Db2 on AIX or Linux - GUI installation	For information on how to install Db2 on AIX or Linux by using the GUI installation process, see <u>"Installing Db2 on AIX or Linux" on page 46</u> .	
	Install Db2 on AIX by using the command line	For more information on how to install Db2 on AIX by using the command line, see <u>"Installing Db2 on AIX by using the</u> command-line" on page 47.	
	Verify Db2 installation	You can verify that Db2 11.5 is installed properly by using the command line processor (CLP) or the First Steps GUI, see "Verifying that Db2 is installed correctly" on page 49.	

IBM Spectrum Control

Install IBM Spectrum Control by using the installation program or the command line in silent mode.

Table 18. Installation check list				
Chec k	Required for	Task		
	Choose installation method	For more information about what methods are available to install IBM Spectrum Control, see <u>"Planning for installation" on page 1</u>		
	Install IBM Spectrum Control on a single server.	For more information about how to install IBM Spectrum Control on a single server, see <u>"Installing IBM Spectrum Control in a</u> single-server environment " on page 54		
	Install IBM Spectrum Control on multiple servers.	For more information about how to install IBM Spectrum Control on multiple servers, see <u>"Installing IBM Spectrum Control in a</u> multiple-server environment " on page 62		

Db2

You can install the most recent version of Db2 that IBM Spectrum Control supports on the Linux, AIX, or Windows operating systems.

For more information about the supported versions, see <u>"Software requirements for the database</u> repository" on page 38.

Preparing to install Db2[®]

Before you install Db2, run the Db2 **db2prereqcheck** command on the target installation server to ensure that the server meets the prerequisites for Db2.

Before you install Db2, a default username and groups are created. This default username and password are used to install IBM Spectrum Control. You can use the default username and password or provide your own.

Note: Windows operating systems do not support systems that are configured only for IP 6. (Windows is enabled for IP 6 and IP 4.)

Preparing to install Db2 on Windows

Before you install Db2 on Windows operating systems, ensure that you correctly configured your directory names.

Short file names

If Db2 is installed on a drive on which 8.3 file names are disabled, and the Db2 installation directory name has spaces in it, Db2 must be reinstalled on a drive that has 8.3 file names enabled, or in a directory that does not have spaces in the name.

To check the current 8.3 file name settings for a drive, in a Db2 command window, run the **'fsutil.exe behavior query disable8dot3'** command.

These are the values when you run the command:

- 0 = Create 8.3 short file names (default)
- 1 = Do not create 8.3 file names
- 2 = Set 8.3 file names on a per volume basis
- 3 = Disable 8.3 file names on all volumes, except the system volume

The registry state of NtfsDisable8dot3NameCreation is 0 $\,$, which means that 8.3 file names are enabled on all volumes.

To enable 8.3 file names on a global basis, run the **fsutil.exe behavior set disable8dot3 0** command.

Preparing to install Db2[®] on UNIX or Linux

To operate Db2[®] on operating systems such as UNIX or Linux, the instance owner, the fenced user, and the Db2[®] administration server user are required. These users and groups are automatically created when Db2[®] is installed.

The user ID you need to install IBM Spectrum Control must be the owner of the instance that you want to use; this user ID and password are created when you install Db2[®].

Table 19 on page 44 provides a list of the default user and group names.

Table 19. Db2 [®] setup 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 and stored procedures that are separate from the address space that is used by the Db2 [®] database.

Related information

Db2 User, user ID and group naming rules Db2 password rules

Installing Db2[®]

You can install IBM[®] Db2[®] on AIX, Linux, or Windows operating systems.

Installing Db2 on Windows

Before you can install IBM Spectrum Control, you must install Db2[®].

If you are installing Db2 in a Windows domain environment: See "Installing Db2 by using a Windows domain user account" on page 10 for additional and alternate steps that are required to install Db2.

To install Db2 on a Windows operating system, complete the following steps:

- 1. Log on with a user ID that has Administrator authority on Windows.
- 2. Use the extracted Db2 installation image. Windows Autorun starts the launchpad.

If you are using Windows Autorun, the installation program should start in 15-30 seconds. If the installation program does not start, complete one of the following steps:

- In a command prompt, to start the Db2 set up page, go to web image extraction *server_folder* and run the **setup.exe** command.
- In Windows Explorer, go to web_image_extraction\server_folder, and double-click the setup.exe file.

Where *server_folder* in the preceding steps is the location of the Db2 installation program.

3. In the DB2 Setup Launchpad, click Install a Product.

4. Click Install New for DB2 Version 11.5 Server Editions.

Note: If you do not see the DB2 Setup program, it is probably running in the background. Look for a blinking icon in the Windows taskbar and click it to bring it to the foreground.

- 5. On the welcome page of the DB2 Setup program, click Next.
- 6. On the Software License Agreement page, review and accept the license agreement, and click Next.
- 7. On the Select the installation type page, click Typical, and click Next.
- 8. On the Select the installation, response file creation, or both page, select Install DB2 Server Edition on this computer and save my settings in a response file.
- 9. Enter a response file name or accept the default, and click Next.
- 10. On the Select the installation folder page, enter a directory or accept the default, and click Next.
- 11. On the **Select the IBM SSH server installation folder and startup option** page, enter a directory or accept the default, and click **Next**.
- 12. On the **Set user information for the DB2 Administration Server** page, enter the following user information:
 - a. Leave the **Domain** field blank.
 - b. In the User name field, type the DB2 user ID that you want to use or accept the default.
 - c. In the **Password** field, type a password and confirm the password by typing it again in the **Confirm password** field.
- 13. Select the Use the same account for the remaining DB2 services check box and click Next.
- 14. On the Configure DB2 instances page, click Next.
- 15. On the **Set up notifications** page, clear the **Set up your DB2 server to send notifications** check box, and click **Next**.
- 16. On the Enable operating system security for DB2 objects page, accept the defaults, and click Next.

The default is to enable operating system security.

Note: If you installed Db2 before on this system, and the DB2ADMS group exists, when you click **Next**, the following message is displayed:

```
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.
```

- 17. On the **Start copying files and create response file** page, review the current settings, and click **Finish**.
- 18. On the Setup is complete page, review the information, and click Finish.
- 19. The setup program closes and the DB2 First Steps page opens. Close the DB2 First Steps page.
- 20. Restart the system.

Note: To prevent the Db2 logs from filling up the C drive on the system you are installing on, you can set the *DIAGPATH* and *SPM_LOG_PATH* variables to point to an external, fast disk drive.

After you restart your computer, you must install IBM Spectrum Control. For more information about installing IBM Spectrum Control in a single-server environment, see <u>"Installing IBM Spectrum Control in a single-server Windows environment" on page 54</u>. For information about installing IBM Spectrum Control in a multiple-server environment, see <u>"Installing IBM Spectrum Control with a remote database by using the installation program" on page 63</u>.

Installing Db2 on AIX or Linux

You can install Db2[®] as a root user or non-root user on an AIX or Linux operating system by using the Db2 Setup program. To install Db2 as a non-root user, the user must have sudo privileges on the target AIX or Linux server.

The X Window System is required on the AIX or Linux server to install Db2 by using the installation program.

If you want to install Db2 as a non-root user, have your system administrator complete the following tasks on the target server before you begin the installation:

• If you are installing Db2 on an AIX server, install sudo on the server. The default AIX distribution does

not include sudo. To get the sudo installation package, go to http://www.ibm.com/systems/power/software/aix/linux/toolbox/date.html. Find sudo-version in the Package column, and click RPM to download the package.

- Ensure that the non-root user has sudo privileges for the following commands on the server:
 - xauth (Enables the non-root user to provide access to their X Window System display for the root user.)
 - **db2setup** (Enables the non-root user to launch the Db2 installation program.)

You must enter the full path to the commands when you configure the sudo privileges. For example:

username ALL=(root) SETENV: /usr/bin/xauth,/home/username/Downloads/DB2/server_dec/db2setup

- Ensure that the following requirements are met to enable the installation of Db2 by using the Setup program:
 - The non-root user is able to use the X Window System on the target server and the X Window System DISPLAY environment variable is set correctly for the not-root user.
 - The DISPLAY environment variable is preserved in the sudo environment.
 - The root user has access to the X Window System display that is owned by the non-root user.

These display requirements do not apply if you install Db2 in silent mode.

- If you are installing Db2 on an AIX server, ensure that the ODMDIR environment variable is preserved in the sudo environment.
 - 1. Log on to the target server as the root user or as a non-root user who has sudo privileges.
 - 2. Use an extraction tool to extract the installation image files on the server.
 - 3. In a command shell, change the directory to the location of the Db2 installation program db2setup, and then enter one of the following commands:

Root user

./db2setup

Non-root user

sudo ./db2setup

- 4. On the DB2 Setup Welcome page, click New Install.
- 5. On the Choose a Product page, select DB2 Version 11.5 Server Editions and click Next.
- 6. On the Confirmation page:
 - a) Enter an installation directory or accept the default.
 - b) Select **Typical** as the installation type.
 - c) Select Create an instance.
 - d) Review and agree to the IBM terms.
 - e) Click **Next**.
- 7. On the Instance Owner page, select **New user**, and enter the following information:

a) User name

Db2 adds this user ID to the db2iadm1 group, and if this user ID does not exist, Db2 creates it.

- b) Group name
- c) Password
- d) Home directory

The Db2 instance owner user is the user that you enter when you install IBM Spectrum Control.

- 8. Select Use default UID and Use default GID, and click Next.
- 9. On the Fenced User page, select **New user**, and enter the following information:
 - a) User name

Db2 adds this user ID to the db2iadm1 group, and if this user ID does not exist, Db2 creates it.

- b) Group name
- c) Password
- d) Home directory

The fenced user is used to run user-defined functions and stored procedures that are separate from the address space that is used by the Db2 database.

- 10. Select Use default UID and Use default GID, and click Next.
- 11. On the Response File and Summary page:
 - a) Select Install DB2 Server Edition on this computer and save my settings in a response file.
 - b) Enter a response file name or accept the default.
 - c) Review the Summary and click **Finish**.

12. On the Setup has completed successfully page, review the information, and click Finish.

To ensure that Db2 starts when the server starts, run the **db2iauto** command.

Root user

DB2_installation_directory/bin/db2iauto -on DB2_instance_name

Non-root user

sudo DB2_installation_directory/bin/db2iauto -on DB2_instance_name

Where *DB2_installation_directory* is the location of Db2 and *DB2_instance_name* is the instance that you created when you installed Db2. The default instance name is *db2inst1*.

Installing Db2 on AIX by using the command-line

You can install Db2 on AIX operating systems by using commands.

Ensure that you have:

- 2 3 GB of hard disk drive space for the Db2 installation tar file and extracted files.
- A file system with at least 30 GB for the IBM Spectrum Control repository.

To install Db2 on the AIX operating system by using a command prompt, complete the following steps:

- 1. Log in with a user ID that has root authority.
- 2. Do one of the following steps.
 - If you are not using a DVD, skip to step 5 and work from the directory where you have the Db2 source installation program.
 - If you are using a DVD, create a mount point that is called /cdrom by entering mkdir /cdrom.
- 3. Insert the Db2 DVD into the DVD drive and mount the file system at the mount point.

On AIX operating system, you can use the **crfs** command to add an entry to /etc/filesystems for the mount point.

4. Run the following commands:

```
/usr/sbin/crfs -v cdrfs -p ro -d'cd0' -m'/cdrom' -A'no'
mount /cdrom
```

The **crfs** command must be run only one time for a mount point. For each DVD you insert after that, you can use **mount** and **umount**, for example, **mount /cdrom** and **umount /cdrom**.

- 5. Enter cd /cdrom and go to the directory where the DVD-ROM is mounted.
- 6. Install the Db2 Manager.
 - a) Create a temporary directory (for example, db2temp) to hold the Db2 installer tar file and extracted files.
 - 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) If the Db2 installer file is compressed, use the appropriate extracting tool. For example, if the name of the file is v11.5_aix64_server.tar.gz, enter gunzip v11.5_aix64_server.tar.gz. In this example, v11.5_aix64_server.tar.gz is displayed in the db2temp directory.
 - d) Create an installation directory by entering, for example, mkdir install.
 - e) Enter cd install to change to the new installation directory.
 - f) Extract the Db2 installation file.
 For example, if the name of the installation file is v11.5_aix64_server.tar , enter tar
 xvf ../v11.5_aix64_server.tar .
 - g) Enter cd /db2temp/install/server_dec and go to the directory that contains the Db2 installation program db2_install.
 - h) Enter ./db2_install to run the command-line installation program.
 - i) Select **SERVER**.
 - j) Select no from the Do you want to install the DB2 pureScale Feature? [yes/no] section. The Installation Summary is displayed, which indicates a successful installation. Db2 is installed in /opt/IBM/db2/V11.5.
- 7. Create users and groups for use with Db2.
 - a) Entermkgroup id=999 db2iadm1.
 - b) Entermkgroup id=998 db2fadm1.
 - c) Entermkuser id=1004 pgrp=db2iadm1 groups=db2iadm1 home=/home/db2inst1 db2inst1.
 - d) Entermkuser id=1003 pgrp=db2fadm1 groups=db2fadm1 home=/home/db2fenc1 db2fenc1.
 - e) Verify the owner of the directories by entering ls -ld /home/db2inst1.

The directory ownership is displayed as follows:

- /home/db2inst1 shows group db2iadm1 and user db2inst1
- /home/db2fenc1 shows group db2fadm1 and user db2fenc1

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
```

f) Enter passwd db2inst1 to set the password that you want to use for the Db2 instance.

```
g) Enter pwdadm -f NOCHECK db2inst1.
```

```
h) Enter passwd db2fenc1 to set the password you want to use for the fenced user.
```

```
i) Enter pwdadm -f NOCHECK db2fenc1.
```

```
j) Enter chgroup users=db2inst1,root db2iadm1.
```

- 8. Create a Db2 instance:
 - a) Enter/opt/IBM/db2/V11.5/instance/db2icrt -a server -u db2fenc1 db2inst1.
 - b) Enter . /home/db2inst1/sqllib/db2profile.
- 9. Change the default location for database repositories.

By default, the location is /home/db2inst1. The /home output is typically not large enough for database repositories.

- 10. To change the default location:
 - a) Enter db2 update dbm cfg using DFTDBPATH *new_repository_path* IMMEDIATE, where *new_repository_path* represents the new location for the repository.
 - b) Enter 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).
- 11. Configure Db2 communication:
 - a) Edit /etc/services and verify or add the following line at the end of the file: db2c_db2inst1 50000/tcp
 - b) Enter db2 update dbm cfg using svcename db2c_db2inst1.
 - c) Enter db2set DB2COMM=tcpip.
 - d) Enter db2stop.
 - e) Enter db2start.
- 12. From a command prompt, do the following to test your Db2 instance:
 - a. Enter . /home/db2inst1/sqllib/db2profile to source the environment.
 - b. Enter db2level to get information about the instance and Db2.
 - c.Enterdb2 create db test.
 - d. Enter db2 list db directory to list information about all the databases that are created for this instance.
 - e. Enter db2 connect to test user db2inst1 using the password to connect to the database.
 - f. Enter db2 disconnect test to disconnect from the test database.
 - g. Enter db2 drop db test to drop the test database.

Installing IBM Data Studio by using the DB2 setup program

IBM Data Studio installation is included with the DB2 version 10.1 and higher product installation. The DB2 Setup program provides an option to install Data Studio components.

Use the DB2 Setup program to define your installation preferences and to install IBM Data Studio full client component.

To use the DB2 Setup program to install Data Studio, follow these steps:

- 1. Start the DB2 Setup program.
- 2. Select Install Data Studio Components.
- 3. Select Install Data Studio full client component.
- 4. Follow the instructions to install Data Studio.

Verifying that Db2 is installed correctly

You can verify that Db2[®] is installed properly by using the command-line processor (CLP) or the First Steps GUI.

To verify that Db2[®] is installed, complete the following steps:

- 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 is successfully installed using the command-line processor (CLP).

To verify that Db2 is installed using the command line processor, complete the following steps:

- 1. Log on to the system as a user with SYSADM authority.
- 2. Enter db2start to start the database manager.

In operating systems such as AIX and Linux, you must source the db2profile before you run the **db2start** command. For more information about sourcing the profile, go to the IBM Spectrum Control Knowledge Center and search for *Using the command line on AIX and Linux*.

3. Enter the **db2samp1** command to create the SAMPLE database.

This command might 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 commands in a Db2 command window to connect to the SAMPLE database, retrieve a list of all the employees who 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 verifying the installation, remove the SAMPLE database to free up disk space.

For more information about verifying Db2 installation, refer to the Db2 documentation for your operating system.

6. Enter db2 drop database sample to drop the SAMPLE database.

Verifying Db2 installation by using the First Steps tool

You can verify that Db2[®] is installed successfully, by using the First Steps tool.

- Ensure that the domain user account that you use to create the sample database has SYSADM or SYSCTRL authority.
- Install IBM Data Studio and the First Steps component.

The First Steps tool is part of the getting started component grouping in the Db2 setup program. It is installed as part of a typical installation or you can select the First Steps tool during a custom installation.

To verify the Db2[®] installation by using the First Steps tool, complete the following steps:

- 1. Log on to the system with the user account that you want to use to verify the installation.
- 2. Start First Steps by completing one of the following steps:
 - On operating systems such as AIX or Linux, run the db2fs command.
 - On Windows, run the db2fs.bat command.
- 3. On the First Steps window, select Create Sample Databases.
- 4. On the **Create Sample Databases** page, select the databases that you want to create and click **OK**. By default, the SAMPLE database is created on the computer where Db2 is installed.
- 5. Click **OK**.
- 6. Open Data Studio.
- 7. Expand the navigation tree to view the SAMPLE database and SAMPLE database objects.
- 8. Select the Tables object to view the SAMPLE database tables.
- 9. After you verify the installation, remove the SAMPLE database to free disk space.
- 10. Enter the **db2 drop database sample** command to drop the SAMPLE database.

Licensing Db2

You can apply a valid license to Db2 by using the **db2licm** command.

The installation and operation of IBM Spectrum Control requires that Db2 is running on your system. After your Db2 11.1 trial license period expires, Db2 11.1 does not start without a valid license.

IBM Spectrum Control does not support the Db2 11.5 Community license.

To apply a valid license to Db2 with the **db2licm** command, complete the following steps:

- 1. Retrieve and extract a valid Db2 license that is supplied on the IBM Spectrum Control download site.
- 2. Open a Db2 command prompt or switch to the Db2 instance owner user and in the location where you extracted your Db2 license, change to the following directory:

awse_o/db2/license/if you are using Db2 11.1std_au_np/db2/license/if you are using Db2 11.5

3. Run the following command:

Using Db2 11.1 on the Windows operating system:

Db2_installation_location\BIN\db2licm -a db2awse_o.lic

Using Db2 11.5 on the Windows operating system:

Db2_installation_location\BIN\db2licm -a db2std_au_np.lic

where *Db2_installation_location* is the base installation directory for Db2 on your computer. For example, C:\Program Files\IBM\SQLLIB.

Using Db2 11.1 on the AIX/Linux operating system:

Db2_installation_location/adm/db2licm -a db2awse_o.lic

Using Db2 11.5 on the AIX/Linux operating system:

Db2_installation_location/adm/db2licm -a db2std_au_np.lic

where *Db2_installation_location* is the base installation directory for Db2 on your computer. For example, /opt/ibm/db2/V11.5.

Related information

db2licm - License management tool command

Starting the installation programs

There are various methods to start the IBM Spectrum Control installation programs and on various operating systems.

Installation program methods

You can use these methods to start the installation programs:

Installation images

You must select an installation image and download and extract these images to a location with adequate disk space.

Storage Resource agent

Contains the files to run local Storage Resource agent installations. You must download the file for the system on which you want the agent to be in.

- The Storage Resource agent location and operating system file name is the same as the product electronic image.
- The Storage Resource agent image is in *installation_dir/data/sra/ operating_system_name*.

The operating systems that are supported for the Storage Resource agents are listed in the following table.

Table 20. Operating system for Storage Resource agents.			
Operating system	Operating system name		
Windows	windows		
AIX	aix_power		
HP-UX	hp-ux_itanium		
Linux x86	linux_ix86		
Linux for Power Systems Servers	linux_power		
Linux s390	linux_s390		
Oracle Solaris	solaris_spark		

Important:

• If you are using IBM Spectrum Control electronic installation images that are decompressed in a directory that has spaces in the name, IBM Spectrum Control does not install correctly.

For example, if you have the following directory name:

- On Windows operating systems:

C:\Spectrum Control\disk\SC

- On AIX and Linux operating systems:

/temp/Spectrum Control/disk/SC

IBM Spectrum Control does not install correctly.

When you remove the spaces, and rename the directory, for example:

- On Windows operating systems:

C:\SpectrumControl\disk\SC

- On AIX and Linux operating systems:

/temp/SpectrumControl/disk/SC

IBM Spectrum Control installs correctly.

• If you are using IBM Spectrum Control electronic installation images for Linux or AIX operating systems and you download the images to a directory, ensure that your folder name *does not* contain a . at the end of the folder name.

For example, if you have a directory name

C:\SpectrumControl\disk\SC.

When you rename the folder and remove the . at the end of the name, for example:

C:\SpectrumControl\disk\SC.August3

IBM Spectrum Control installs correctly.

Starting the installation program on the Windows operating system

To start the IBM Spectrum Control installation program by using an electronic image, complete the following steps.

1. Download the image into a directory.

- 2. Extract the image files.
- 3. At the command prompt, enter cd *source_installation_directory*\SC and then enter **setup.bat**.

Starting the installation program on the Linux operating system

To start the IBM Spectrum Control installation program from the electronic image, complete the following steps.

1. Enter the following to create a directory:

mkdir /SpectrumControl

- 2. Download the image into the SpectrumControl directory.
- 3. Enter this command to extract the image files:

tar -xzvf filename.tar.gz

4. Ensure that the user name that you plan to use as the IBM Spectrum Control common user is in the root group and the db2iadm1 group. If the user name is not in a group, you can add the user as shown in the following command example. In this example, the user name is *db2inst1*.

usermod -a -G root db2inst1

5. Navigate to the /SpectrumControl/SC directory by entering:

cd /SpectrumControl/SC

6. Set up your shell environment to point to the instance where the database repository is installed. Source the db2profile for the instance that you want. For example, if the Db2 instance is db2inst1, you can source the db2profile by entering:

```
. /home/db2inst1/sqllib/db2profile
```

Remember: There is a space between . and /home.

7. Start the installation program by running the **./setup.bin** command from the same command shell that you used in step 6.

Starting the installation program on the AIX operating system

To start the IBM Spectrum Control installation program from the electronic image, complete the following steps:

1. Enter the following to create a directory:

mkdir /SpectrumControl

- 2. Download the image into the SpectrumControl directory.
- 3. Enter this command to extract the image files:

tar -xzvf filename.tar.gz

4. Ensure that the user name that you plan to use as the IBM Spectrum Control common user is in the system group and the db2iadm1 group. If the user name is not in a group, you can add the user as shown in the following command example. In this example, the user name is *db2inst1*.

usermod -G system db2inst1

Tip: If the user is already a member of secondary groups, the **usermod** command removes the db2inst1 user name from all of the secondary groups except for the system group. To preserve the existing secondary group memberships, provide a comma separated list of secondary groups after the **-G** flag. For more information, enter man usermod at the command prompt.

5. Navigate to the /SpectrumControl/SC directory.

cd /SpectrumControl/SC

6. Set up your shell environment to point to the instance where the database repository is installed. Source the db2profile for the instance that you want. For example, if the Db2 instance is db2inst1, you can source the db2profile by entering:

. /home/db2inst1/sqllib/db2profile

Remember: There is a space between . and /home.

7. Start the installation program by running the **./setup.bin** command from the same command shell that you used in step 6.

Installing IBM Spectrum Control in a single-server environment

Install IBM Spectrum Control by using the installation program or the command line in silent mode.

Installation considerations

Before you begin the installation of IBM Spectrum Control, ensure that Db2 is installed. To learn how to install Db2, see <u>Installing Db2</u>. If you install Db2 on a Windows server, reboot the system before you install IBM Spectrum Control.

When you install IBM Spectrum Control, a database that is called *TPCDB* is created. In this repository, the IBM Spectrum Control database schema is created, which describes the structure of the database repository. If you already have the *TPCDB* database on your system, IBM Spectrum Control assigns a new default database repository name with a number as a suffix. For example, *TPCDB*1.

If the operating system on which you are installing IBM Spectrum Control is sensitive to spaces in directory paths, change the default installation location to not include spaces, for example, C:\apps \IBM\SC.

Installing IBM Spectrum Control in a single-server Windows environment

You can install IBM Spectrum Control by using the IBM Spectrum Control installation program.

To install IBM Spectrum Control in a single-server environment, complete the following steps:

1. Log on to the target server a user who as administrator privileges.

Note: Confirm that your Windows firewalls are disabled in the Control Panel.

2. When you install IBM Spectrum Control, the TPCDB database is created in the location that you specify in the Db2 DFTDBPATH variable.

To determine the current DFTDBPATH value, run the following command in a Db2 CLI window:

get dbm cfg

If you want to install this database in a location that is other than the default location, run the following command in a Db2 CLI window:

update dbm cfg using DFTDBPATH path

where path is the new value for the DFTDBPATH variable.

- 3. Use an extraction tool to extract the installation image files on the server.
- 4. In a command window, change the directory to the location of the IBM Spectrum Control installation files and enter the following command:

setup.bat

5. Follow the prompts in the installation program to install IBM Spectrum Control.

If an error occurred during the IBM Spectrum Control installation process, review the IBM Spectrum Control installation log files to find details about the error.

Installing IBM Spectrum Control in a single-server AIX or Linux environment

You can install IBM Spectrum Control as a root user or non-root user on an AIX or Linux operating system by using the IBM Spectrum Control installation program. To install IBM Spectrum Control as a non-root user, the user must have sudo privileges on the target AIX or Linux server.

Ensure that X Window System is installed on the target AIX or Linux server. The X Window System is required to install IBM Spectrum Control by using the installation program.

If you want to install IBM Spectrum Control as a non-root user, have your system administrator complete the following tasks on the target server before you begin the installation:

• If you are installing IBM Spectrum Control on an AIX server, install sudo on the server. The default AIX

distribution does not include sudo. To get the sudo installation package, go to <u>http://www.ibm.com/</u> systems/power/software/aix/linux/toolbox/date.html. Find **sudo-version** in the **Package** column, and click **RPM** to download the package.

- Ensure that the non-root user has sudo privileges for the following commands on the server:
 - xauth (Enables the non-root user to provide access to their X Window System display for the root user.)
 - db21n (Enables the non-root user to create the links for the Db2 system files.)
 - **setup.bin** (Enables the non-root user to launch the IBM Spectrum Control installation program.)

You must enter the full path to the commands when you configure the sudo privileges. For example:

username ALL=(root) SETENV: /usr/bin/xauth./opt/ibm/db2/V11.5/cfg/db2ln./home/username/Downloads/IBMSC/SC/setup.bin

- If the sudo environment on the server uses the secure_path option, ensure that the following directories are included in the secure_path value for the non-root user who is installing IBM Spectrum Control:
 - DB2_instance_owner_home_directory/sqllib/bin(Example:/home/db2inst1/sqllib/ bin)
 - DB2_instance_owner_home_directory/sqllib/adm(Example:/home/db2inst1/sqllib/ adm)
 - DB2_instance_owner_home_directory/sqllib/misc (Example: /home/db2inst1/sqllib/ misc)
- Ensure that the following requirements are met to enable the installation of IBM Spectrum Control by using the installation program:
 - The non-root user is able to use the X Window System on the target server and the X Window System DISPLAY environment variable is set correctly for the not-root user.
 - The DISPLAY environment variable is preserved in the sudo environment.
 - The root user has access to the X Window System display that is owned by the non-root user.
 - These display requirements do not apply if you install IBM Spectrum Control in silent mode.
- If you are installing IBM Spectrum Control on an AIX server, ensure that the ODMDIR environment variable is preserved in the sudo environment.

To install IBM Spectrum Control in a single-server environment, complete the following steps:

- 1. Log on to the target server as the root user or as a non-root user who has sudo privileges.
- 2. If you logged on as a non-root user, run the following command in a command shell:

sudo DB2_installation_directory/cfg/db2ln

For example:

sudo /opt/ibm/db2/V11.5/cfg/db2ln

3. When you install IBM Spectrum Control, the TPCDB database is created in the location that you specify in the Db2 DFTDBPATH variable.

To determine the current DFTDBPATH value, run the following command in a Db2 CLI window:

get dbm cfg

If you want to install this database in a location that is other than the default location:

a. Run the following command in a Db2 CLI window:

update dbm cfg using DFTDBPATH path

where *path* is the new value for the DFTDBPATH variable.

- b. Run the **db2stop** and **db2start** commands to stop and restart Db2.
- 4. Use an extraction tool to extract the installation image files on the server.
- 5. In a command shell, source the Db2 user profile db2profile for the Db2 instance owner. For example:

. /home/db2inst1/sqllib/db2profile

6. In a command shell, change the directory to the location of the IBM Spectrum Control installation program setup.bin, and then enter the following command:

Root user

./setup.bin

Non-root user

sudo -E ./setup.bin

7. Follow the prompts in the installation program to install IBM Spectrum Control.

If an error occurred during the IBM Spectrum Control installation process, review the IBM Spectrum Control installation log files to find details about the error.

Installing IBM Spectrum Control in a single-server environment by using silent mode

You can install IBM Spectrum Control by using silent mode. The installation program does not display any configuration options during the installation process.

If you plan to install IBM Spectrum Control as a non-root user, have your system administrator complete the tasks that are described in <u>"Installing IBM Spectrum Control in a single-server AIX or Linux</u> environment" on page 55 on the target server before you begin the installation.

If you are installing on a Windows operating system, confirm that your Windows firewalls are disabled in the Control panel.

To install IBM Spectrum Control in a single-server environment by using silent mode, complete the following steps:

1. Log on to the server where you want to install IBM Spectrum Control.

If you are installing on a Windows operating system, log on as a user who as administrator privileges. If you are installing on an AIX or Linux operating system, log on as the root user or as a non-root user who has *sudo* privileges.

2. If you logged on as an AIX or Linux non-root user, run the following command in a command shell:

sudo Db2_installation_directory/cfg/db2ln

For example:

sudo /opt/ibm/db2/V11.5/cfg/db2ln

3. When you install IBM Spectrum Control, the TPCDB database is created in the location that you specify in the Db2 DFTDBPATH variable.

To determine the current DFTDBPATH value, run the following command from a Db2 CLI window:

get dbm cfg

If you want to install this database in a location that is other than the default location:

a. Run the following command in a Db2 CLI window:

update dbm cfg using DFTDBPATH path

where *path* is the new value for the DFTDBPATH variable.

- b. If you are installing on an AIX or Linux operating system, run the **db2stop** and **db2start** commands to stop and restart Db2.
- 4. Edit and save the appropriate response file.

For more information about editing the response file, see "Editing the response file" on page 58.

5. If you are installing on an AIX or Linux operating system, in a command shell, source the Db2 user profile db2profile for the Db2 instance owner.

For example:

```
. /home/db2inst1/sqllib/db2profile
```

- 6. Run the silent mode installation program.
 - For Windows operating systems, run the following command:

setup.bat -1 language -i silent -f absolute_path_to_response_file

where *language* can be one of the following values:

- Czech cs
- English en
- French fr
- German de
- Hungarian hu
- Italian it
- Japanese ja
- Korean ko
- Polish pl
- Brazilian Portuguese pt_BR
- Russian ru
- Spanish es
- Chinese (Simplified) zh_CN
- Chinese (Traditional) zh_TW

absolute_path_to_response_file is the absolute path to the response file. For example, the following command specifies the language and the path:

setup.bat -1 fr -i silent -f c:\TPC\silent_SingleServerTypical.properties

• For AIX or Linux operating systems, run the following command:

Root user

./setup.bin -1 language -i silent -f /absolute_path_to_response_file

For example, the following command specifies the language and the path:

./setup.bin -1 de -i silent -f /TPC/silent_SingleServerTypical.properties

Non-root user

sudo -E ./setup.bin -l language -i silent -f /absolute_path_to_response_file

For example, the following command specifies the language and the path:

sudo -E ./setup.bin -l de -i silent -f /TPC/silent_SingleServerTypical.properties

If you do not specify a language or if the language is not specified correctly, the installation program uses the English language as the default.

- 7. Monitor the progress of the installation.
 - To view the progress of the silent mode installation on Windows operating systems, check the trace log in the following path:

```
installation_dir\logs\traceTPCInstall.log
```

• To view the progress of the silent mode installation on AIX or Linux operating systems, check the trace log in the following path:

installation_dir/logs/traceTPCInstall.log

Editing the response file

You must edit and save the appropriate response file when you install IBM Spectrum Control by using silent mode. The silent mode installation option for the response file is -f absolute_path_to_response_file. For example, in the Windows operating system, you enter -f C:\installimage\silent_SingleServerTypical.properties.

Use the following response files during a silent mode installation:

silent_SingleServerTypical.properties

This file specifies that all the IBM Spectrum Control components are installed on one server. You can customize this file by changing the ports for the Data server, Device server, Alert server, web server, and Storage Resource agent.

silent_SingleServerCustom.properties

This file specifies that all the IBM Spectrum Control components are installed on one server with the following customization options:

- Change the user name and password to install the database repository.
- Change the name of the database repository.
- Change the paths for the database repository.
- Change the path for the database repository log.
- Change the ports for the Data server, Device server, Alert server, web server, and Storage Resource agent.

silent_MultipleServer.properties

This file specifies the information that is required for a multiple-server environment. You can install the database repository on a remote server and install the other IBM Spectrum Control components on a local server.

Common response file parameters

These installation parameters are valid for all the response files.

CHOSEN_INSTALL_TYPE="option"

Specifies the installation type. Not all options are available in all the response files. <u>Table 21 on page 59</u> shows you the options that you can specify.

Table 21. Options for the CHOSEN_INSTALL_TYPE parameter			
Properties file	Valid options		
<pre>silent_SingleServerTypical</pre>	Single Server InstallLicense Upgrade		
silent_SingleServerCustom	Single Server InstallLicense Upgrade		
silent_MultipleServer	Multiple Server InstallLicense Upgrade		

For example:

CHOSEN_INSTALL_TYPE="Single Server Install"

LICENSE_ACCEPTED=false

Specifies whether the user accepts the IBM Spectrum Control license agreement. The options are as follows:

true

The user accepts all the terms and conditions of the IBM Spectrum Control license agreement.

false or any other value

The user does not accept the IBM Spectrum Control license agreement. The installation program exits.

USER_INSTALL_DIR=option

Specifies the location where you want to install IBM Spectrum Control.

On Windows operating systems, you must use double backslashes. For example:

USER_INSTALL_DIR=C:\\Program Files\\IBM\\TPC

The default value for Windows operating systems is C:\\Program Files\\IBM\\TPC.

Note: If the operating system on which you are installing IBM Spectrum Control is sensitive to spaces in directory paths, change the default installation location to not include spaces, for example, C:\apps\IBM\SC.

The default value for AIX or Linux operating systems is /opt/IBM/TPC.

varSrvName=option

Specifies the fully qualified host name of the server.

If your system is configured for dual stack networking (with both IPv4 and IPv6 addresses), IBM Spectrum Control defaults to IPv4 addressing.

Ensure that DNS is configured correctly on your server and verify that these files exist on your target server:

- For Windows operating systems, C:\Windows\system32\drivers\etc\hosts.
- For AIX or Linux operating systems, /etc/hosts.

These files must have an entry similar to the following example:

myserver.example.mycompany.com myserver

varTPCPortRangeSP=port

Specifies the first port in a range of ports. The default beginning port is 9549. These ports are used by the IBM Spectrum Control servers, and the Storage Resource agent.

varCommonUsrID=user_name

Specifies the user name to install IBM Spectrum Control. The default user name for Windows operating system is db2admin. The default user name for AIX or Linux operating system is db2inst1.

The user name that you select must have the following operating system privileges:

- For Windows operating systems, the user name must be in the administrators group.
- For Linux operating systems, the user name must be in the root group.
- For AIX operating systems, the user name must be in the system group.

If you are using the common user name to also install the database repository, the user name must have these Db2 privileges:

- For Windows operating systems, the user name must be in the DB2ADMNS group.
- For AIX or Linux operating systems, the user name must be in the db2iadm1 group.

varCommonUsrPw=password

Specifies the password for the common user name.

varFullRollback=value

Specifies whether a full rollback or partial rollback is done when an installation failure occurs. These are the values:

0

Specifies that a partial rollback occurs. This value is the default.

1

Specifies that a full rollback occurs.

varUseLicenseKeyOnImage=value

Specifies whether to use the license key file that is present on the installation image. The value can be:

0

Uses the license key that is present on the installation image (default value)

1

Provides the location of the license key file

Depending on the license package you purchased, one of these license files is included with IBM Spectrum Control in the root installation directory and is on the product electronic image:

nodelock

IBM Spectrum Control Standard Edition license

nodelock.SEL

IBM Spectrum Control Standard Select Edition license

nodelock.AE

IBM Spectrum Control Advanced Edition license

nodelock.AS

IBM Spectrum Control Advanced Select Edition license

varLicenseKeyFile=location_of_license_key_file

Specifies the path for the license key file. This value must be set if the **varUseLicenseKeyOnImage=1** parameter is specified.

On the Windows operating system, you must use double backslashes. For example:

C:\\license\\key\\nodelock.SEL

Response file parameters for advanced customization of the database repository

These parameters are used for the silent_SingleServerCustom.properties and silent_MultipleServer.properties response files to configure the database repository.
varDBAdmUsr=user_name

Specifies the user name that you must use to install the IBM Spectrum Control database. The user who logs in with this user name must be the owner of the Db2 instance where the database is created.

This user name must have these Db2 privileges:

- For Windows operating systems, the user name must be in the DB2ADMNS group. The default user name is db2admin.
- For AIX or Linux operating systems, the user name must be in the db2iadm1 group. The default user name is db2inst1.

varDBAdmPW=password

Specifies the password that is associated with the Db2 user name.

varDBName=database_name

Specifies the name of the IBM Spectrum Control database. The default database name is TPCDB.

Specify the database name by using the following rules:

• The name can contain the following characters:

- a-z
- A Z
- 0-9
- The name must be 1 8 characters long.

Restriction: The database name cannot have the following conditions:

- Contain a space or a blank.
- Begin with SYS, DBM, or IBM.
- Be the name of an existing database.

varDBPath=database_location, database_location, ...

Specifies the absolute paths for the database.

The database path must follow these rules:

- The path cannot be longer than 242 bytes.
- The path must be an absolute path and not a relative path, for example, C: $\$

You can specify a maximum of 10 database paths and separate them with commas. For example, in the Windows operating system, you would specify C:,D:. In the AIX or Linux operating system, you would specify /home/db2inst1,/testPath.

• For example, on the Windows operating system, if the database is on the C drive, you can add a D drive, an E drive.

On Windows operating systems, you must use double backslashes. For example:

```
C:\\DB2\\TPCDB,D:\\TPCDB,E:\\TPCDB
```

• For example, on the AIX operating system:

/home/db2inst1,/testPath

varDBLogPath=log_location

Specifies the absolute path where the database log files are stored. The default value of the variable is set to <dftdbpath>/<instance name>/<varDBName>/SQLLOG.

For example:

• On Windows operating systems, c:\\DB2\\TPCDB\\SQLLOG

• On AIX operating systems, /home/db2inst1/db2inst1/TPCDB/SQLLOG

Response file parameter for the multiple-server environment

This parameter is valid for the silent_MultipleServer.properties file.

varMultipleServerComponentList=components

Specifies the IBM Spectrum Control components to install.

database

Installs the IBM Spectrum Control database repository.

servers

Installs the Data server, Device server, Alert server, Web server, the Storage Resource agent, CLI, and the IBM Spectrum Control GUI.

Response file parameters for the remote database

The following parameters are used only in the silent_MultipleServer.properties response file to access the IBM Spectrum Control database on a remote server.

Remember: The Db2 database must be installed before you can use these parameters to access the database.

varRemoteDBSrvName=host_name

Specifies the fully qualified host name or IP address of the remote server where the IBM Spectrum Control database repository is installed.

IBM Spectrum Control accepts both IPv4 and IPv6 addresses. If you have a system that is configured for dual stack networking (with both IPv4 and IPv6 addresses), IBM Spectrum Control defaults to IPv4 addressing.

For example, an IPv6 address in long form can be 2001:DB8:0:0:0:0:0:0. An IPv6 address in short form can be 2001:DB8:: or 2001:DB8:0.0.0.0.0.

varRemoteDBPort=port

Specifies the Db2 port on the remote server. The default port is 50000.

varRemoteDBAdmUsr=user_name

Specifies the administrative user name to connect to the remote database. The default user name for the Windows operating system is db2admin. The default user name for the AIX or Linux operating system is db2inst1.

varRemoteDBAdmPW=password

Specifies the password for the user name.

varRemoteDBName=database_name

Specifies the IBM Spectrum Control database on the remote server. The default name is TPCDB.

Related reference

"Ports used by IBM Spectrum Control" on page 25

When you install IBM Spectrum Control, the ports must be opened through the firewall. You must disable the firewall program or open the ports to allow incoming requests to the IBM Spectrum Control ports. Review these ports before you install IBM Spectrum Control.

Installing IBM Spectrum Control in a multiple-server environment

You can install IBM Spectrum Control by using the installation program or by using silent mode from the command line. Note, installing IBM Spectrum Control by using console mode is not supported.

A multiple-server environment is ideal if you are monitoring large storage environments, where one server is not sufficient to manage the IBM Spectrum Control components.

If you have different administrators for Db2 and IBM Spectrum Control, this environment allows the database repository and Db2 to be installed and managed on a separate server.

Installation considerations

When you install IBM Spectrum Control, a database that is called TPCDB is created. In this repository, the IBM Spectrum Control database schema is created, which describes the structure of the database repository. If you already have the TPCDB database on your system, IBM Spectrum Control assigns a new default database repository name with a number as a suffix. For example, TPCDB1.

If the operating system on which you are installing IBM Spectrum Control is sensitive to spaces in directory paths, change the default installation location to not include spaces, for example, C:\apps \IBM\SC.

Related tasks

Installing IBM Spectrum Control with a remote database by using the installation program You can install IBM Spectrum Control in a multiple-server environment by using the installation program.

Installing IBM Spectrum Control with a remote database by using silent mode You can install IBM Spectrum Control in a multiple-server environment by using silent mode.

Installing IBM Spectrum Control with a remote database by using the installation program

You can install IBM Spectrum Control in a multiple-server environment by using the installation program.

For this procedure, the terms *Server A* and *Server B* denote the two servers. If you plan to install IBM Spectrum Control as a non-root user, have your system administrator complete the tasks that are described in <u>"Installing IBM Spectrum Control in a single-server AIX or Linux environment" on page 55</u> on both servers before you begin the installation.

Server A will have Db2 and the IBM Spectrum Control database repository installed. Server B will have the IBM Spectrum Control servers installed.

To install IBM Spectrum Control with a remote database by using the installation program, complete the following steps:

- 1. Complete the following steps on Server A:
 - a) Log on to Server A.

If you are installing on a Windows operating system, log on as a user who has administrator privileges. If you are installing on an AIX or Linux operating system, log on as the root user or as a non-root user who has sudo privileges.

Note: Confirm that your Windows firewalls are disabled in the Control Panel.

b) Install Db2 on Server A.

For more information about installing Db2, see <u>Installing Db2</u>. If you install Db2 on a Windows server, restart the server before you install IBM Spectrum Control.

c) If you logged on as an AIX or Linux non-root user, run the following command in a command shell:

```
sudo DB2_installation_directory/cfg/db2ln
```

For example:

sudo /opt/ibm/db2/V11.5/cfg/db2ln

d) When you install IBM Spectrum Control, the TPCDB database is created in the location that you specify in the Db2 DFTDBPATH variable.

To determine the current DFTDBPATH value, run the following command in a Db2 CLI window:

get dbm cfg

If you want to install this database in a location that is other than the default location:

1) Run the following command in a Db2 CLI window:

update dbm cfg using DFTDBPATH path

where *path* is the new value for the DFTDBPATH variable.

- 2) If you are installing on an AIX or Linux operating system, run the **db2stop** and **db2start** commands to stop and restart Db2.
- e) If you are installing on an AIX or Linux operating system, in a command shell, source the Db2 user profile db2profile for the Db2 instance owner.

For example:

- . /home/db2inst1/sqllib/db2profile
- f) Start the IBM Spectrum Control installation program on Server A.

In a command window or command shell, change the directory to the location of the IBM Spectrum Control installation files and enter the following command:

Windows

setup.bat

AIX or Linux root user

./setup.bin

AIX or Linux non-root user

sudo -E ./setup.bin

- g) On the **Before You Begin** page, because only the IBM Spectrum Control database repository will be installed on Server A, click **Next**.
- h) On the Choose Installation Location and Type page, select Multiple servers and click Next.
- i) On the **Multiple Server Option: Select the Components** page, select **Database repository** and click **Next**.
- j) Follow the prompts in the installation program to install the IBM Spectrum Control database repository on Server A.
- k) After the installation is finished, review the message log on Server A to ensure that no errors occurred.
- 2. Complete the following steps on Server B:
 - a) Log on to Server B.

If you are installing on a Windows operating system, log on as a user who has administrator privileges. If you are installing on an AIX or Linux operating system, log on as the root user or as a non-root user who has sudo privileges.

b) Start the IBM Spectrum Control installation program on Server B.

In a command window or command shell, change the directory to the location of the IBM Spectrum Control installation files and enter the following command:

Windows

setup.bat

AIX or Linux root user

./setup.bin

AIX or Linux non-root user

sudo -E ./setup.bin

- c) On the **Choose Installation Location and Type** page, select **Multiple servers** and click **Next**.
- d) On the **Multiple Server Options: Select the Components** page, select **IBM Spectrum Control Servers** and click **Next**.



Attention: IBM Spectrum Control servers include the following components:

- IBM Spectrum Control GUI
- CLI
- Storage Resource agent
- e) Follow the prompts in the installation program to install the IBM Spectrum Control Servers on Server B.
- f) After the installation program is finished, review the message log on Server B to ensure that no errors occurred.

Related reference

"Planning for IBM Spectrum Control authentication and authorization" on page 17 An operating system user name is required to install and log on to IBM Spectrum Control for the first time. After you install IBM Spectrum Control, you can assign roles to users. Roles determine the product functions that are available to users.

"Installing IBM Spectrum Control in a multiple-server environment" on page 62 You can install IBM Spectrum Control by using the installation program or by using silent mode from the command line. Note, installing IBM Spectrum Control by using console mode is not supported.

"Starting the installation programs" on page 51

There are various methods to start the IBM Spectrum Control installation programs and on various operating systems.

"IBM Spectrum Control components" on page 37

You can install IBM Spectrum Control in single-server or multiple-server environments. In a single-server environment, all components are installed on one server.

"Verifying the installation" on page 75

After you install IBM Spectrum Control, you can verify whether the installation was successful.

"Reviewing the log files to resolve installation issues" on page 77

If an error occurs during IBM Spectrum Control installation, you can review the error log files to resolve issues and continue the installation.

Installing IBM Spectrum Control with a remote database by using silent mode

You can install IBM Spectrum Control in a multiple-server environment by using silent mode.

For this procedure, the terms *Server A* and *Server B* denote the two servers. If you plan to install IBM Spectrum Control as a non-root user, have your system administrator complete the tasks that are described in <u>"Installing IBM Spectrum Control in a single-server AIX or Linux environment" on page 55</u> on both servers before you begin the installation.

If you are installing IBM Spectrum Control in silent mode on a Windows operating system, confirm that your Windows firewalls are disabled in the Control Panel.

Server A will have Db2 and the IBM Spectrum Control database repository installed. Server B will have the IBM Spectrum Control servers installed.

To install IBM Spectrum Control in a multiple-server environment by using silent mode, complete the following steps:

- 1. Complete the following steps on Server A:
 - a) Log on to Server A.

If you are installing on a Windows operating system, log on as a user who has administrator privileges. If you are installing on an AIX or Linux operating system, log on as the root user or as a non-root user who has sudo privileges.

b) Install Db2 on Server A.

For more information about installing Db2, see <u>Installing Db2</u>. If you install Db2 on a Windows server, make sure that you restart the server before you install IBM Spectrum Control.

c) If you logged on as an AIX or Linux non-root user, run the following command in a command shell:

sudo DB2_installation_directory/cfg/db2ln

For example:

sudo /opt/ibm/db2/V11.5/cfg/db2ln

d) When you install IBM Spectrum Control, the TPCDB database is created in the location that you specify in the Db2 DFTDBPATH variable.

To determine the current DFTDBPATH value, run the following command in a Db2 CLI window:

get dbm cfg

If you want to install this database in a location that is other than the default location:

1) Run the following command in a Db2 CLI window:

update dbm cfg using DFTDBPATH path

where *path* is the new value for the DFTDBPATH variable.

- 2) If you are installing on an AIX or Linux operating system, run the **db2stop** and **db2start** commands to stop and restart Db2.
- e) On Server A, set the following parameters in the silent_MultipleServer.properties response file to install the remote database repository.
 - LICENSE_ACCEPTED=true
 - CHOSEN_INSTALL_TYPE="Multiple Server Install"
 - varMultipleServerComponentList=database
 - USER_INSTALL_DIR=option
 - varSrvName=option
 - varDBAdmUsr=user_name
 - varDBAdmPW=password
 - varDBName=database_name
 - varDBPath=database_location
 - varDBLogPath=log_location

For more information about editing the silent_MultipleServer.properties file, see <u>"Editing</u> the response file" on page 58.

- f) Save the response file.
- g) If you are installing on an AIX or Linux operating system, in a command shell, source the Db2 user profile db2profile for the Db2 instance owner.

For example:

```
. /home/db2inst1/sqllib/db2profile
```

- h) Run the silent mode installation program on Server A.
 - For Windows operating systems, run the following command:

```
setup.bat -1 language -i silent -f absolute_path_to_response_file
```

where *language* can be one of the following values:

- Czech cs
- English en
- French fr
- German de

- Hungarian hu
- Italian it
- Japanese ja
- Korean ko
- Polish pl
- Brazilian Portuguese pt_BR
- Russian ru
- Spanish es
- Chinese (Simplified) zh_CN
- Chinese (Traditional) zh_TW

absolute_path_to_response_file is the absolute path to the response file. For example, the following command specifies the language and the path:

setup.bat -l fr -i silent -f c:\TPC\silent_MultipleServer.properties

• For AIX or Linux operating systems, run the following command:

Root user

./setup.bin -1 language -i silent -f /absolute_path_to_response_file

For example, the following command specifies the language and the path:

./setup.bin -l de -i silent -f /TPC/silent_MultipleServer.properties

Non-root user

sudo -E ./setup.bin -l language -i silent -f /absolute_path_to_response_file

For example, the following command specifies the language and the path:

sudo -E ./setup.bin -l de -i silent -f /TPC/silent_MultipleServer.properties

If you do not specify a language or if the language is not specified correctly, the installation program uses the English language as the default.

- i) Monitor the progress of the installation.
 - To view the progress of the silent mode installation on Windows operating systems, check the trace log in the following path:

installation_dir\logs\traceTPCInstall.log

• To view the progress of the silent mode installation on AIX or Linux operating systems, check the trace log in the following path:

installation_dir/logs/traceTPCInstall.log

Tip: If there are preinstallation errors, you can review the lax*out.txt and lax*err.txt files that are in the /tmp and %TEMP% directories.

- 2. Complete the following steps on Server B:
 - a) Log on to Server B.

If you are installing on a Windows operating system, log on as a user who has administrator privileges. If you are installing on an AIX or Linux operating system, log on as the root user or as a non-root user who has sudo privileges.

b) On Server B, set the following parameters in the silent_MultipleServer.properties response file:

- LICENSE_ACCEPTED=true
- CHOSEN_INSTALL_TYPE="Multiple Server Install"
- varMultipleServerComponentList=servers
- USER_INSTALL_DIR=option
- varSrvName=option
- varTPCPortRangeSP=port
- varCommonUsrID=user_name
- varCommonUsrPw=password
- varRemoteDBSrvName=host_name
- varRemoteDBPort=port
- varRemoteDBAdmUsr=user_name
- varRemoteDBAdmPW=password
- varRemoteDBName=database_name

For more information about editing the silent_MultipleServer.properties file, see <u>"Editing</u> the response file" on page 58.

- c) Run the silent mode installation program on Server B.
 - For Windows operating systems, run the following command:

```
setup.bat -1 language -i silent -f absolute_path_to_response_file
```

where *language* can be one of the following values:

- Czech cs
- English en
- French fr
- German de
- Hungarian hu
- Italian it
- Japanese ja
- Korean ko
- Polish pl
- Brazilian Portuguese pt_BR
- Russian ru
- Spanish es
- Chinese (Simplified) zh_CN
- Chinese (Traditional) zh_TW

absolute_path_to_response_file is the absolute path to the response file. For example, the following command specifies the language and the path:

setup.bat -1 fr -i silent -f c:\TPC\silent_MultipleServer.properties

• For AIX or Linux operating systems, run the following command:

Root user

./setup.bin -1 language -i silent -f /absolute_path_to_response_file

For example, the following command specifies the language and the path:

./setup.bin -1 de -i silent -f /TPC/silent_MultipleServer.properties

Non-root user

sudo -E ./setup.bin -l language -i silent -f /absolute_path_to_response_file

For example, the following command specifies the language and the path:

sudo -E ./setup.bin -l de -i silent -f /TPC/silent_MultipleServer.properties

If you do not specify a language or if the language is not specified correctly, the installation program uses the English language as the default.

d) Monitor the progress of the installation.

• To view the progress of the silent mode installation on Windows operating systems, check the trace log in the following path:

```
installation_dir\logs\traceTPCInstall.log
```

• To view the progress of the silent mode installation on AIX or Linux operating systems, check the trace log in the following path:

installation_dir/logs/traceTPCInstall.log

Note: If there are preinstallation errors, you can review the lax*out.txt and lax*err.txt files that are in the /tmp and %TEMP% directories.

Related reference

"Planning for IBM Spectrum Control authentication and authorization" on page 17 An operating system user name is required to install and log on to IBM Spectrum Control for the first time. After you install IBM Spectrum Control, you can assign roles to users. Roles determine the product functions that are available to users.

"Installing IBM Spectrum Control in a multiple-server environment" on page 62 You can install IBM Spectrum Control by using the installation program or by using silent mode from the command line. Note, installing IBM Spectrum Control by using console mode is not supported.

"Starting the installation programs" on page 51

There are various methods to start the IBM Spectrum Control installation programs and on various operating systems.

"IBM Spectrum Control components" on page 37

You can install IBM Spectrum Control in single-server or multiple-server environments. In a single-server environment, all components are installed on one server.

"Verifying the installation" on page 75 After you install IBM Spectrum Control, you can verify whether the installation was successful.

"Reviewing the log files to resolve installation issues" on page 77 If an error occurs during IBM Spectrum Control installation, you can review the error log files to resolve issues and continue the installation.

Accessing IBM Spectrum Control server from a remote computer using Command Line Interface

Accessing client components on a remote computer helps you complete storage management tasks from a computer that does not have a IBM Spectrum Control server that is installed on it.

To access IBM Spectrum Control server on a remote computer, complete the following steps:

1. Go to the client_images subdirectory in the IBM Spectrum Control installation directory.

• On AIX or Linux operating systems, here is an example of a subdirectory:

/opt/IBM/TPC/client_images

• On Windows operating systems, here is an example of a subdirectory:

C:\Program Files\IBM\TPC\client_images

- 2. To create a client image, run one of the following commands for the operating system of the computer on which you want to access the command-line interface (CLI):
 - On AIX or Linux operating systems, run the following command:

```
createClientImage.sh [aix | linux | windows | all]
```

When you include the [aix | linux | windows | all] parameters, you can create AIX, Linux, and Windows client images on a computer that is running AIX or Linux operating systems.

• On Windows operating systems run the following command:

createClientImage.bat [aix | linux | windows | all]

When you include the [aix | linux | windows | all] parameters, you can create AIX, Linux, and Windows client images on a computer that is running AIX and Linux or Windows operating systems.

Tip: Each parameter creates one of the following compressed client image files:

aix

Creates a TPC_CLIENT_AIX.tar image.

linux

```
Creates a TPC_CLIENT_LINUX.zip image.
```

windows

Creates a TPC_CLIENT_WIN.zip image.

all

Creates all of the client images.

- 3. Extract the appropriate compressed file on the remote computer.
 - On AIX operating systems, extract the TPC_CLIENT_AIX.tar file to a folder, for example:

/opt/IBM/TPCClient

• On Linux operating systems, extract the TPC_CLIENT_LINUX.zip file to a folder, for example:

/opt/IBM/TPCClient

• On Windows operating systems, extract the TPC_CLIENT_WIN.zip file to a folder, for example:

c:/Program Files/IBM/TPCClient

4. Ensure that the following directories appear in the folder where you extracted the client image compressed file:

• cli

• jre

The cli folder contains the files to start the IBM Spectrum Control command-line interface and the Replication command-line interface. The jre folder contains other files that are necessary to start the command-line interface.

- 5. To start the IBM Spectrum Control command-line interface, run one of the following commands:
 - On AIX or Linux operating systems:

```
/opt/IBM/TPCClient/cli/tpctool.sh
```

• On Windows operating systems:

```
C:\Program Files\IBM\TPCClient\cli\tpctool.bat
```

Installing IBM Spectrum Control on a Windows domain

You can install IBM Spectrum Control and Db2 by using a Windows domain or a local user account.

Installing Db2 and IBM Spectrum Control by using local user accounts

Prerequisite: If the local user account is used to install the database repository, this account must be a member of the Db2 administrator (DB2ADMNS) group.

To install IBM Spectrum Control and Db2 by using local user account, complete the following steps:

- 1. Install Db2 by using a local user account.
- 2. Log on to the Windows domain computer on which you plan to install IBM Spectrum Control by using a local user account that is a member of the local Administrators group and the local Db2 Administrators (DB2ADMNS) group.
- 3. On the **Single Server Installation Information** page, in the **User name** field, enter a local user account that is a member of local administrator group.

Installing Db2 by using a local user account and IBM Spectrum Control by using a domain user account

Prerequisite: If the local user account is used to install the database repository, this account must be a member of the Db2 administrator (DB2ADMNS) group.

To install Db2 with a local user account and IBM Spectrum Control with a domain user account, complete the following steps:

- 1. Install Db2 by using a local user account.
- 2. Log on to the Windows domain computer on which you plan to install IBM Spectrum Control by using a domain user account that is a member of the local Administrators group and the local Db2 Administrators (DB2ADMNS) group.

This user must have the **Act as part of the operating system** and **Login as a service** permissions set in the security policy.

- 3. On the **Single Server Installation Information** page, in the **User name** field, enter a domain user account (with a Windows domain name prefix) that is a member of the local administrators group.
- 4. Click Configure Database repository.
- 5. On the **Configure the Database Repository** page, enter the Db2 user name **without** a Windows domain name prefix, enter the password for the Db2 user, and click **Validate**.
- 6. When the validation is complete, click **OK** to return to the **Single Server Installation Information** page.

Restriction: If the domain security policy overrides the local security policy, you must set the indicators on the domain controller computer.

Installing Db2 and IBM Spectrum Control by using domain user accounts

Prerequisite: If the domain user account is used to install the database repository, this user account must have Db2 SYSADM authority.

To install IBM Spectrum Control and Db2 by using domain user accounts complete the following steps:

- 1. Install Db2 by using a domain user account.
- 2. Log on to the Windows domain computer on which you plan to install IBM Spectrum Control by using a domain user account that is a member of the local Administrators group and the domain Db2 Administrators (DB2ADMNS) group.

- 3. On the **Single Server Installation Information** page, in the **User name** field, enter a domain user account (with a Windows domain name prefix) that is a member of the local administrators group.
- 4. Click Configure Database repository.
- 5. On the **Configure the Database Repository** page, enter the Db2 user name **without** a Windows domain name prefix, enter the password for the Db2 user, and click **Validate**.
- 6. When the validation is complete, click **OK** to return to the **Single Server Installation Information** page.

Resolving Windows domain prevalidation errors

Adding Windows domain user accounts to a local group, such as Administrator or DB2ADMNS, and later deleting these user accounts from the domain controller computer can cause an error when the account is validated.

When you delete user accounts from the domain controller computer, a reference to the user account is created as a security ID on the computer that is a member of a Windows domain. If these references are not removed, the IBM Spectrum Control installation can fail.

To locate the references that have a security ID, complete these steps:

- 1. On the domain member computer, click **Start > Control Panel > Administrative Tools > Computer Management**. If you are prompted by a **User Account Control** window, click **Yes**.
- 2. In the Computer Management navigation tree view, expand the **Local Users and Groups** node and select **Groups**.
- 3. In the **Name** column, look for a security ID like the following example:

S-1-5-21-337177553-1671989427-887411491-500

4. To remove a reference, select the security ID and click **Delete**.

a. To add the user account back to the group, click Add. The user account now belongs to the group.

When a prevalidation error occurs, depending on the type of user account and the group, error messages might be displayed:

• BPCIN0109E An unexpected error occurred..... For more information, review the log files and see the IBM Knowledge Center.

To resolve this situation, use these steps:

- 1. On the domain controller computer, open **Users and Groups** on the Active Directory.
- 2. Delete all groups from the user account, and then add the groups again.
- 3. Log on to the computer again that is the member of the domain.

You have to add the DB2ADMNS rights to the user account again.

Locate the installation log files, lax*-out.txt and lax*-err.txt, for more details about the root cause of the error message. For example,

name=DB2ADMNS An error occurred while enumerating the groups. The group could be found.

```
• BPCIN0244E An error occurred while enumerating the
local administrator group membership. On the current computer, on
the Properties page of this group, remove the user names that are
displayed with a security ID (SID). An example of a SID is
S-1-5-21-337177553-1671989427-887411491-500 and is used instead
of a user name.
```

• BPCIN0245E An error occurred while enumerating the local DB2 administrator group membership. On the current computer, on the Properties page of this group, remove the user names that are displayed with a security ID (SID). An example of a SID is S-1-5-21-337177553-1671989427-887411491-500 and is used instead of a user name. For more information about these messages, go to IBM Knowledge Center and search for the message number.

In the error message window, click **OK** to resume the installation program or **Quit** to restart the IBM Spectrum Control.

Related reference

"Windows domain and local user accounts" on page 8

When a computer is a member of a Windows domain, you can install IBM Db2 on the local computer or on a computer that is a member of a Windows domain. The installation process creates a local Db2 user account or a domain Db2 user account.

"Adding a computer to the Windows domain" on page 9

Before you can install IBM Spectrum Control in a Windows domain, you must first add the computer on which you plan to install IBM Spectrum Control to the domain.

"Installing Db2 by using a Windows domain user account" on page 10 Before you install IBM Spectrum Control in a Windows domain, you must install Db2 and register the Db2 license key.

<u>"Creating a Windows domain common user account for IBM Spectrum Control" on page 11</u> You must create a Windows domain common user account before you can install IBM Spectrum Control in a Windows domain.

"Granting Db2 SYSADM authority to a Windows domain user account" on page 12 If a Windows domain user account is used to install IBM Spectrum Control, the user account may not have the Db2 SYSADM authority, because Db2 goes to the domain controller computer to list the groups. Before you install IBM Spectrum Control, you must grant the Windows domain user accounts the Db2 SYSADM authority.

Verifying the connection to the domain controller computer by using the Dcdiag tool

Use the Dcdiag command-line tool to help you determine whether the domain controller computer is registered with the domain name server (DNS), whether the controller can be pinged, and whether the controller has Lightweight Directory Access Protocol (LDAP) connectivity.

To install and use the Dcdiag tool, complete the following steps:

- 1. On a computer that is a member of a Windows domain, go to http://www.microsoft.com/en-us/download/details.aspx?id=15326.
- 2. Download the following files to the same location:
 - support.cab
 - suptools.msi
- 3. Run the suptools.msi file.
- 4. Proceed through the installation software and click **Finish** to install the tool.
- 5. In a command prompt window, to run the tool, enter the following command:

DCDIAG /TEST:DNS /V /E /S:domaincontroller

Where *domaincontroller* is the name of the domain controller computer, for example, TPCDomain.

Important: You can run the command only if you are logged in with a Windows domain user name. If you try to run the command when you are logged in with a local user name, the following error message is displayed:

Connecting to directory service on server 10.10.10.10 LDAP bind failed with error 1326, Logon failure: unknown user name or bad password.

When you run the **DCDIAG** command, and you connect to the domain controller computer, the output contains text such as passed test Connectivity. This text is displayed even if text such as

system1.srm.tpc.example.com failed test DNS": Testing server: Default-First-Site-Name\TPCDomain is displayed at the end of the output.

The following output shows that the connection was successful:

Installing IBM Spectrum Control and associated products using minimal space on the Windows C: drive

There might be situations in which you do not want to install Db2 or IBM Spectrum Control on the C: drive.

For example, you might have limited space on the drive. You can install these products on a different drive that meets the space requirements for the products. You can also minimize the space that is used on the C: drive during the installation process by directing temporary files to another drive.

The procedures that are provided apply to installing the products on a single server using the appropriate installation programs. The procedures can be modified to suit different installation scenarios.

Installing Db2

Complete the following steps to install Db2 with minimal space used on the C: drive

- 1. Open a command window and complete the following steps in the same window session:
 - a. At the command prompt, change the directory to the location of the DB2 Setup program setup.exe file.
 - b. Run the following commands to change the TEMP and TMP environment variable settings to the drive and directory where you want to direct the temporary files that are created during the installation of Db2.

Important: The directory that is specified in these commands must be an existing directory. If the directory does not exist, you must create it before you start the installation of Db2.

```
set TEMP=drive_and_directory
set TMP=drive_and_directory
```

For example:

set TEMP=Q:\Temp
set TMP=Q:\Temp

- 2. Start the DB2 Setup program and follow the prompts in the program to complete a typical installation on a drive other than the C: drive. Ensure that you set the correct drive and directory on the following pages:
 - Select the installation folder
 - Select the IBM SSH server installation folder and startup option

After the installation, the files and directories that are related to Db2 use approximately 75 MB of space on the C: drive.

Installing IBM Spectrum Control

Complete the following steps to install IBM Spectrum Control with minimal space used on the C: drive:

1. Open a command window and complete the following steps in the same window session:

- a. At the command prompt, change the directory to the location of the IBM Spectrum Control installation program setup.bat file.
- b. Run the following commands to change the **TEMP** and **TMP** environment variable settings to the drive and directory where you want to direct the temporary files that are created during the installation of IBM Spectrum Control.

Important: The directory that is specified in these commands must be an existing directory. If the directory does not exist, you must create it before you start the installation of IBM Spectrum Control.

```
set TEMP=drive_and_directory
set TMP=drive_and_directory
```

For example:

set TEMP=Q:\Temp
set TMP=Q:\Temp

2. Start the IBM Spectrum Control program and follow the prompts to complete the installation on a drive other than the C: drive.

Ensure that you set the correct drive and directory on the following pages:

- Choose the Installation Location and Type page in the IBM Spectrum Control installation program.
- Configure the Database Repository page in the IBM Spectrum Control installation program.

After the installation, the files and directories that are related to IBM Spectrum Control use approximately 5 MB on the C: drive.

Verifying the installation

After you install IBM Spectrum Control, you can verify whether the installation was successful.

Use the following questions to guide you through the verification process.

Remember the following information when you are verifying the installation:

- You must use a user name with Db2 administrative privileges to run any Db2 commands.
- You must run any Db2 commands on the Db2 command line.

Was the TPCDB database created?

Run the following Db2 command:

db2 list db directory

This command returns information about the TPCDB database.

Are the tables and views present in the TPCDB database?

Run the following Db2 commands:

```
db2 connect to TPCDB
db2 list tables for schema TPC
db2 disconnect TPCDB
```

These commands indicate that you can connect to and disconnect from the IBM Spectrum Control database repository and lists the tables and views in the TPCDB database.

Is the Data server running?

On the Windows operating system:

Go to the Services listing and find IBM Spectrum Control - Data Server.

On the AIX or Linux operating system:

Run the following command:

ps -eaf | grep DataServer.jar

This command returns a list of the Data server processes in the process table.

Is the Device server running?

On the Windows operating system:

- 1. Go to the Services listing and find **IBM Spectrum Control Device Server**.
- 2. In a Windows command window, go to the following directory:

installation_dir\wlp\bin\

where *installation_dir* is the top-level directory in which you installed IBM Spectrum Control (for example, C:\Program Files\IBM\TPC\).

3. Run the following command:

server.bat status deviceServer

This command returns a status of running.

On the AIX or Linux operating system:

1. In a command-line window, go to the following directory:

installation_dir/wlp/bin/

where *installation_dir* is the top-level directory in which you installed IBM Spectrum Control (for example, /opt/IBM/TPC/).

2. Run the following command:

./server status deviceServer

This command returns a status of running.

It can take several minutes after the Device server starts for all services to be running.

Are all Device server services running?

Go to

https://localhost:port/ITSRM/ServiceManager

Where *port* is the value of the WC_defaulthost_secure key in the *installation_dir*/device/ portdef.props file. The default port number is 9551.

Is the Storage Resource agent running?

On the Windows operating system:

Go to the Services window and find IBM Spectrum Control Storage Resource Agent.

On the AIX or Linux operating system:

Run the following command:

ps -eaf | grep Agent

This command returns a list of the Storage Resource agent processes in the process table.

Is the web server running?

On the Windows operating system:

Go to the Services window and find IBM Spectrum Control - Web Server.

On the AIX or Linux operating system:

Run the following command:

ps -eaf | grep webServer

This command returns a list of the web server processes in the process table.

Can I log on to the IBM Spectrum Control GUI?

Open a web browser and enter the following web address:

https://host_name:port/srm

Where *host_name* is the fully qualified host name of the computer where the IBM Spectrum Control Web server is installed and *port* is the value of the httpsPort key in the *installation_dir/wlp/usr/servers/webServer/server.xml* file. The default port is 9569.

Reviewing the log files to resolve installation issues

If an error occurs during IBM Spectrum Control installation, you can review the error log files to resolve issues and continue the installation.

To resolve errors that occur during the preinstall steps in the IBM Spectrum Control installation program, complete the following steps:

- 1. Navigate to one of the following directories:
 - For the Windows operating system, go to %TEMP% directory
 - For the AIX or Linux operating system, go to /tmp directory
- 2. Review the following log files:
 - lax-xxxxxr-out.txt
 - lax-xxxxx-err.txt

Tip: The files are InstallAnywhere log files and are automatically generated. The *xxxxx* are numeric characters that are assigned by the InstallAnywhere software.

To resolve errors after the IBM Spectrum Control installation starts, complete the following steps:

1. Navigate to one of the following default directories:

- For the Windows operating system, go to C:\Program Files\IBM\TPC\logs
- For the AIX or Linux operating system, go to /opt/IBM/TPC/logs
- 2. Review these log files:
 - msgTPCInstall.log
 - traceTPCInstall.log
 - sra\install\agent.trace
 - sra\install\agent_number.log
- 3. For agent log files, navigate to one of the following default directories:
 - For the Windows operating system, go to SRA_location\log
 - For the AIX or Linux operating system, go to SRA_location/log

where SRA_location is where the Storage Resource agent is installed.

If an installation error occurred and you decide to do a partial rollback, the msgTPCInstall.log and traceTPCInstall.log files are updated with additional information when you resume the installation.

Changing languages

You can change the operating system language and web browser that determines the language in which IBM Spectrum Control services and the IBM Spectrum Control GUI are displayed.

For IBM Spectrum Control, the following languages are supported:

- English
- Czech
- French

- German
- Hungarian
- Italian
- Japanese
- Korean
- Polish
- Brazilian Portuguese
- Russian
- Spanish
- Chinese (Simplified)
- Chinese (Traditional)

Changing the language of the IBM Spectrum Control GUI

Change the language that is displayed in your web browser for the IBM Spectrum Control GUI.

1. Choose one of these options to access the settings page in the web browser:

Option	Description	
Mozilla Firefox (ESR 31 and later)	In the menu bar, click Tools > Options .	
Google Chrome	Click the customization control in the upper-right corner of the page and click Settings .	
Internet Explorer (v11 and later)	In the menu bar, click Tools > Internet Options .	

2. Access the language settings in the web browser:

Option	Description
Mozilla Firefox (ESR 31 and later)	Scroll to the Language and Appearance section and click Choose.
Google Chrome	Scroll to the bottom of the Settings page and click Advanced .
Internet Explorer (v11 and later)	In the General tab on the Internet Options page , click Languages .

3. Select the language that you want to display:

Option	Description
Mozilla Firefox (ESR 31 and later)	Select the language that you want to display in the browser and click Move up until it's at the top of the list. Click Ok .
Google Chrome	Scroll to the Languages section, click the action customization next to the language that you want to display, and select Move to the top .
Internet Explorer (v11 and later)	Select the language that you want to display in the browser and click Move up until it's at the top of the list. Click Ok twice to return to the main browser page.

4. Refresh the browser tab where the IBM Spectrum Control GUI is displayed to apply the language setting.

Changing the operating system language for Windows

Change the operating system language for Windows.

To change the operating system language for Windows servers, for example from English to German (de_DE), complete these steps:

1. Choose one of these options:

Option	Description
Windows Server 2012	On the Dashboard page, hover the mouse over the lower left corner of the page next to the Server Manager taskbar button, and then click Start .
Windows Server 2012 R2, Windows Server 2016, Windows Server 2019	Click Start .

- 2. Click Control Panel .
- 3. Click Clock, Language, and Region > Region and Language.

Tip: The exact links that you click might vary between the different versions of Windows. For example, **Region** and **Language** might be separate links in more recent versions of Windows. In those cases, click **Language**.

4. On the Format tab, select a language and click OK.

Tip: The exact links that you click might vary between the different versions of Windows. For example, you might need to click the **Administrative** tab rather than the **Format** tab to change the system locale.

5. Restart all the IBM Spectrum Control services or restart the Windows server.

Changing the operating system language for AIX

Change the operating system language for AIX.

To change the operating system language for AIX systems, for example from English to German (de_DE), complete these steps:

1. At the command prompt, run the following commands:

chlang -m de_DE de_DE export LANG=de_DE

2. Restart all the IBM Spectrum Control services or restart the AIX system.

Adding an installation license

If you installed IBM Spectrum Control and want to add a IBM Spectrum Control license to use additional functions of the software, you can use the installation program or silent-mode installation.

To determine the type of license you have, find these files in the <component_root>/swidtag directory:

ibm.com_IBM_Spectrum_Control_Standard_Edition-*version.swidtag* Indicates that you have a IBM Spectrum Control Standard Edition license.

ibm.com_IBM_Spectrum_Control_Standard_Select_Edition-*version.swidtag* Indicates that you have a IBM Spectrum Control Standard Select Edition license.

- **ibm.com_IBM_Spectrum_Control_Advanced_Edition**-*version*.**swidtag** Indicates that you have a IBM Spectrum Control Advanced Edition license.
- **ibm.com_IBM_Spectrum_Control_Advanced_Select_Edition**-*version.swidtag* Indicates that you have a IBM Spectrum Control Advanced Select Edition license.

Depending on the license you purchased, one of the following license key files can be found in the license\key sub-directory of the electronic image:

nodelock

IBM Spectrum Control Standard Edition license

nodelock.SEL

IBM Spectrum Control Standard Select Edition license

nodelock.AE

IBM Spectrum Control Advanced Edition license

nodelock.AS

IBM Spectrum Control Advanced Select Edition license

Adding an installation license using the installation program

If you installed IBM Spectrum Control and want to add an IBM Spectrum Control license for additional function, you can do so by using the installation program.

To add the license to your system using the installation program, complete the following steps:

- 1. If you are adding a license on the AIX or Linux operating system, source the db2profile.
- 2. Log on to the IBM Spectrum Control system with the appropriate user privileges.
- 3. Start the IBM Spectrum Control installation program.
- 4. On the Choose Installation Location and Type page, select License upgrade and click Next.
- 5. On the Upgrade License page, select which license key file to use and click **Next**.
- 6. Verify the information on the Preinstallation Summary page and click Install.
- 7. On the Installation Completed page, click **Done**.

When the installer upgrades the license, it also stops and restarts the following IBM Spectrum Control servers: Web, Data, and Device.

Related reference

<u>"Planning for IBM Spectrum Control authentication and authorization" on page 17</u> An operating system user name is required to install and log on to IBM Spectrum Control for the first time. After you install IBM Spectrum Control, you can assign roles to users. Roles determine the product

functions that are available to users.

Adding an installation license using silent mode

If you installed IBM Spectrum Control and want to add an IBM Spectrum Control license to access more function, you can do so by using silent-mode installation.

To add the license to your system that uses silent mode, complete the following steps:

- 1. If you are adding a license on the AIX or Linux operating system, source the db2profile.
- 2. Log on to your IBM Spectrum Control system with the appropriate user privileges.
- 3. Modify the following parameters in the silent_SingleServerTypical.properties, silent_SingleServerCustom.properties, or silent_MultipleServer.properties file:
 - CHOSEN_INSTALL_TYPE="License Upgrade"
 - varUseLicenseKeyOnImage=
 - varLicenseKeyFile=

For more information on the parameters in the response file, see <u>"Editing the response file" on page</u> 58.

- 4. Save the appropriate response file.
- 5. Start the IBM Spectrum Control installation program.

For Windows operating system, run the command:

setup.bat -l language -i silent -f absolute_path_to_response_file

For AIX or Linux operating system, run the following command:

/setup.bin -l language -i silent -f absolute_path_to_response_file

6. Stop and restart the IBM Spectrum Control GUI.

Related reference

"Planning for IBM Spectrum Control authentication and authorization" on page 17

An operating system user name is required to install and log on to IBM Spectrum Control for the first time. After you install IBM Spectrum Control, you can assign roles to users. Roles determine the product functions that are available to users.

Installing Storage Resource agents

You can install Storage Resource agents by using the IBM Spectrum Control user interface or a command.

You can select one of the following agent installation scenarios:

- To deploy a Storage Resource agent using the GUI, go to the product documentation at http:// fqz0_r_native_agents.html.
- To install the agent using a command, see <u>"Installing Storage Resource agents by using a command" on page 81</u>.
- To install the agent on a Virtual I/O Server, see <u>"Installing Storage Resource agents on the Virtual I/O Server" on page 84</u>.
- To deploy the agent remotely on the Virtual I/O Server, see <u>"Deploying Storage Resource agents</u> remotely" on page 84.

Restriction:

- You cannot use Storage Resource agents as data sources for switches and fabrics. For Brocade switches, you must use CIM agents. For Cisco switches, you must use SNMP agents.
- Before you install or deploy a Storage Resource agent on a system, you must disable the firewall on that system.
- If you are using IBM PowerHA[®] SystemMirror[®] for AIX, a Storage Resource 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 scan a cluster resource group, you must configure the cluster resource group to have at least one IP address that is accessible from the IBM Spectrum Control server.

To deploy a Storage Resource agent, you must log in as a user with the following authority:

On Windows operating systems

You must have Windows Administrator authority.

On UNIX or Linux operating systems

You must be logged in as the root user.

Installing Storage Resource agents by using a command

You typically install Storage Resource agents by using the IBM Spectrum Control GUI. However, if you must install Storage Resource agents locally, you can do so with limited support.

During this installation method, a return code of zero means that a successful installation occurred and a nonzero return code means that an unsuccessful installation occurred. If you have an unsuccessful installation, you must review the log files to determine the problem.

The **-force** option can be used when you have a Storage Resource agent point to multiple servers. If an agent is installed on one server, 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 installation method, when you enter a directory to install the Storage Resource agent, do not add an ending slash mark (\). For example, do not specify C:\agent1\. This action causes 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 <u>Table 22 on page 82</u> for the required parameters for each protocol.

Table 22. Parameters required 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.	

The Storage Resource Agent image contains the installation images for the Storage Resource agents in the following directory:

DVD_installation_image_location/data/sra/operating_system

See Table 23 on page 82 for the Storage Resource agent installation images.

Table 23. Storage Resource agent installation images		
Operating system	Operating system name	
AIX	aix_power	
HP-UX	hp-ux_itanium	
Linux x86	linux_ix86	
Linux for Power Systems Servers	linux_power	
Linux s390	linux_s390	
Oracle Solaris	solaris_sparc	
Windows	windows	

To install the Storage Resource agents locally, complete the following steps:

1. Go to the installation image location:

cd DVD_installation_image_location

2. Run the following command:

► bin/Agent — -installserverPort — server_secure_port →
-serverIP — server_IP_address — -installLoc — Agent_install_location →
-debug MAX
-agentPort — agent_port — -commtype daemon ->
▶ -userID — user_ID — -password — password — -certFile — certificate_file →
\rightarrow \rightarrow

```
▶ -passphrase — passphrase →
```

Notes:

¹ Parameters when the agent is run as a daemon service.

² Parameters when the agent is run as a non-daemon service. See <u>Table 22 on page 82</u> to determine which parameter is required for each protocol.

³ Parameters when the agent is run as a non-daemon service. See <u>Table 22 on page 82</u> to determine which parameter is required for each protocol.

The parameters are as follows.

-install

Installs the Storage Resource agent.

-force

Forces the agent to be installed. The two different situations in which this parameter must be specified are as follows.

- If an earlier installation failed and there is residue on the system that causes further installations to fail. You must verify that all the parameters that are provided are valid, such as the installation location, port.
- If the agent is already installed from one server and you now must install the agent pointing to another server.

-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 is installed. Enclose the directory name in quotation marks, for example, "C:\Program Files\IBM\TPC_SRA".

-debug MAX

Optional parameter for debugging purposes.

-agentPort agent_port

If the agent is run as a daemon service, the agent port must be specified. The default agent port is 9510.

-commtype daemon

If the agent is run as a daemon service, then this parameter must be specified.

-userID user_ID

For non-daemon service. The user ID defined on the agent system. This user ID is used by the server to connect to the agent system.

-password *password*

For non-daemon service. Password for the user ID.

-certFile "certificate_file"

For non-daemon service. The certificate that is used for SSH communication between the server and agent. This certificate must be stored on the server system. Enclose the directory name in quotation marks, for example, "c:\keys\id_sra".

For information about SSH protocol and SSL protocol certificates, see http://www.ibm.spectrum.sc.doc/fqz0_r_create_certificate_ssh.html and http://www.ibm.com/support/knowledgecenter/sssr93_5.3.7/com.ibm.spectrum.sc.doc/ssr93_5.3.7/com.s

-passphrase *passphrase*

For non-daemon service. The passphrase that is defined for the certificate that is used in SSH communication.

After you install a Storage Resource agent by using a command, you must schedule a probe to collect data about the associated resource. For information about how to schedule a probe, see https://www.ibm.com/support/knowledgecenter/en/SS5R93_5.3.7/com.ibm.spectrum.sc.doc/fqz0_t_creating_probes.html.

Installing Storage Resource agents on the Virtual I/O Server

You can install Storage Resource agents on the Virtual I/O Server.

Local installation

To install the Storage Resource agent on the Virtual I/O Server, complete the following steps:

- 1. Log in to the Virtual I/O Server using the **padmin** user ID.
- 2. Run the following command to set up the AIX environment:

oem_setup_env

3. Change to the directory where the Storage Resource agent installation image is located.

Note: You can either mount the Storage Resource agent installation DVD or FTP to the Storage Resource agent installation image to the padmin home directory.

4. Run the Storage Resource agent installation command. For information about the Storage Resource agent installation command, see <u>"Installing Storage Resource agents by using a command" on page 81</u>.

Deploying Storage Resource agents remotely

You can deploy Storage Resource agents remotely for the Virtual I/O Server from your local workstation.

Remote deployment

To deploy the Storage Resource agent remotely, complete the following steps:

- 1. Enable remote access for the **root** user ID. Follow these steps:
 - a. Connect to the Virtual I/O Server using ssh/telnet with the **padmin** user ID.
 - b. Run the following command to set up the AIX environment:

oem_setup_env

c. Run the following command:

smitty login_user

- d. In the User NAME field, type root and press Enter.
- e. In the User can LOGIN REMOTELY(rsh,tn,rlogin)? field, set the value to true.
- 2. Click Save.
- 3. Create an SSH certificate for the root user ID. For information about creating the SSH certificate for the

root user, go to the IBM Knowledge Center at ^{http://www.ibm.com/support/knowledgecenter/ SS5R93_5.3.7/com.ibm.spectrum.sc.doc/fqz0_t_sra_vio_create_ssh_certificate.html.}

4. Start the remote deployment.

Installing IBM Cognos Analytics

You can install the optional IBM[®] Cognos[®] Analytics 11.0.9 or later reporting tool on one computer, on multiple servers for a distributed installation, or you can expand an existing single computer installation

to another server to improve performance. Cognos Analytics provides an installation program that guides you through the installation process.

Once you have installed Cognos Analytics you can view predefined reports and create custom reports about IBM Spectrum Control. You can access reports from IBM Spectrum Control, and work with the reports in the Cognos Analytics reporting tool.

Installing Cognos Analytics in a single Windows environment

You can install Cognos Analytics in a Microsoft Windows environment by using the Cognos Analytics installation program.

The IBM Cognos Analytics 11.1 or later installation consists of the following components:

- Installer executable file
- Repository .zip file

When you run the installer, you must point to the server repository .zip file.

For Microsoft Windows operating system installations, ensure that you have administrator privileges for the Windows computer you are doing the installation on. Also, ensure that your computer has a TEMP system variable that points to the directory where you want to store temporary files. During installation, files from the disk are temporarily copied to this directory.

- 1. Log in to your Windows computer as a user with administrative privileges.
- 2. Start the Cognos Analytics installer executable file.
- 3. Select the language to use for your installation and click **Next**.
- 4. On the **Repository selection** page, click **Choose**.
- 5. On the **Please Choose a File** page, select the server repository zip file and click **Open**.
- 6. Click Next.
- 7. On the Product Install page, select IBM Cognos Analytics and click Next.
- 8. On the **License Agreement** page, accept the license agreement and click **Next**.
- 9. On the **Location** page, provide your installation location and name of the **Shortcut** folder and click **Next**.

If you want the IBM Cognos Analytics installation to automatically create the installation location for you, click Yes.

10. On the Installation type page, select Custom and click Next.

The Custom option offers full flexibility to select the IBM Cognos Analytics components that you want to install. You might want to customize or integrate Cognos Analytics with third-party software? If so, this option is one you would select.

- 11. On the **Choose components** page, accept the default selections, and click **Next**.
- 12. On the **Pre-Installation Summary** page, review your information for accuracy and click **Install**.

13. When the installation is complete, click **Done**.

Related information

Silent installation, uninstallation, and configuration Uninstall IBM Cognos Analytics on Microsoft Windows operating systems

Installing Cognos Analytics in a single Linux environment

You can install Cognos Analytics in a Linux environment by using the Cognos Analytics installation program. To run the graphical-mode installation program, your computer must support a Java-based graphical user interface.

The IBM Cognos Analytics 11.1 or later installation consists of the following components:

- Installer executable file
- Repository .zip file

When you run the installer, you must point to the server repository .zip file.

For Linux operating system installations, ensure that you are a root user for the computer you are doing the installation on.

Verify that the Cognos Analytics installer executable file has 755 permissions and that the Cognos Analytics repository .zip file has 644 permissions.

You *do not* need to set the **JAVA_HOME** environment variable before you start the IBM Cognos Analytics 11.0.9 or later installation program.

Verify that you have installed the following prerequisite packages on a Linux computer for IBM Cognos Analytics 11.0.9 or later.

The prerequisite packages for Red Hat Enterprise Linux (RHEL) 6 are:

```
glibc-2.12-1.166.el6 or later (both i686 and x86_64 packages)
libstdc++-4.4.7-16.el6 or later (both i686 and x86_64 packages)
nspr-4.9.2-1.el6 or later (both i686 and x86_64 packages)
nss-3.14.0.0-12.el6 or later (both i686 and x86_64 packages)
openmotif-2.3.3-5.el6 or later (both i686 and x86_64 packages)
```

The prerequisite packages for Red Hat Enterprise Linux (RHEL) 7 are:

glibc-2.17-55.el7 or later (both i686 and x86_64 packages) libstdc++-4.8.2-16.el7 or later (both i686 and x86_64 packages) nspr-4.10.2-4.el7 or later (both i686 and x86_64 packages) nss-3.15.4-6.el7 or later (both i686 and x86_64 packages) motif-2.3.4-7.el7 or later (both i686 and x86_64 packages)

For more information, see Software Product Compatibility Reports.

You need to set the correct ulimit values in the /etc/security/limits.conf file for IBM Cognos Analytics Version 11.0.9 or later.

Here is an example of the entries you might need to add to the /etc/security/limits.conf file:

*	soft	nproc	unlimited
*	hard	nproc	unlimited
*	soft	nofile	8192
*	hard	nofile	8192
*	soft	stack	unlimited
*	hard	stack	unlimited

After you set and save your ulimit values, restart your computer and verify the correct ulimit values.

For more information, see Set the ulimit values on UNIX and Linux operating systems .

- 1. Log in to your Linux computer as a root user.
- 2. Start the Cognos Analytics installer executable file.
- 3. Select the language to use for your installation and click **Next**.
- 4. On the **Repository selection** page, click **Choose**.
- 5. On the **Please Choose a File** page, select the server repository zip file and click **Open**.
- 6. Click Next.
- 7. On the Product Install page, select IBM Cognos Analytics and click Next.
- 8. On the License Agreement page, accept the license agreement and click Next.
- 9. On the **Location** page, provide your installation location and click **Next**.

If you want the IBM Cognos Analytics installation to automatically create the installation location for you, click Yes.

- 10. On the **Choose components** page, accept the default selections, and click **Next**.
- 11. On the **Pre-Installation Summary** page, review your information for accuracy and click **Install**.
- 12. When the installation is complete, click **Done**.

Related information

<u>Silent installation, uninstallation, and configuration</u> Uninstall IBM Cognos Analytics on UNIX or Linux operating systems

Installing Cognos Analytics in a single AIX environment

You can install Cognos Analytics in an AIX environment by using the Cognos Analytics installation program. To run the graphical-mode installation program, your computer must support a Java-based graphical user interface.

The IBM Cognos Analytics 11.1 or later installation consists of the following components:

- Installer executable file
- Repository .zip file

When you run the installer, you must point to the server repository .zip file.

For AIX operating system installations, ensure that you are a root user for the computer you are installing on.

Verify that the Cognos Analytics installer executable file has 755 permissions and that the Cognos Analytics repository .zip file has 644 permissions.

You *do not* need to set the **JAVA_HOME** environment variable before you start the IBM Cognos Analytics 11.0.9 or later installation program.

Verify that you have the following prerequisite packages installed on a AIX computer for IBM Cognos Analytics 11.0.9 or later.

The prerequisites for AIX 6.1 are:

- TL7
- SP05 (6100-07-05-1228)
- IBM XL C/C++ for AIX, V12.1 Runtime Environment
- bos.pmapi.lib

The prerequisites for AIX 7.1 are:

- IBM XL C/C++ for AIX, V12.1 Runtime Environment
- bos.pmapi.lib

For more information, see Software Product Compatibility Reports.

You need to set the correct ulimit values in the /etc/security/limits file for IBM Cognos Analytics Version 11.0.9 or later.

Here is an example of the entries you might need to add to the /etc/security/limits file:

default: fsize = -1 core = -1 rss = -1 stack = 16384 nofiles = 8192

After you set and save your ulimit values, restart your computer and verify the correct ulimit values.

For more information, see Set the ulimit values on UNIX and Linux operating systems .

- 1. Log in to your AIX computer as a root user.
- 2. Start the Cognos Analytics installer executable file.
- 3. Select the language to use for your installation and click **Next**.
- 4. On the **Repository selection** page, click **Choose**.
- 5. On the **Please Choose a File** page, select the server repository zip file and click **Open**.

- 6. Click Next.
- 7. On the Product Install page, select IBM Cognos Analytics and click Next.
- 8. On the **License Agreement** page, accept the license agreement and click **Next**.
- 9. On the Location page, provide your installation location and click Next.
 - If you want the IBM Cognos Analytics installation to automatically create the installation location for you, click Yes.
- 10. On the **Choose components** page, accept the default selections, and click **Next**.
- 11. On the Pre-Installation Summary page, review your information for accuracy and click Install.
- 12. When the installation is complete, click **Done**.

Related information

Silent installation, uninstallation, and configuration Uninstall IBM Cognos Analytics on UNIX or Linux operating systems

Configuring IBM Cognos Analytics

After you install the optional IBM[®] Cognos[®] Analytics, to view predefined reports and create custom reports about IBM Spectrum Control, you must copy Db2[®] files, create a content store database, save your configuration settings, and start the services.

Important: The configuration procedures assume that you are going to use Db2 for the Cognos Analytics content store. *It is not required* that the Cognos Analytics content store use Db2. Cognos Analytics supports other database products for the content store.

The IBM Spectrum Control database repository uses Db2. If you do not use Db2 for the content store, you still need to copy the Db2 JDBC driver files into the Cognos Analytics installation location and link the 32-Bit Db2 library file (Linux and AIX only) in order for Cognos Analytics to connect to the IBM Spectrum Control database repository.

A general overview to complete the configuration tasks in order to view predefined reports and create custom reports about IBM Spectrum Control:

- Copying Db2 files and linking Db2 libraries
- · Creating the content store
- Creating a data source
- · Importing pre-defined reports package

Related information

Guidelines for creating the content store Set up database connectivity for the content store database Set Database Connection Properties for the content store

Copying JDBC files for Db2 on Windows

You must copy three JDBC driver files from your Db2[®] installation directory to your Cognos Analytics installation location.

Copy the following Db2 JDBC driver files from the *Db2_installation_dir*java\ directory to the *Cognos_installation_dir*\drivers\ directory:

- db2jcc.jar
- db2jcc_license_cu.jar
- db2jcc4.jar

For more information, see Configuration actions that are critical to the success of your installation.

Copying Db2 files and linking the Db2 library on Linux and AIX

You must copy three JDBC driver files from your Db2[®] installation directory to your Cognos Analytics installation location and then link the Db2 library.

- 1. Copy the following Db2 JDBC driver files from the *Db2_installation_dir/java/* directory to the *Cognos_installation_dir/*drivers/ directory:
 - db2jcc.jar
 - db2jcc_license_cu.jar
 - db2jcc4.jar

For more information, see Configuration actions that are critical to the success of your installation.

2. Enter the following command as the root user:

```
cd Cognos_installation_dir/drivers/
chmod +x db2jcc*.jar
```

3. Enter the following command as the root user:

On the Linux operating system:

ln -s Db2_instance_owner_home directory/sqllib/lib32/libdb2.so Cognos_installation_dir/bin/

On the AIX operating system:

ln -s Db2_instance_owner_home directory/sqllib/lib32/libdb2.a Cognos_installation_dir/bin/

In the IBM Spectrum Control Predefined Reports use Compatibility Query Mode, Cognos Analytics needs to use the 32-Bit Db2 library in order to connect to the IBM Spectrum Control database as a data source.

Creating a content store and starting Cognos Analytics on Windows

The information that you enter in IBM Cognos Configuration for Cognos Analytics is used to generate a script that you use to create the content store database.

- 1. Create the content store for Cognos Analytics.
 - a) From the Windows Start menu, select IBM Cognos Analytics > IBM Cognos Configuration.
 - b) In the **Explorer** window, expand **Data Access** > **Content Manager** and click **Content Store**.
 - c) In the Type property, enter DB2 database.
 - d) In the **Database server and port number** property, enter localhost or the fully qualified domain name of the machine where Db2 is installed.

For example, localhost: 50000 or *FQDN_Of_Your_Machine*: 50000 where 50000 is the default port number that is used by Db2. If you are using a different port number, ensure that you use that value. To determine the port that is used by Db2, examine the **varDBPort** parameter in the *installation_dir*\config\InstallVariable.properties file.

e) In the **User ID and password** property, enter the user name of the owner of the Db2 instance where the content store database will be located and the password that is associated with that user name.

Typically, this user name is *db2admin*. If the user name is a Windows domain user name, enter the user name *without* a Windows domain name prefix or suffix.

- f) In the **Database name** property, verify that the default value is **cm**.
- g) From the **File** menu, click **Save**.
- h) In the **informational** window, click **Close**.
- i) In the **Explorer** window, expand **Data Access** > **Content Manager** and click **Content Store**.
- j) Right-click Content Store and click Generate DDL.
- k) In the informational window, click Close.

I) From the Windows Start menu, select IBM DB2 DB2COPY1 (Default) > DB2 Command Window -Administrator. Then, enter the following command:

db2 -tvf "Cognos_installation_dir\configuration\schemas\content\db2\createDb.sql"

On Windows, add quotes around the directory path if it contains spaces. For example:

db2 -tvf "C:\Program Files\IBM\Cognos\analytics\configuration\schemas\content\db2\createDb.sql"

This process might take a few minutes.

m) From the Actions menu, click Test.

You are testing the connection between content manager and the content store database.

n) In the **informational** window, click **Close**.

For more information, see Generating a script file to create a database for a DB2 content store.

2. Start Cognos Analytics (content manager and application services).

It might take Cognos Analytics a few minutes to start.

- a) In IBM Cognos Configuration, in the **Explorer** window, click **Local Configuration**.
- b) From the Actions menu, click Test.

Tip: If you are not configuring Cognos Analytics to send notifications, you can ignore the testing the mail server connection failure message. If there is a failure related to NIST SP800-131A conformance, click **Details** in the dialog to see more information. The integration between Cognos Analytics and IBM Spectrum Control is not affected by this setting.

- c) From the **Actions** menu, click **Start**.
- 3. Exit IBM Cognos Configuration.

Creating a content store and starting Cognos Analytics on Linux or AIX

The information that you enter in IBM Cognos Configuration for Cognos Analytics is used to generate a script that you use to create the content store database.

- 1. Create the content store for Cognos Analytics.
 - a) Enter the following commands to start IBM Cognos Configuration:

```
cd <Cognos_installation_dir>/bin64/
. /home/db2inst1/sqllib/db2profile
./cogconfig.sh
```

Notice the space between the . and the / in the second command.

Tip:

It's recommended to source-in the db2profile (. /home/db2inst1/sqllib/db2profile) anytime you are going to start IBM Cognos Configuration.

- b) In the **Explorer** window, expand **Data Access** > **Content Manager** and click **Content Store**.
- c) In the **Database server and port number** property, enter localhost or the fully qualified domain name of the computer where Db2 is installed.

For example, localhost: 50000 or *FQDN_Of_Your_Machine*: 50000 where 50000 is the default port number that is used by Db2. If you are using a different port number, ensure that you use that value. To determine the port that is used by Db2, examine the **varDBPort** parameter in the *installation_dir/*config/InstallVariable.properties file.

- d) In the User ID and password property, enter the user name of the owner of the Db2 instance where the content store database is located and the password that is associated with that user name.
- e) In the **Database name** property, verify that the default value is **cm**.
- f) From the **File** menu, click **Save**.

- g) In the Explorer window, go to Data Access > Content Manager and click Content Store.
- h) Right-click Content Store and click Generate DDL.
- i) In the **informational** window, click **Close**.
- j) While you are logged in to the Linux or AIX operating system as the root user, switch to the user that is the Db2 instance owner (for example, db2inst1).
- k) Enter the following Db2 command:

db2 -tvf Cognos_installation_dir/configuration/schemas/content/db2/createDb.sql

If the results of this command contain the following similar messages, you can safely ignore those messages because the Db2 instance owner already has the necessary privileges:

GRANT CREATETAB,BINDADD,CONNECT,IMPLICIT_SCHEMA ON DATABASE TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

GRANT CREATEIN, DROPIN, ALTERIN ON SCHEMA DB2COGNOS TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

GRANT USE OF TABLESPACE TSN_USR_cm TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

GRANT USE OF TABLESPACE TSN_REG_cm TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

- l) Go back to the root user.
- m) From the Actions menu, click Test.

You are testing the connection between Content Manager and the content store database.

n) In the **informational** window, click **Close**.

For more information, see Generating a script file to create a database for a DB2 content store.

- 2. Start Cognos Analytics (Content Manager and application services).
 - a) In IBM Cognos Configuration, in the **Explorer** window, click **Local Configuration**.
 - b) From the Actions menu, click Test.

Tip: If you are not configuring Cognos Analytics to send notifications, you can ignore the testing the mail server connection failure message. If there is a failure related to NIST SP800-131A conformance, click **Details** in the dialog to see more information. The integration between Cognos Analytics and IBM Spectrum Control is not affected by this setting.

- c) From the Actions menu, click Start.
- 3. When Cognos Analytics starts, exit IBM Cognos Configuration.

Creating Cognos Analytics data source for the IBM Spectrum Control database

You can create an IBM Cognos Analytics data source for your IBM Spectrum Control database.

The following table shows the Db2 actions that are required before you create an IBM Cognos Analytics data source for the IBM Spectrum Control database:

Table 24. Required Db2 actions for IBM Spectrum Control/Cognos Analytics integration scenarios		
IBM Spectrum Control - Cognos Analytics integration scenario	Required Db2 actions	
IBM Spectrum Control database and Cognos Analytics on the same Windows or Linux computer	There are no Db2 actions required	
IBM Spectrum Control database and Cognos Analytics on the same AIX computer	Configure the connectivity with the IBM Spectrum Control database to use the loopback mode, or Cognos Analytics will fail to connect to the IBM Spectrum Control database source when running reports multiple times.	
	Complete the following steps on the AIX computer:	
	 Log on to the computer as a user with root privileges 	
	2. Switch to the user that is the Db2 instance owner (for example, <i>db2inst1</i>).	
	3. Run this command:	
	db2 catalog tcpip node loopbk remote 127.0.0.1 server 50000	
	If your Db2 instance uses a different port other than 50000, provide that port value in the command.	
	4. Run this command:	
	db2 catalog database TPCDB as TPCDB_LP at node loopbk	
	If your IBM Spectrum Control database has a name other than TPCDB, provide that database name in the command.	
	If you have upgraded from an earlier version of IBM Spectrum Control, you might find that you already have the loopback connection configured and the above mentioned commands return errors. Confirm the configuration using the 'db2 list database directory' command and look for TPCDB_LP.	

Table 24. Required Db2 actions for IBM Spectrum C (continued)	ontrol/Cognos Analytics integration scenarios
IBM Spectrum Control - Cognos Analytics integration scenario	Required Db2 actions
IBM Spectrum Control database on a different computer than where you installed Cognos Analytics, all platforms	Catalog the node and database for the remote IBM Spectrum Control database.
	Complete the following steps on the computer where you installed Cognos Analytics:
	1. On Windows operating system: Log in as a user with administrative privileges.
	a. On Linux or AIX operating system: Log in as a user with root privileges.
	2. On Windows operating system, from the Start Menu, select IBM DB2 DB2COPY1 (Default) > DB2 Command Window - Administrator.
	a. On Linux or AIX operating system: Switch to the user that is the Db2 instance owner (for example, <i>db2inst1</i>).
	3. Enter the following command to catalog the remote node:
	db2 catalog tcpip node <i>node_name</i> remote <i>server_fqdn</i> server <i>port</i>
	Where <i>node_name</i> is a new value you provide to name the node. For example, remoteSC. The <i>server_fqdn</i> value is the fully qualified domain name of the machine where the IBM Spectrum Control database resides. For example, myserver.mycompany.com. The <i>port</i> value is the port number that is used by Db2. The default value is 50000.
	Example:
	db2 catalog tcpip node remoteSC remote myserver.mycompany.com server 50000
	4. Enter the following command to catalog the remote database:
	db2 catalog database <i>database_name</i> as <i>alias</i> at node <i>node_name</i>
	Where <i>database_name</i> is the name of the IBM Spectrum Control database. Typically, this name is TPCDB. The <i>alias</i> value is a new value that you provide to reference the cataloged database. For example, remDB. The <i>node_name</i> value is the value that you set in Step 3.
	Example:
	db2 catalog database TPCDB as remDB at node remoteSC

Г

٦

To create an Cognos Analytics data source for the IBM Spectrum Control database, complete the following steps:

1. Open a web browser and enter the following URL:

http://FQDN_0f_Your_Machine:9300/bi

Where http is the protocol, and *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*).

- 2. Select Manage > Administration console.
- 3. In the IBM Cognos Administration GUI, select the **Configuration** tab.
- 4. In the **Configuration** tab, select **Data Source Connections**.
- 5. On the toolbar, click the **New Data Source** icon. It is the first icon in the list.
- 6. On the Specify a name and description page, in the Name property, enter TPCDB. You must enter the TPCDB value or the IBM Spectrum Control predefined reports will not generate successfully.
- 7. On the Specify a name and description page, click Next.
- 8. On the **Specify the connection** page, select **IBM DB2** from the **Type** field.
- 9. Verify that Use the default object gateway is selected.
- 10. Unmark Configure JDBC connection and click Next.
- 11. On the **Specify the IBM DB2 connection string** page, in the **DB2 database name** property, complete one of the following steps:
 - a) If the IBM Spectrum Control database is on the same Windows or Linux computer as where you installed Cognos Analytics (first row scenario from Table 1), enter the name of the IBM Spectrum Control database. Typically, this name is TPCDB.
 - b) If the IBM Spectrum Control database is on the same AIX computer as where you installed Cognos Analytics (second row scenario from Table 1), enter the alias value that you created when you cataloged the loopback database. Typically, this value is TPCDB_LP.
 - c) If the IBM Spectrum Control database is on a different computer than where you installed Cognos Analytics (third row scenario from Table 1), enter the *alias* value that you created when you cataloged the remote database. For example, remDB.
- 12. On the Specify the IBM DB2 connection string page, in the Signon section, do the following:
 - a) Verify that **Signons** is selected.
 - b) Select Password.
 - c) In the **User ID** property, enter the user name of the owner of the Db2 instance where the IBM Spectrum Control database is located. On a Window operating system, this user name is typically *db2admin*.

On Linux or AIX operating system, this user name is typically *db2inst1*.

- d) In the **Password** and **Confirm password** properties, enter the password that is associated with the **User ID** property from the previous substep.
- 13. On the **Specify the IBM DB2 connection string** page, in the **Testing** section, click **Test the connection**.
- 14. On the **Test the connection** page, click **Test**.
- 15. When the test is successful, on the **View the results** page, click **Close**.
- 16. On the **Test the connection** page, click **Close**.
- 17. On the **Specify the IBM DB2 connection string** page, click **Next**.
- 18. On the Specify the commands page, click Finish.
- 19. Close your web browser.

Related information

Creating a data source connection

Using Cognos Analytics with multiple remote IBM Spectrum Control databases

You can configure multiple connections within a single Cognos Analytics data source to use Cognos Analytics with multiple remote IBM Spectrum Control databases.

On the machine where you have Cognos Analytics installed, you must catalog the node and the database for each remote IBM Spectrum Control database that you want to query when generating Cognos Analytics reports.

Follow the steps in the *Before you begin* section of <u>"Creating Cognos Analytics data source for the IBM Spectrum Control database" on page 91 to catalog the node and the database for each remote IBM Spectrum Control database. Then, follow the steps in the *Procedure* section of the same topic to create the single data source for the IBM Spectrum Control database and to create the first connection to a specific IBM Spectrum Control database within that data source.</u>

At this point, you will have one data source named TPCDB defined in Cognos Analytics and within that one data source, you will have one connection defined, which is also named TPCDB.

It's assumed that Cognos Analytics is installed on its own machine and that you have multiple IBM Spectrum Control systems installed on separate machines.

To rename the TPCDB connection and to create more connections to other remote IBM Spectrum Control databases within the single data source, complete the following steps:

1. Open a web browser and enter the following URL:

http://FQDN_Of_Your_Machine:9300/bi

Where http is the protocol, and *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*) of the machine where you installed Cognos Analytics.

- 2. Select Manage > Administration console.
- 3. In the IBM Cognos Administration GUI, select the **Configuration** tab.
- 4. In the Configuration tab, select Data Source Connections.
- 5. On the **Data Source Connections** page, click the **TPCDB** data source. This action will drill down one level and you will see the **TPCDB** connection.
- 6. In Actions, click the Set properties TPCDB icon; it's the first icon in the list.
- 7. On the **Set properties TPCDB** page, change the **Name** value from **TPCDB** to a value that reflects the particular IBM Spectrum Control database that this connection uses (for example, *scserv1*).
- 8. Click **OK**.

You are returned to the **Data Source Connections** page and your first data source has been renamed.

- 9. On the **Data Source Connections** page, in the toolbar, click the **New Connection** icon. It's the first icon in the list.
- 10. On the **Specify a name and description New Connection** page, in the **Name** property, enter a value that reflects the particular IBM Spectrum Control database that this connection will use (for example, *myserv2*).
- 11. On the Specify a name and description New Connection page, click Next.
- 12. On the **Specify a name and description New Connection** page, select **IBM Db2** from the **Type** field.
- 13. Verify that **Use the default object gateway** is selected.
- 14. Unmark Configure JDBC connection and click Next.
- 15. On the **Specify the IBM Db2 connection string New Connection** page, in the **DB2 database name** property, enter the *alias* value that you created when you cataloged a particular remote IBM Spectrum Control database.
- 16. On the **Specify the IBM Db2 connection string New Connection** page, in the **Signon** section, do the following:
 - a) Verify that **Signons** is selected.
 - b) Select Password.

- c) In the **User ID** property, enter the user name of the owner of the Db2 instance where the remote IBM Spectrum Control database is located. Note: On a Windows operating system, this user name is typically *db2admin*. On Linux or AIX operating systems, this user name is typically *db2atmin*.
- d) In the **Password** and **Confirm password** properties, enter the password that is associated with the **User ID** value from the previous substep.
- 17. On the **Specify the IBM Db2 connection string New Connection** page, in the **Testing** section, click **Test the connection**.
- 18. Click **Test**.
- 19. When the test is successful, on the View the results page, click Close.
- 20. On the **Test the connection New Connection** page, click **Close**.
- 21. On the Specify the IBM Db2 connection string New Connection page, click Next.
- 22. On the **Specify the commands New Connection** page, click **Finish**.

Your new connection is added to the list of connections defined for the single TPCDB data source. You can repeat Steps 10 - 23 to create a new connection for each remote IBM Spectrum Control database that you want to use when you generate reports. When you have multiple connections defined and you generate a report, you are prompted to select a specific connection to use for that report.

Importing IBM Spectrum Control pre-defined reports package

Complete this procedure to import the IBM Spectrum Control predefined reports package into the IBM Cognos Analytics reporting tool.

- 1. Copy the IBM Spectrum Control predefined reports package TPC_deployment_pckg.zip file from the *installation_dir*\data\gui\ directory, on the machine where you installed IBM Spectrum Control, to the *Cognos_Install_Dir*\deployment\ directory on the machine where you installed Cognos Analytics.
- 2. Import the package into Cognos Analytics.
 - a) Open a web browser and enter the following URL:

http://machine_FQDN:9300/bi

Where *machine_FQDN* is the fully qualified domain name of the machine where you installed Cognos Analytics. For example, *mycognos.mycompany.com*.



Warning: At this point Cognos Analytics is configured with anonymous access so that anyone is able to access it.

- b) Select Manage > Administration console.
- c) In the IBM Cognos Administration GUI, select the **Configuration** tab.
- d) In the **Configuration** tab, select **Content Administration**.
- e) On the toolbar, click the **New Import** icon.
 - It is the fourth icon in the list.
- f) On the Select a deployment archive page, select TPC_deployment_pckg and click Next.
- g) On the **Specify a name and description** page, enter a name for your import and click **Next**.
- h) On the Select the public folders, directory, and library content page, select the following entries:
 - IBM Spectrum Control Packages
 - IBM Spectrum Control Predefined Reports
 - IBM Spectrum Control Report Layouts
- i) Click **Next**.
- j) On the **Specify the general options** page, click **Next**.
- k) On the **Review the summary** page, click **Next**.
- l) On the Select an action page, select Save and run once and click Finish.
m) On the **Run with Options** page, select **Upgrade all report specifications to the latest version** and **Assign new IDs during import**.

For more information, see Run an import.

- n) Click **Run**.
- o) On the **IBM Cognos software** page, select **View the details of this import after closing this dialog** and click **OK**.
- p) On the View run history details page, click Refresh.

Do not log off from the IBM Cognos Administration GUI until the import job is complete.

Important:

The import job might take 15 minutes or more to resolve. Click **Refresh** periodically to check the status.

- q) After the import job is complete, on the View an import deployment record page, click Close.
- r) Exit the IBM Cognos Administration GUI and return to the Cognos Analytics GUI.
- 3. Verify that the imported content is displayed in Cognos Analytics.
 - a) Open a web browser and enter the following URL:

http://machine_FQDN:9300/bi

Where *machine_FQDN* is the fully qualified domain name of the machine where you installed Cognos Analytics. For example, *mycognos.mycompany.com*.

- b) On the IBM Cognos Analytics Welcome page, click Team content.
- c) Verify that the following content is listed:
 - IBM Spectrum Control Packages
 - IBM Spectrum Control Predefined Reports
 - IBM Spectrum Control Report Layouts

Configuring access to the Cognos Analytics reporting tool

Specify which user IDs and groups of user IDs can use reports, report tools, and report administration functions in the Cognos Analytics tool.

You can configure access in the following ways in the Cognos Analytics reporting tool:

- Create user IDs and groups of user IDs so that you can specify access for those users and groups.
- Assign administrative privileges to administrator IDs and remove administrative privileges from other user IDs.
- Specify which user IDs or groups can access individual reports or report folders.
- Specify which user IDs or groups can access individual Cognos Analytics reporting tool functions.

Information about how to configure security for Cognos Analytics is available in the IBM Knowledge Center for Cognos Analytics. Use the following links to view this information:

Table 25. Information about configuring security for Cognos Analytics	
Task	Link to information
Learn about the security model, authorization, and the default Cognos namespace in Cognos Analytics.	Security model
Learn about the initial security settings in Cognos Analytics.	Initial security

Table 25. Information about configuring security for Cognos Analytics (continued)		
Task	Link to information	
Learn about the initial access permissions in Cognos Analytics.	Initial access permissions	
Learn about users, groups, and roles in Cognos Analytics.	Users, Groups, and Roles	
Learn about configuring Cognos Analytics with LDAP authentication.	Configuring authentication providers	
Learn about configuring access permissions in Cognos Analytics.	 Access Permissions and Credentials Set access permissions for an entry 	

Reinstalling the software if a failure occurs

If an installation failure occurs, you do not have to uninstall components that were successfully installed. IBM Spectrum Control provides an option to partially, or fully, roll back the installation.

A full rollback uninstalls all the components (even if they were installed successfully), and a partial rollback uninstalls only the components that were not successfully installed. The partial rollback option helps you resolve the problems that are causing the installation failure. After you resolve the problem, you can install the remaining components. For example, if the correct libraries were not installed for the Linux operating system, and the installation stops. You can install the correct libraries and resume the installation.

If you install IBM Spectrum Control on the Windows operating system and select **Full Rollback**, you must restart the server after the rollback is complete.

If you originally selected a partial rollback, but decided to completely uninstall, you must run the uninstallation program before you reinstall IBM Spectrum Control.

Table 26. Results from a partial rollback	
If an installation failure occurs when you install this component	Partial rollback results are
IBM Spectrum Control common files and Java Runtime Environment	There is no partial rollback. The installation program completes a full rollback.
Database repository	The database repository is uninstalled.
Data server	The Data server is uninstalled.
WebSphere Application Server Liberty profile	WebSphere Application Server Liberty profile is uninstalled.
Alert server	The Alert server is uninstalled.
Device server	The Device server is uninstalled.
Export server	The Export server is uninstalled.
IBM Spectrum Control GUI	The IBM Spectrum Control GUI is uninstalled.

The following table shows the results from a partial rollback. The components are listed in the order in which they were installed.

Table 26. Results from a partial rollback (continued)	
If an installation failure occurs when you install this component	Partial rollback results are
CLI	The command-line interface is uninstalled.
Storage Resource agent	The Storage Resource agent is uninstalled.

Taking the first steps after installation

After IBM Spectrum Control is installed, configure it to monitor the resources in your environment.

Access the IBM Spectrum Control GUI

To configure IBM Spectrum Control for your environment, access the GUI.

For more information about how to start the GUI, see Copening IBM Spectrum Control GUIs and CLIs at http://www.ibm.com/support/knowledgecenter/SS5R93_5.3.7/com.ibm.spectrum.sc.doc/fqz0_t_windows_start_tpc_apps.html.

To set up IBM Spectrum Control for monitoring and managing resources, complete the following tasks:

Add resources for monitoring.

You can add the following resources for monitoring:

- Storage systems
- Servers
- Hypervisors
- Switches
- Fabrics
- NetApp Filers

Configure the retention of data in the database repository

Determine how long that IBM Spectrum Control stores data about the resources that are being monitored.

(Optional) Configure the collection of data about the sizes of GPFS snapshots

By default, IBM Spectrum Control does not collect information about the size of GPFS snapshots. To view that information, you must enable IBM Spectrum Control to collect information about the size of GPFS snapshots.

For information about how to configure collection of snapshot size information, see <u>Collecting</u> information about the sizes of GPFS snapshots.

Configure alert notifications for conditions that are detected on monitored resources

Determining when and how you're alerted to configuration and performance conditions within your storage environment is important to helping you maintain and administer storage resources. Many conditions can trigger alerts. IBM Spectrum Control provides default alert policies for each resource type, or you can configure alert definitions so that IBM Spectrum Control examines the data about your resources for the conditions that you specify.

Specify the users that can access the product and the functions that are available to them

Assign roles to groups of users to determine which functions are available in IBM Spectrum Control. When a user ID is authenticated to IBM Spectrum Control through the GUI, CLI, or APIs, membership in an operating system or LDAP group determines the authorization level of the user.

Deploy Storage Resource agents to set up data features

Deploy Storage Resource agents on servers to enable data collection and to monitor the fabrics that are visible to the server.

Monitor and manage resources

Access the IBM Spectrum Control GUI to monitor and manage your storage, including the following tasks:

- · Monitor the status of resources
- · View capacity and asset information about resources
- Troubleshoot the performance of resources
- · Set performance thresholds and alerts
- View the relationships between resources
- Optimize storage
- Configure for the cloud and storage provisioning
- · Generate detailed reports about resources

Remove the IBM Spectrum Control installation directory from the antivirus scan

Scans that are conducted by antivirus software cause more I/O write operations on the IBM Spectrum Control and server disk drives. For example, the antivirus software can be set to scan any file, record, or process that is written to or read from. The scan includes logs, read/write operations for database records, and Java processes that are used by IBM Spectrum Control. The antivirus software performs write operations on the objects that it identifies with these scans. These additional operations affect product performance and are visible in the performance monitoring tools for the operating system on which the IBM Spectrum Control server is installed. For example, on the Windows operating system, the Reliability and Performance Monitor might show an unusually high number of active write operations for IBM Spectrum Control. To improve performance, update your antivirus software so that it excludes the IBM Spectrum Control installation directory from scans.

For more information about these tasks and how to manage and monitor your resources with IBM

Spectrum Control, go to the product documentation at: http://www.ibm.com/support/knowledgecenter/SS5R93_5.3.7/com.ibm.spectrum.sc.doc/fqz0_c_wg_managing_resources.html.

Chapter 3. Upgrading and migrating

Learn about the key tasks in the upgrade process for IBM Spectrum Control.

The IBM Spectrum Control upgrade process guides you through the steps for upgrading from Tivoli Storage Productivity Center Version 5.2 or later to the current version.

Important: Upgrading the operating system of a server where IBM Spectrum Control is installed is not supported. If you upgrade the operating system of the server, IBM Spectrum Control might be unable to continue monitoring your resources. If you must upgrade the server, contact the IBM Support team for IBM Spectrum Control Support to discuss your options.

Preparing for an upgrade

You can use the following information to help prepare for your upgrade of IBM Spectrum Control. Good planning helps you avoid delays and problems when you upgrade your system.

General considerations

Important: Upgrading the operating system of a server where IBM Spectrum Control is installed is not supported. If you upgrade the operating system of the server, IBM Spectrum Control might be unable to continue monitoring your resources. If you must upgrade the server, contact the IBM Support team for IBM Spectrum Control Support to discuss your options.

Before you upgrade

Consider the following information before you upgrade:

• You cannot upgrade from any release before Tivoli Storage Productivity Center 5.2.0. If you are currently running a version of Tivoli Storage Productivity Center earlier than 5.2.0, you must upgrade

your system to Tivoli Storage Productivity Center 5.2.7.1. For more information, see **IBM Spectrum** Control interoperability matrix. For more information about downloading Tivoli Storage Productivity

Center Version 5.2.7.1, see Latest IBM Spectrum Control downloads. When you are at Tivoli Storage Productivity Center 5.2.7.1, you can upgrade to the highest version of IBM Spectrum Control.

• IBM Spectrum Control no longer supports Tivoli Storage Productivity Center for Replication. It is recommended that your backup your replication environment before you proceed with any upgrade.

See <u>"Backing up a replication environment" on page 106</u> and verify that your replication backup file location is outside of the IBM Spectrum Control installation directory structure or the replication backup file is deleted during the uninstall of replication. IBM Copy Services Manager is the replacement product

for replication. To learn more about how to download and install IBM Copy Services Manager, see 🖙 IBM Copy Services Manager.

• The time and space considerations that are required to upgrade IBM Spectrum Control varies from site to site. Several factors, such as how many devices are being monitored and the version from which you are upgrading, affect the time that is required for the upgrade to complete. In some cases, the upgrade might take up to several hours to complete.

Note, that when you upgrade IBM Spectrum Control, the database repository for metadata is reorganized to include all the latest changes and improvements that are included in the new release. During the upgrade, the database reorganization process might take some time to complete or appear to be frozen. This behavior is typical, especially for larger environments or when you are upgrading from a much older release.

To help ensure that the upgrade and database reorganization complete successfully, make sure that you have enough space on your file system:

- On a Windows operating system: 1 GB - 2 GB on the drive where you installed IBM Spectrum Control.

- On a Linux operating system: 100 MB 300 MB in the /home file system and 1 GB 2 GB in the/ file system.
- On a AIX operating system: 100 MB 300 MB in the /home file system and 1 GB 2 GB in the/opt file system.
- When you do upgrades of IBM Spectrum Control an offline reorganization of tables in the database
 repository occurs. These table reorganizations do not use temporary table space, so you need to
 consider the amount of free disk space you need to have before your upgrade. During an upgrade of IBM
 Spectrum Control, you must have free disk space equivalent to the largest amount of disk space that is
 being used by a single table in the database repository.

To determine the largest amount of disk space that is being used by a single table in the database repository, complete the following tasks on the computer where the IBM Spectrum Control database repository is installed:

- 1. Open a Db2 command prompt or switch to the Db2 instance owner.
- 2. Run the following commands:

```
a. db2 connect to <database name>
b. db2 "select MAX(physical_space) as needed_space from
(select decimal((DATA_OBJECT_P_SIZE+INDEX_OBJECT_P_SIZE+LONG_OBJECT_P_SIZE
+LOB_OBJECT_P_SIZE+XML_OBJECT_P_SIZE+COL_OBJECT_P_SIZE)/1024,10,2)
as physical_space from sysibmadm.admintabinfo where TABSCHEMA='TPC' order by
physical_space desc)"
```

C. db2 disconnect <database name>

where *<database name>* is the name of the IBM Spectrum Control database repository, which is *TPCDB* by default.

Record the result from Step 2b and increase that value by 10 percent; this is the required amount of free disk space in megabytes.

The required free disk space must be available in each file system or drive where the database repository tables are stored.

To determine the file systems or drives where the database repository tables are stored, do the following tasks on the computer where the IBM Spectrum Control database repository is installed:

- 1. Examine the *installation_dir*/config/InstallVariable.properties file.
- 2. Record the value of the following parameters:

DFTDBPATH CSTDBPATH

Each directory that is listed in the previously mentioned values is in a file system (AIX /Linux) or in a drive (Windows). The required free disk space must be available in each file system or drive.

During the upgrade of IBM Spectrum Control, the reorganization of tables in the database repository is logged to the *installation_dir/logs/log/traceInstaller_0.log*. file.

- On Windows operating systems, ensure that all command prompts are closed. If you have open command prompts that have a current working directory in the IBM Spectrum Control installation directory structure, the upgrade might fail in various places because the upgrade process modifies certain directories.
- On Windows operating systems, ensure that the user who logs into the operating system to perform the upgrade of IBM Spectrum Control is an Administrator and does have the *Debug programs* privilege and does *not* have the *Deny access to this computer from the network* privilege in the Windows operating system security policy. These privileges can be found in Administrative Tools -> Local Security Policy
 -> Local Policies -> User Rights Assignment. After the upgrade of IBM Spectrum Control is complete, the required privileges for the user who performed the upgrade can be changed, but only if that user is *not* set as the Common User or the Db2 user in IBM Spectrum Control.

- The full X Window System must be installed to display the IBM Spectrum Control installation program on AIX and Linux operating systems.
- On Windows operating systems, if you installed the IBM Monitoring Agent, stop the Monitoring Agent for Windows OS Primary and Monitoring Agent for Windows OS Watchdog services. After your upgrade is complete, you can start these services again.

Security

Consider the following security information related to upgrades:

- Installing IBM Spectrum Control involves using your operating system in manners typical for installing new application software. If your antivirus software is set on the maximum mode, it might prevent some of your changes from being accepted. To verify that your upgrade completes correctly, enable your antivirus software product to allow the following instances:
 - The /etc/hosts file can be edited
 - Files can be created in the /temp directory
 - New executable files can be created in the C:\Program Files directory.
- If you upgrade Tivoli Storage Productivity Center earlier than 5.2.2 to the current version of IBM Spectrum Control, the SSL certificates that are used by the Data server and Storage Resource agents are not updated automatically to 2048-bit encryption keys.

If you want to use 2048-bit encryption keys after you upgrade to the current version of IBM Spectrum

Control, you must perform the steps in 📴 Replacing default SSL certificates with custom certificates.

• There are new certificate requirements that are strictly enforced for macOS Catalina users that might affect your ability to access the IBM Spectrum Control GUI. During an upgrade of IBM Spectrum Control, certificates self-signed by IBM Spectrum Control will be made automatically compliant. However, if one or more of your certificates are not self-signed by IBM Spectrum Control, see IBM Spectrum Control and macOS Catalina (10.15) Increased Security Policies on SSL Certificates and validate that your certificates are compliant.

After you upgrade

Consider the following information after you upgrade:

- If your upgrade process fails and a component cannot be upgraded, the upgrade process ends and the status of the component is shown as failed. When you start the upgrade process again, the installation program resumes upgrading the failed component.
- If you do a version upgrade of Db2 (examples: 10.5 to 11.1 or 11.1 to 11.5), you must apply a valid license to Db2 following the upgrade.
- After you upgrade to IBM Spectrum Control, all trace settings are reset to the default values. If you changed the trace settings, you must reset the trace settings after an upgrade.

Cognos Analytics

Consider the following information if you use Cognos Analytics 11:

- If you plan to upgrade your Cognos Analytics 11 environment, see <u>How to upgrade your version of</u> <u>Cognos Analytics</u>. After you upgrade IBM Spectrum Control and upgrade your Cognos Analytics 11 environment, you can upgrade the pre-defined reports by importing the pre-defined reports package from the most updated version of IBM Spectrum Control into Cognos Analytics. See <u>"Importing IBM</u> Spectrum Control pre-defined reports package" on page 96.
- After you complete the upgrade of your Cognos Analytics 11 environment on Linux or AIX, verify that the link from the 32-Bit Db2 library to the *Cognos_installation_dir/bin/* directory is still present. If it is not present, perform Step 3 in <u>"Copying Db2 files and linking the Db2 library on Linux</u> and AIX" on page 89.

- When you complete the upgrade of your Cognos Analytics 11 environment, and you save the Cognos Configuration, if you encounter a failure in the **Check password for JVM truststore** step, and it generates the CAM-CRP-1613 error in the Details, see <u>How to regenerate cryptographic keys in Cognos</u> Anaytics 11.
- The IBM Cognos BI Reports component is no longer part of the IBM Spectrum Control product and is uninstalled during the upgrade. It is recommended that you back up your entire IBM Spectrum Control system before you proceed with an upgrade.

If you plan to migrate your custom report content from Tivoli Common Reporting to IBM Cognos

Analytics, see 🖙 <u>"Migrating reports to IBM Cognos Analytics during upgrade" on page 108</u>

Important: After you upgrade IBM Spectrum Control and are using IBM Cognos Analytics, import the

pre-defined reports package into Cognos Analytics. See 🖙 <u>"Importing IBM Spectrum Control pre-</u>defined reports package " on page 96

Considerations before you upgrade from versions of Tivoli Storage Productivity Center, IBM Spectrum Control 5.2.x

Review the following considerations before you upgrade from Tivoli Storage Productivity Center, IBM Spectrum Control Version 5.2.x:

- A direct upgrade from IBM Spectrum Control 5.2.12 to IBM Spectrum Control 5.3.2 or later is not supported. If you are currently at 5.2.12, upgrade to another release earlier than 5.3.2 first and then you will be able to upgrade to the latest version.
- If you upgrade from IBM Spectrum Control 5.2.13 or earlier, the upgrade attempts to migrate the current LDAP configuration and web server keystore contents automatically into the new web server. The overall upgrade proceeds even if these migrations are not successful. After the upgrade completes, if you are unable to log on to IBM Spectrum Control using LDAP credentials, add the LDAP repository to IBM Spectrum Control.

For more information, see Adding an LDAP repository to the federated repositories for IBM Spectrum Control. After the upgrade completes, if your web server SSL certificate is incorrect, replace the default

SSL certificate for the web server. For more information, see 🖙 <u>Replacing the default SSL certificate for</u> the Device, Alert, or Web server.

• If your current IBM Spectrum Control server 5.2.13 or earlier is running in a Windows Domain environment and you *do not* have LDAP authentication that is configured by using the same Active Directory as your Windows Domain, after you upgrade to IBM Spectrum Control 5.2.14 or later, each mapped Domain group that is listed on the User Management page contains the Windows Domain prefix, *domain_name\group_name*.

If your current IBM Spectrum Control server 5.2.13 or earlier is running in a Windows Domain environment, and you *do* have LDAP authentication configured using the same Active Directory as your Windows Domain, after you upgrade to IBM Spectrum Control 5.2.14 or later, each mapped group that is listed on the User Management page has the following entries:

- One entry without the Windows Domain prefix, group_name
- One entry with the Windows Domain prefix, *domain_name*\group_name

Before 5.2.14, IBM Spectrum Control did not properly distinguish between local groups, LDAP groups, and Windows Domain groups. During the upgrade, each group is updated with a second entry to authorize local users, LDAP users and Windows Domain users correctly following the upgrade.

- Do not generate Cognos Business Intelligence reports during the upgrade process.
- If you are upgrading from 5.2.7.1 or earlier, the stand-alone GUI is uninstalled as part of the upgrade process. The stand-alone GUI was removed in 5.2.8 to consolidate the functions of IBM Spectrum Control into a single GUI. Functions of the stand-alone GUI were moved into the web-based GUI, such as the ability to add and monitor vCenter servers and NetApp filers, and the ability to change the hostname or IP address of a resource. However, other functions, such as file system scans, policy management, the topology viewer, database monitoring, and online and batch reporting, are no longer

available in 5.2.8 and later. If you are currently using the stand-alone GUI, ensure that you take a snapshot of your data and set up similar data collection schedules and alerting definitions in the web-based GUI before you upgrade.

- Tivoli Storage Productivity Center for Replication is not delivered with IBM Spectrum Control. Tivoli Storage Productivity Center for Replication is available under the following conditions:
 - In Tivoli Storage Productivity Center 5.2.7.1 or earlier, Tivoli Storage Productivity Center for Replication is automatically available.
 - In IBM Spectrum Control 5.2.8 and through IBM Spectrum Control 5.2.17, Tivoli Storage Productivity Center for Replication is only available if you upgrade from Tivoli Storage Productivity Center 5.2.7.1 or earlier. Maintenance is applied to the existing Tivoli Storage Productivity Center for Replication components if you upgraded from Tivoli Storage Productivity Center to IBM Spectrum Control.
 - Tivoli Storage Productivity Center for Replication gets uninstalled if you upgrade to IBM Spectrum Control 5.3.0 or later.
- If you enabled the legacy connection protocols SSL3 and MD5 hash before the upgrade of IBM Spectrum Control, your SSL3 and MD5 settings are maintained through the upgrade and the same

storage subsystem connections persist after the upgrade. For more information, see **Enabling and** disabling legacy protocols.

Related concepts

Backups

Before you upgrade, you must back up the entire IBM Spectrum Control system.

Related tasks

<u>"Licensing Db2" on page 50</u> You can apply a valid license to Db2 by using the **db21icm** command.

Related reference

"Editing the response file" on page 58

You must edit and save the appropriate response file when you install IBM Spectrum Control by using silent mode. The silent mode installation option for the response file is -f

absolute_path_to_response_file. For example, in the Windows operating system, you enter -f
C:\installimage\silent_SingleServerTypical.properties.

Parameters in the silent_Upgrade.properties file

When you upgrade using the silent mode, use the silent_Upgrade.properties file.

"Planning for installation" on page 1

You can install IBM Spectrum Control by using the installation program or the command line in silent mode. Installing IBM Spectrum Control by using console mode is not supported. Also, upgrading the operating system of a server where IBM Spectrum Control is installed is not supported. If you must upgrade the server, contact the IBM Support team for IBM Spectrum Control Support to discuss your options.

Backups

Before you upgrade, you must back up the entire IBM Spectrum Control system.

The process involves backing up the following parts:

• IBM Spectrum Control database by using Db2 backup utilities.

For more information about backing up your database, see http://www.ibm.com/support/knowledgecenter/SS5R93_5.3.7/com.ibm.spectrum.sc.doc/fqz0_t_backing_up_tpc_database.html.

• The entire IBM Spectrum Control server by using software such as IBM Spectrum Protect.

Tip: The frequency of backups depends on the data protection policies of your company, the IBM Spectrum Control work load, and the size of the IBM Spectrum Control environment. Your backup plan must include documentation with the user names and passwords for Db2 and IBM Spectrum Control.

If you experience problems during the migration, use these backups to restore your original IBM Spectrum Control system and try to migrate again. For more information about restoring the IBM

Spectrum Control database, see https://www.ibm.com/support/knowledgecenter/en/SS5R93_5.3.7/ com.ibm.spectrum.sc.doc/adm_restoring_tpcdb.html.

Restriction:

Do not restore the IBM Spectrum Control database from one version of IBM Spectrum Control into another version. For example, do not restore a backup from IBM Spectrum Control 5.2.14 into 5.2.15, or any other version.

Backing up a replication environment

Before you uninstall Tivoli Storage Productivity Center for Replication, back up your replication environment.

To back up your replication environment, complete these steps:

- 1. Log on to IBM Spectrum Control server with administrative privileges.
- 2. Open a command prompt and change the directory.
 - On a Windows operating system, change the directory to:

installation_dir\cli

• On a AIX or Linux operating system, change the directory to:

installation_dir/cli

- 3. Run a replication CLI script and provide the necessary credentials to access the replication CLI.
 - On a Windows operating system, run the csmcli.bat script.
 - On a AIX or Linux operating system, run the ./csmcli.sh script.
- 4. From the replication CLI, run the **mkbackup** command.
- 5. Note the location of your replication backup file.
- 6. Copy or move the replication backup file to a directory outside of the IBM Spectrum Control installation directory.

Important: If you do not copy or move the backup file location outside of the IBM Spectrum Control installation directory structure, the backup file will get deleted when you uninstall replication.

You successfully performed a backup of your replication environment.

Upgrade to IBM Spectrum Control and uninstall Tivoli Storage Productivity Center for Replication.

Example of upgrading Db2

To complete an upgrade from IBM[®] DB2[®] 10.5 to IBM[®] Db2[®] 11.5, stop the IBM Spectrum Control servers before you begin the upgrade.

You can upgrade to the latest version of Db2[®] that IBM Spectrum Control supports before you install the latest version of IBM Spectrum Control.

Important: The following steps are an example of one way to upgrade from DB2 10.5 to Db2[®] 11.5 on a Windows operating system.

- 1. Stop all of the Windows services for the IBM Spectrum Control servers.
- 2. In a Db2 command window, run the following commands to force all users or applications to disconnect from Db2:

```
db2 force application all
db2 terminate
```

3. In a Db2 command window, run the following command to ensure that no applications are accessing Db2:

db2 list applications

- 4. Create a directory to back up the database. For example: *C*:*downloads**db2_backup*
- 5. In a Db2 command window, run the following command:

db2 BACKUP DATABASE database to C:\downloads\db2_backup

Where *database* is the name of the IBM Spectrum Control database (usually TPCDB).

- 6. Stop all Db2 Windows services and exit Db2 in the Windows System Tray.
- 7. In Windows Explorer, go to the following directory:

C:\Db2_11.5_download_directory\SERVER_DEC\image

Where Db2_11.5_download_directory is where you downloaded the Db2 installation files.

- 8. Double-click the setup.exe file.
- 9. On the DB2 Setup Launchpad navigation tree view, click Install a Product.
- 10. On the Install a Product page, in the DB2 Version 11.5 Server Editions section, click Work with Existing.
- 11. In the Work with an Existing DB2 Copy window, select the DB2 copy for DB2 10.5.
- 12. Click Launch DB2 Setup wizard.
- 13. On the Warning window about upgrading DB2, click OK.
- 14. In the DB2 Setup wizard, complete the following steps:
 - a) On the **Welcome** page, click **Next**.
 - b) On the **Software License Agreement** page, review and accept the license agreement, and click **Next**.
 - c) On the Select the installation type page, select Typical and click Next.
 - d) On the Select the installation, response file creation, or both page, keep the default selection and click **Next**.
 - e) On the Installation folder page, click Next.
 - f) On the Set the DB2 copy name page, click Next.
 - g) On the **Set user information for the default DB2 instance** page, enter the correct user name and password values for the existing DB2 10.5 installation, and click **Next**.
 - h) On the **Enable operating system security for DB2 objects** page, ensure that the settings and values are correct for the existing DB2 10.5 installation, and click **Next**.
 - i) If the Warning window about existing group names is displayed, click OK.
 - j) On the Start copying files and create response file page, click Finish.
 - k) If Warning windows are displayed about a restart that is required to complete the setup, click OK.
 - l) On the Setup is complete page, click Finish.
 - m) In the DB2 First Steps dialog, click **Do not create profile**.
 - n) Close the **DB2 First Steps** window.
- 15. In a **Db2 command** window, run the following command to upgrade the IBM Spectrum Control database to Db2 11.5:

db2 UPGRADE DATABASE database USER user_name USING password

Where *database* is the name of the IBM Spectrum Control database (usually TPCDB), *user_name* is the user who owns the Db2 instance where the database is located (usually db2admin), and *password* is the password that is associated with that user name.

16. Restart your computer and ensure that all of the Windows services for the IBM Spectrum Control servers are started.

Related tasks

<u>"Licensing Db2" on page 50</u> You can apply a valid license to Db2 by using the **db21icm** command.

Related information

Applying fix packs in Db2 database environments Upgrading a DB2 server (Windows) Upgrading a DB2 server (Linux and UNIX)

Migrating reports to IBM Cognos Analytics during upgrade

If you plan to use IBM[®] Cognos[®] Business Intelligence reports in IBM Spectrum Control, you can install IBM[®] Cognos[®] Analytics 11.09 or later and migrate your reports. **If you do not have custom report content, you can skip the migration procedures.**

Important: You no longer need to install Jazz for Service Management and Tivoli[®] Common Reporting with the latest version of IBM Spectrum Control to run reports.

The migration procedures assume that you are going to use Db2 for the Cognos Analytics content store. *It is not required* that the Cognos Analytics content store use Db2. Cognos Analytics supports other database products for the content store.

The IBM Spectrum Control database repository uses Db2. If you do not use Db2 for the content store, you still need to copy the Db2 JDBC driver files into the Cognos Analytics installation location and link the 32-Bit Db2 library file (Linux and AIX only) in order for Cognos Analytics to connect to the IBM Spectrum Control database repository.

High level overview of upgrade and migration tasks for reports

Complete the following high level tasks for an upgrade and migration to view predefined reports and create custom reports about IBM Spectrum Control:

- Export content from Tivoli Common Reporting.
- Upgrade IBM Spectrum Control.
- (Optional) Uninstall Tivoli Common Reporting, Jazz for Service Management, WebSphere Application Server, and Installation Manager.
- Install and configure Cognos Analytics.
- Import content into Cognos Analytics and then verify the content.

Helpful information

The following information will assist you as you go through the procedure for migrating your reports during an upgrade of IBM Spectrum Control.

Table 27. Helpful information to migrate reports during an upgrade	
Product	Information
Jazz for Service Management	Default installation location:
	• Windows:C:\Program Files\IBM\JazzSM\
	 Linux and AIX: /opt/IBM/JazzSM/
	To determine the installation location of Jazz for Service Management in your particular environment, examine the value of the JAZZSM_INSTALL_DIR parameter in the <i>installation_dir</i> \config \InstallVariable.properties file.
	Default user on all operating systems: smadmin
	To determine the Jazz for Service Management user in your particular environment, examine the value of the varJazzSMUsrID parameter in the <i>installation_dir</i> \config\InstallVariable.properties file.
	You will also need to know the password associated with the Jazz for Service Management user.
	Default secure HTTP port on all operating systems: 16311
	To determine the Jazz for Service Management secure HTTP port in your particular environment, examine the value of the varTCRPort parameter in the <i>installation_dir</i> \config \InstallVariable.properties file.
	Default Jazz for Service Management server name to use when you want to stop Jazz for Service Management on all operating systems: server1

Table 27. Helpful information to migrate reports during an upgrade (continued)	
Product	Information
Db2	Default installation location:
	• Windows:C:\Program Files\IBM\SQLLIB\
	• Linux:/opt/ibm/db2/version/
	• AIX:/opt/IBM/db2/version/
	Where <i>version</i> can be 10.1, 10.5 or 11.1
	To determine the installation location of Db2 in your particular environment, examine the value of the varDBPath parameter in the <i>installation_dir</i> \config \InstallVariable.properties file.
	Default Db2 user:
	• Windows: db2admin
	• Linux and AIX: db2inst1
	To determine the Db2 user in your particular environment, examine the value of the varDBAdmUsr parameter in the <i>installation_dir</i> \config \InstallVariable.properties file.
	You will also need to know the password associated with the Db2 user.
	Default port on all operating systems: 50000
	To determine the Db2 port in your particular environment, examine the value of the varDBPort parameter in the <i>installation_dir</i> \config \InstallVariable.properties file.
Cognos Analytics	Default installation location:
	• Windows:C:\Program Files\IBM\cognos\analytics
	 Linux and AIX: /opt/ibm/cognos/analytics/
	Default port on all operating systems: 9300

Video about migrating IBM Spectrum Control custom reports to Cognos Analytics

In the following video, you learn how migrate IBM Spectrum Control custom reports from Cognos Business Intelligence to Cognos Analytics.

Related information

IBM Cognos Analytics - One analytics solution for your entire organization Guidelines for creating the content store Set up database connectivity for the content store database Set Database Connection Properties for the content store

Migrating Cognos BI reports to IBM Cognos Analytics in a single Windows environment

If you do not have custom report content, you can skip this migration procedure. You can upgrade to IBM[®] Cognos[®] Analytics 11.0.9 or later when you upgrade to the latest version of IBM Spectrum Control.

Complete this procedure to migrate your existing custom report content from Tivoli Common Reporting to Cognos Analytics.

Review the content of <u>Migrating reports to IBM Cognos Analytics during upgrade</u> before you start this procedure.

This procedure assumes that you installed Db2[®], IBM Spectrum Control 5.2.15 or earlier, IBM[®]Jazz for Service Management, IBM[®] Tivoli Common Reporting on a single Microsoft[®] Windows[®] computer.

Important: Only reports in the Cognos Analytics Public Folders are exported from Tivoli Common Reporting. If you saved reports to Private Folders or My Folder, you *must* save them again in Public Folders before you export them.

If you plan to upgrade Db2 as part of your upgrade to the latest version of IBM Spectrum Control, upgrade Db2, upgrade the IBM Spectrum Control database (TPCDB) and then upgrade the Tivoli Common Reporting Content Store database (TCRDB).

A high level overview of the migration:

- Export content from Tivoli Common Reporting.
- Upgrade IBM Spectrum Control.
- (Optional) Uninstall Tivoli Common Reporting, Jazz for Service Management, IBM[®] WebSphere[®] Application Server, and Installation Manager.
- Install and configure Cognos Analytics.
- Import content into Cognos Analytics and then verify the content.
 - 1. Log in to Jazz for Service Management and Tivoli Common Reporting to export content.
 - a) Open a web browser and enter the following URL:

https://FQDN_0f_Your_Machine:port/tarf/servlet/dispatch

Where https is the protocol, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*) and the *port* value is the secure HTTP port number that was specified during the installation of Jazz for Service Management.

To determine the secure HTTP port number for Jazz for Service Management, open the JazzSM_installation_dir\profile\properties\portdef.props file. The default JazzSM_installation_dir value is C:\Program Files\IBM\JazzSM. The port number is the value that is assigned to the **WC_defaulthost_secure** parameter. The default value is 16311.

If you receive a security certificate warning when you attempt to connect to the server, confirm the security exception and continue to the web page.

- b) Log in to the reporting interface using the Jazz for Service Management user name that was created when you installed Jazz for Service Management. The default value is smadmin.
- c) Select Launch > IBM Cognos Administration.
- d) In the IBM Cognos Administration GUI, select the **Configuration** tab.
- e) In the Configuration tab, select Content Administration.
- f) On the toolbar, click the New Export icon.

It is the third icon in the list.

- g) On the **Specify a name and description** page, enter a name for your export package and click **Next**.
- h) On the **Choose a deployment method** page, select **Select public folders and directory content** and click **Next**.
- i) On the **Select the public folders content** page, click the **Add** link.
- j) On the **Select entries** page, select the following items to export.
 - Custom content that you saved to Public Folders before running this procedure.
 - IBM Spectrum Control Packages and (or the IBM Tivoli Storage Productivity Center Packages).

- IBM Spectrum Control Predefined Reports and (or the IBM Tivoli Storage Productivity Center Predefined Reports).
- IBM Spectrum Control Report Layouts and (or the IBM Tivoli Storage Productivity Center Report Layouts).
- k) Click the **Green** arrow to transfer the content to the list.
- l) Click **OK**.
- m) On the Select the public folders content page, click Next.

Tip: If you want to export your schedules with your IBM[®] Cognos[®] Business Intelligence content from Tivoli Common Reporting, complete the following steps:

- 1) On the Select the public folders content page, select Include schedules.
- 2) Set Conflict resolution to Replace existing entries.
- 3) Click Next.
- n) On the **Select the directory content** page, select **Include data sources and connections** and **Include signons**.
- o) Set Conflict resolution to Replace existing entries and click Next.
- p) On the **Specify the general options** page, click **Next**.
- q) On the Specify a deployment archive page, click Set the encryption password.
- r) On the **Enter the encryption password** page, enter, and then confirm your password and click **OK**.

Tip: The encryption password is *not* an existing password in IBM Spectrum Control, Db2 or the operating system. The encryption password is a new password for the purpose of securing the content you are exporting from Jazz for Service Management and Tivoli Common Reporting.

Make note of your new password. You will need to provide it later in this procedure.

- s) On the **Specify a deployment archive** page, click **Next**.
- t) On the Review the summary page, click Next.
- u) On the Select an action page, select Save and run once and click Finish.
- v) On the **Run with options** page, click **Run**.
- w) On the **IBM Cognos software** page, select **View the details of this report after closing this dialog** and click **OK**.
- x) On the View run history details page, click Refresh.

Do not log off from the IBM Cognos Administration GUI until the export job is complete. You can click **Refresh** periodically to check the status of the export job.

- y) After the export job is complete, on the **View an export deployment record** page, click **Close**.
- z) Log off from the reporting interface.
- aa) Copy the exported file from the JazzSM_installation_dir\reporting\cognos \deployment\ directory to a directory that is outside of the Jazz for Service Management installation directory.

Make note of the name and location of this exported file. You will need this information in Step 10.

Tip: If you *do not* copy the exported file outside of the Jazz for Service Management installation directory, the exported file is deleted when you uninstall Tivoli Common Reporting.

2. Upgrade your system to latest version of IBM Spectrum Control; this step uninstalls the IBM Spectrum Control Cognos BI Reports component.

For more information, see Upgrading IBM Spectrum Control in a single-server environment.

3. Optional: Uninstall Tivoli Common Reporting, Jazz for Service Management, WebSphere Application Server, and Installation Manager.

For more information, see Uninstalling Tivoli Common Reporting and Jazz for Service Management.

If you *did not* uninstall Tivoli Common Reporting, Jazz for Service Management, WebSphere Application Server, and Installation Manager, you *must* stop Jazz for Service Management and Tivoli Common Reporting before you proceed with the rest of this procedure.

a) To stop Jazz for Service Management and Tivoli Common Reporting, open a command prompt and enter the following command:

```
JazzSM_Installation_dir\profile\bin\stopServer.bat server_name
-username JazzSM_username -password JazzSM_password
```

For example:

```
C:\Program Files\IBM\JazzSM\profile\bin\stopServer.bat server1 -username smadmin -password abc123
```

- b) If you have a Windows Service named IBM WebSphere Application Server V8.5 -JazzSMProfile, you *must* change Startup Type from Automatic to Manual so that Jazz for Service Management and Tivoli Common Reporting do not start when you reboot the computer. For more information, see Accessing administration tools.
- 4. Install IBM Cognos Analytics 11.0.9 or later.
 - a) Log in to your Windows computer as a user with administrative privileges.
 - b) Start the IBM Cognos Analytics installation program.
 - c) Select the language to use for your installation and click **Next**.
 - d) On the **Product installation** page, select **IBM Cognos Analytics (IBM Bundler Edition)** and click **Next**.
 - e) On the License agreement page, accept the license agreement and click Next.
 - f) On the **Location** page, provide your installation location and name of the **Shortcut** folder and click **Next**.

Make note of your Cognos Analytics installation location. You will need to provide it later in this procedure.

Tip: If you want the Cognos Analytics installation to automatically create the installation location for you, click **Yes**.

g) On the Installation type page, select Custom and click Next.

The Custom option offers full flexibility to pick and choose the IBM Cognos Analytics components that you want to install.

- h) On the **Custom install** page, click **Next**.
- i) On the Choose components page, accept the default selections and click Next.
- j) On the **Pre-installation summary** page, review your information for accuracy and click **Install**.

k) When the installation is complete, click **Done**.

5. Copy the following Db2 JDBC driver files from the C:\Program Files\IBM\SQLLIB\java\ directory to the *Cognos_installation_dir*\drivers\ directory:

The Cognos Analytics installation location is what you provided in the previous step.

- db2jcc.jar
- db2jcc_license_cu.jar
- db2jcc4.jar
- 6. Create the content store for Cognos Analytics.
 - a) From the Windows Start menu, select IBM Cognos Analytics > IBM Cognos Configuration.
 - b) In the **Explorer** window, expand **Data Access** > **Content Manager** and click **Content Store**.
 - c) In the Type property, enter DB2 database, if it is not already displayed.
 - d) In the **Database server and port number** property, enter localhost or the fully qualified domain name of the machine.

For example, localhost: 50000 or *FQDN_0f_Your_Machine*: 50000 where 50000 is the default port number that is used by Db2.

Tip: If you are using a different port number, ensure that you use that value. To determine the port that is used by Db2, examine the **varDBPort** parameter in the *installation_dir*\config \InstallVariable.properties file.

e) In the **User ID and password** property, enter the user name of the owner of the Db2 instance where the content store database will be located and the password that is associated with that user name.

Typically, this user name is *db2admin*. If the user name is a Windows domain user name, enter the user name *without* a Windows domain name prefix or suffix.

- f) In the Database name property, verify that the default value is cm.
- g) From the **File** menu, click **Save**.

This step might take a few minutes to complete. Track the progress in the window.

- h) In the **informational** window, click **Close**.
- i) In the Explorer window, expand Data Access > Content Manager and click Content Store.
- j) Right-click Content Store and click Generate DDL.
- k) In the **informational** window, click **Close**.

Important: Do not exit IBM Cognos Configuration in this step. Wait until Step 9.

l) From the Windows Start menu, select IBM DB2 DB2COPY1 (Default) > DB2 Command Window - Administrator. Then, enter the following command:

db2 -tvf "Cognos_installation_dir\configuration\schemas\content\db2\createDb.sql"

On Windows, add quotes around the directory path if it contains spaces. For example:

db2 -tvf "C:\Program Files\IBM\Cognos\analytics\configuration\schemas\content\db2\createDb.sql"

This process might take a few minutes.

m) In IBM Cognos Configuration, from the Actions menu, click Test.

You are testing the connection between content manager and the content store database.

- n) In the **informational** window, click **Close**.
- 7. Optional: You can change the IBM Cognos Analytics ports to match the ports that are used by Jazz for Service Management and Tivoli Common Reporting.

You would do this so that you do not have to get new firewall exceptions for the default Cognos Analytics ports.

- a) While you are still in IBM Cognos Configuration, in the Explorer window, click Environment.
- b) In the **Group Properties** window, select the **Value** next to the **URI** property and change the following properties (names):

Table 28. Group Property values		
Property	Change the value to	
Gateway URI	Computer fully qualified domain name (for	
External dispatcher URI	example, <i>myserver.mycompany.com</i>).	
Internal dispatcher URI	• The https protocol.	
Dispatcher URI for external applications	WC_defaulthost_secure parameter in the	
Content Manager URIs	JazzSM_installation_dir\profile \properties\portdef.props file. The default value is 16311.	

c) From the **File** menu, click **Save**.

- d) In the informational window, click Close.
- 8. Start Cognos Analytics (content manager and application services).

It might take Cognos Analytics a few minutes to start.

- a) While you are still in IBM Cognos Configuration, in the **Explorer** window, click **Local Configuration**.
- b) From the **Actions** menu, click **Test**.

Tip: If you are not configuring Cognos Analytics to send notifications, you can ignore the testing the mail server connection failure message.

- c) In the informational window, click Close.
- d) From the **Actions** menu, click **Start**.

It might take Cognos Analytics a few minutes to start.

- 9. Exit IBM Cognos Configuration.
- 10. Copy the exported file that you created in <u>Step 1</u> to the *Cognos_installation_dir*\deployment \ directory.
- 11. Import content into Cognos Analytics.
 - a) Open a web browser and enter either of the following URLs:

http://FQDN_0f_Your_Machine:port/bi

Or

```
https://FQDN_Of_Your_Machine:port/bi
```

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in <u>Step 7</u> (Optional). If you *did not* perform <u>Step 7</u>, the default port value is 9300.



Warning: At this point Cognos Analytics is configured with anonymous access so that anyone is able to access it.

- b) In the lower left-hand part of the page, select Manage > Administration console.
- c) In the IBM Cognos Administration GUI, select the **Configuration** tab.
- d) In the Configuration tab, select Content Administration.
- e) On the toolbar, click the **New Import** icon.

It is the fourth icon in the list.

- f) On the **Select a deployment archive** page, select the name of the file that you exported from Jazz for Service Management in Step 1 and click **Next**.
- g) On the **Enter the encryption password** page, enter the encryption password that you created in Step 1 and click **OK**.
- h) On the **Specify a name and description** page, enter a name for your import (or keep the default setting) and click **Next**.
- i) On the **Select the public folders, directory, and library content** page, select the following items to import:
 - Custom content that you exported.
 - IBM Spectrum Control Packages and (or the IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or the IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or the IBM Tivoli Storage Productivity Center Report Layouts).
- j) Accept the default settings in the **Options** section and click **Next**.

Tip: If you want to import your schedules with your IBM[®] Cognos[®] Business Intelligence content from Tivoli Common Reporting, complete the following steps:

1) In the **Options** section, verify that **Include schedules** is selected.

2) In the **Options** section, verify that **Conflict resolution** is set to **Replace existing entries**.

3) Click Next.

- k) On the Select directory content page, verify that Include data sources and connections and Include signons are selected and that Conflict resolution is set to Replace existing entries and click Next.
- l) On the **Specify the general options** page, click **Next**.
- m) On the Review the summary page, click Next.
- n) On the Select an action page, select Save and run once and click Finish.
- o) On the **Run with Options** page, select **Upgrade all report specifications to the latest version** and **Assign new IDs during import**.
- p) Click Run.
- q) On the IBM Cognos software page, select View the details of this import after closing this dialog and click OK.
- r) On the View run history details page, click Refresh.

Check the **Status** field to monitor that the job is executing. Do *not* log off from the IBM Cognos Administration GUI until the import job is complete.

Tip: The import job might take approximately 15 minutes or more to resolve. Click **Refresh** periodically to check the status.

The results of importing the reports and schedules into Cognos Analytics contain the following similar messages:

```
CM-REQ-4328 A problem was encountered while importing the object
"/content/folder[@name="IBM Spectrum Control Predefined Reports"]/
folder[@name="Servers"]/report[@name="Servers Capacity"]/schedule".
CM-REQ-4329 The following references cannot be resolved and were cleared:
"credential: CAMID("VMMProvider:smadmin")/credential[@name='Credential '] "
CM-REQ-4328 A problem was encountered while importing the object
"/content/folder[@name="IBM Spectrum Control Predefined Reports"]/
folder[@name="Servers"]/report[@name="Servers Capacity"]/
schedule[@name="Servers"]/report[@name="Servers Capacity"]/
schedule[@name="2018-04-27T18:03:22.638Z"]".
CM-REQ-3282 The schedule will not run because the credential is missing.
```

You can safely ignore the messages as they are expected.

- s) After the import job is complete, check the **Completion time** and **Status** fields to verify that the job is complete. If it is complete, on the **View an import deployment record** page, click **Close**.
- t) To exit the IBM Cognos Administration GUI, close the browser tab.
- 12. Verify that the imported content is displayed in Cognos Analytics.
 - a) Return to the browser tab where the Cognos Analytics GUI is running. If it is not running, open a web browser and enter either of the following URLs:

http://FQDN_Of_Your_Machine:port/bi

Or

https://FQDN_Of_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in <u>Step 7</u> (Optional).

If you did perform <u>Step 7</u>, then you will use https. If you *did not* perform Step 7, then you use http.

If you *did not* perform Step 7, the default port value is 9300.

b) On the IBM Cognos Analytics Welcome page, click Team content.

- c) Verify that the following content is listed:
 - Custom content that you saved to Public Folders before you ran this procedure.
 - IBM Spectrum Control Packages and (or IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or IBM Tivoli Storage Productivity Center Report Layouts).
- d) Optional: Attempt to generate a custom report or a predefined report and verify the contents.

Important: If you encounter APAR IT23800 or other problems when generating a predefined report in Cognos Analytics that was migrated from Tivoli Common Reporting, import the predefined reports package for the version of IBM Spectrum Control you are currently running on your system.

If you encounter APAR IT23800 or other problems when generating a custom report in Cognos Analytics that was migrated from Tivoli Common Reporting, you must update or recreate the custom report to use the predefined reports package for the version of IBM Spectrum Control you are currently running and remove references to tables that are no longer used in the IBM Spectrum Control database repository.

13. After you import the report content and schedules into Cognos Analytics, the schedules will not run due to missing credentials.

To update the schedules in Cognos Analytics with the correct credentials, complete the following steps:

a. Return to the browser tab where the Cognos Analytics GUI is running. If it is not running, open a web browser and enter either of the following URLs:

http://FQDN_0f_Your_Machine:port/bi

Or

https://FQDN_Of_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 7 (Optional).

If you did perform <u>Step 7</u>, then you will use https. If you *did not* perform Step 7, then you use http.

If you *did not* perform Step 7, the default port value is 9300.

- b. On the IBM Cognos Analytics Welcome page, click Team content.
- c. Select a report that has an existing schedule.
- d. Select the **Properties** for the report.
- e. Select the **Schedule** tab.
- f. Select the > icon to open the schedule.
- g. Click **Update** on the schedule page.

Repeat steps c-g for each migrated report schedule you want to run in Cognos Analytics.

You migrated your custom IBM[®] Cognos[®] Business Intelligence reports and upgraded to the latest version of IBM Spectrum Control and are able to use Cognos[®] BI reports.

Change the configuration of Cognos Analytics from anonymous access to authenticated access.

For more information, see Configuring an LDAP namespace for IBM Directory Server.

For more information, see Configuring an LDAP namespace for Active Directory Server.

For more information, see Managing user authentication.

Related tasks

"Importing IBM Spectrum Control pre-defined reports package " on page 96 Complete this procedure to import the IBM Spectrum Control predefined reports package into the IBM Cognos Analytics reporting tool.

Related information

APAR IT23800 Upgrading Db2 servers Upgrading a Db2 server (Windows) IBM Cognos Analytics server components Install and configure server components Installing server components on Windows operating system Installing Content Manager on Windows operating system Installing the Application services components on Windows operating system

Migrating Cognos BI reports to IBM Cognos Analytics in a multiple-server Windows environment with a remote database

If you do not have custom report content, you can skip this migration procedure. You can upgrade to IBM[®] Cognos[®] Analytics 11.0.9 or later when you upgrade to the latest version of IBM Spectrum Control. Complete this procedure in a multiple server environment to migrate your existing custom report content from Tivoli Common Reporting to Cognos Analytics.

Review the content of <u>Migrating reports to IBM Cognos Analytics during upgrade</u> before you start this procedure.

For this procedure, the terms *Server A* and *Server B* denote the two servers. *Server A* has DB2[®] Enterprise Server Edition and the IBM Spectrum Control database repository installed. *Server B* has all of the other IBM Spectrum Control components installed and DB2[®] Enterprise Server Edition, Jazz for Service Management, and Tivoli Common Reporting.

Important: Only reports in the Cognos Analytics Public Folders are exported from Tivoli Common Reporting. If you saved reports to Private Folders or My Folder, you *must* save them again in Public Folders before you export them.

If you plan to upgrade Db2 as part of your upgrade to the latest version of IBM Spectrum Control, upgrade Db2 on *Server A*, upgrade the IBM Spectrum Control database (TPCDB) on *Server A*, upgrade Db2 on *Server B* and then upgrade the Tivoli Common Reporting Content Store database (TCRDB) on *Server B*.

A high level overview on completing this upgrade:

- Export content from Tivoli Common Reporting on Server B.
- Upgrade IBM Spectrum Control on Server A.
- Upgrade IBM Spectrum Control on Server B.
- (Optional) Uninstall Tivoli Common Reporting, Jazz for Service Management, IBM[®] WebSphere[®] Application Server, and Installation Manager, from *Server B*.
- Install and configure Cognos Analytics on Server B.
- Import content into Cognos Analytics on Server B and then verify the content.
 - 1. Log in to Jazz for Service Management and Tivoli Common Reporting on Server B to export content.
 - a) Open a web browser and enter the following URL:

https://FQDN_Of_Your_Machine:port/tarf/servlet/dispatch

Where https is the protocol, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*) and the *port* value is the secure HTTP port number that was specified during the installation of Jazz for Service Management.

To determine the secure HTTP port number for Jazz for Service Management, open the JazzSM_installation_dir\profile\properties\portdef.props file. The default JazzSM_installation_dir value is C:\Program Files\IBM\JazzSM. The port number is the value that is assigned to the **WC_defaulthost_secure** parameter. The default value is 16311.

If you receive a security certificate warning when you attempt to connect to the server, confirm the security exception and continue to the web page.

- b) Log in to the reporting interface using the Jazz for Service Management user name that was created when you installed Jazz for Service Management. The default value is smadmin.
- c) Select Launch > IBM Cognos Administration.
- d) In the IBM Cognos Administration GUI, select the **Configuration** tab.
- e) In the **Configuration** tab, select **Content Administration**.
- f) On the toolbar, click the New Export icon.It is the third icon in the list.
- g) On the **Specify a name and description** page, enter a name for your export package and click **Next**.
- h) On the **Choose a deployment method** page, select **Select public folders and directory content** and click **Next**.
- i) On the Select the public folders content page, click the Add link.
- j) On the Select entries page, select the following items to export.
 - Custom content that you saved to Public Folders before running this procedure.
 - IBM Spectrum Control Packages and (or the IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or the IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or the IBM Tivoli Storage Productivity Center Report Layouts).
- k) Click the **Green** arrow to transfer the content to the list.
- l) Click **OK**.
- m) On the Select the public folders content page, click Next.

Tip: If you want to export your schedules with your IBM[®] Cognos[®] Business Intelligence content from Tivoli Common Reporting, complete the following steps:

- 1) On the Select the public folders content page, select Include schedules.
- 2) Set Conflict resolution to Replace existing entries.
- 3) Click Next.
- n) On the **Select the directory content** page, select **Include data sources and connections** and **Include signons**.
- o) Set **Conflict resolution** to **Replace existing entries** and click **Next**.
- p) On the **Specify the general options** page, click **Next**.
- q) On the Specify a deployment archive page, click Set the encryption password.
- r) On the **Enter the encryption password** page, enter, and then confirm your password and click **OK**.

Tip: The encryption password is *not* an existing password in IBM Spectrum Control, Db2 or the operating system. The encryption password is a new password for the purpose of securing the content you are exporting from Jazz for Service Management and Tivoli Common Reporting.

Make note of your new password. You will need to provide it later in this procedure.

- s) On the Specify a deployment archive page, click Next.
- t) On the **Review the summary** page, click **Next**.

- u) On the Select an action page, select Save and run once and click Finish.
- v) On the **Run with options** page, click **Run**.
- w) On the **IBM Cognos software** page, select **View the details of this report after closing this dialog** and click **OK**.
- x) On the **View run history details** page, click **Refresh**.

Do not log off from the IBM Cognos Administration GUI until the export job is complete. You can click **Refresh** periodically to check the status of the export job.

- y) After the export job is complete, on the **View an export deployment record** page, click **Close**.
- z) Log off from the reporting interface.
- aa) Copy the exported file from the *JazzSM_installation_dir*\reporting\cognos \deployment\ directory to a directory that is outside of the Jazz for Service Management installation directory.

Make note of the name and location of this exported file. You will need this information in Step 11.

Tip: If you *do not* copy the exported file outside of the Jazz for Service Management installation directory, the exported file is deleted when you uninstall Tivoli Common Reporting.

2. Upgrade Server A to the latest version of IBM Spectrum Control.

For more information, see Upgrading from Tivoli Storage Productivity Center Version 5.2.0 and later with a remote database by using the installation program.

- 3. Upgrade *Server B* to the latest version of IBM Spectrum Control. For more information, see <u>Upgrading from Tivoli Storage Productivity Center Version 5.2.0 and later</u> with a remote database by using the installation program.
- 4. Optional: Uninstall Tivoli Common Reporting, Jazz for Service Management, WebSphere Application Server, and Installation Manager from *Server B*.

For more information, see Uninstalling Tivoli Common Reporting and Jazz for Service Management.

If you *did not* uninstall Tivoli Common Reporting, Jazz for Service Management, WebSphere Application Server, and Installation Manager, you *must* stop Jazz for Service Management and Tivoli Common Reporting before you proceed with the rest of this procedure.

a) To stop Jazz for Service Management and Tivoli Common Reporting, open a command prompt and enter the following command:

```
JazzSM_Installation_dir\profile\bin\stopServer.bat server_name
-username JazzSM_username -password JazzSM_password
```

For example:

```
C:\Program Files\IBM\JazzSM\profile\bin\stopServer.bat server1 -username smadmin -password abc123
```

b) If you have a Windows Service named IBM WebSphere Application Server V8.5 -JazzSMProfile, you must change Startup Type from Automatic to Manual so that Jazz for Service Management and Tivoli Common Reporting do not start when you reboot the computer.

For more information, see <u>Accessing administration tools</u>.

- 5. Install IBM Cognos Analytics 11.0.9 or later on Server B.
 - a) Log in to your Windows computer as a user with administrative privileges.
 - b) Start the IBM Cognos Analytics installation program.
 - c) Select the language to use for your installation and click Next.
 - d) On the **Product installation** page, select **IBM Cognos Analytics (IBM Bundler Edition)** and click **Next**.
 - e) On the License agreement page, accept the license agreement and click Next.
 - f) On the **Location** page, provide your installation location and name of the **Shortcut** folder and click **Next**.

Make note of your Cognos Analytics installation location. You will need to provide it later in this procedure.

Tip: If you want the Cognos Analytics installation to automatically create the installation location for you, click **Yes**.

g) On the Installation type page, select Custom and click Next.

The Custom option offers full flexibility to pick and choose the IBM Cognos Analytics components that you want to install.

- h) On the **Custom install** page, click **Next**.
- i) On the **Choose components** page, accept the default selections and click **Next**.
- j) On the **Pre-installation summary** page, review your information for accuracy and click **Install**.
- k) When the installation is complete, click **Done**.
- 6. On *Server B*, copy the following Db2 JDBC driver files from the C:\Program Files\IBM\SQLLIB \java\ directory to the *Cognos_installation_dir*\drivers\ directory:

The Cognos Analytics installation location is what you provided in the previous step.

- db2jcc.jar
- db2jcc_license_cu.jar
- db2jcc4.jar
- 7. Create the content store for Cognos Analytics on Server B.
 - a) From the Windows Start menu, select IBM Cognos Analytics > IBM Cognos Configuration.
 - b) In the **Explorer** window, expand **Data Access** > **Content Manager** and click **Content Store**.
 - c) In the **Type** property, enter **DB2 database**, if it is not already displayed.
 - d) In the **Database server and port number** property, enter localhost or the fully qualified domain name of the machine.

For example, localhost: 50000 or *FQDN_Of_Your_Machine*: 50000 where 50000 is the default port number that is used by Db2.

Tip: If you are using a different port number, ensure that you use that value. To determine the port that is used by Db2, examine the **varDBPort** parameter in the SC_installation_dir\config \InstallVariable.properties file.

e) In the **User ID and password** property, enter the user name of the owner of the Db2 instance where the content store database will be located and the password that is associated with that user name.

Typically, this user name is *db2admin*. If the user name is a Windows domain user name, enter the user name *without* a Windows domain name prefix or suffix.

- f) In the **Database name** property, verify that the default value is **cm**.
- g) From the **File** menu, click **Save**.

This step might take a few minutes to complete. Track the progress in the window.

- h) In the informational window, click Close.
- i) In the **Explorer** window, expand **Data Access** > **Content Manager** and click **Content Store**.
- j) Right-click Content Store and click Generate DDL.
- k) In the **informational** window, click **Close**.

Important: Do not exit IBM Cognos Configuration in this step. Wait until Step 10.

l) From the Windows Start menu, select IBM DB2 DB2COPY1 (Default) > DB2 Command Window - Administrator. Then, enter the following command:

db2 -tvf "Cognos_installation_dir\configuration\schemas\content\db2\createDb.sql"

On Windows, add quotes around the directory path if it contains spaces. For example:

db2 -tvf "C:\Program Files\IBM\Cognos\analytics\configuration\schemas\content\db2\createDb.sql"

This process might take a few minutes.

m) In IBM Cognos Configuration, from the Actions menu, click Test.

You are testing the connection between content manager and the content store database.

- n) In the **informational** window, click **Close**.
- 8. Optional: On *Server B*, you can change the IBM Cognos Analytics ports to match the ports that are used by Jazz for Service Management and Tivoli Common Reporting.

You would do this so that you do not have to get new firewall exceptions for the default Cognos Analytics ports.

- a) While you are still in IBM Cognos Configuration, in the **Explorer** window, click **Environment**.
- b) In the **Group Properties** window, select the **Value** next to the **URI** property and change the following properties (names):

Table 29. Group Property values		
Property	Change the value to	
Gateway URI	• Computer fully qualified domain name (for	
External dispatcher URI	example, <i>myserver.mycompany.com</i>).	
Internal dispatcher URI	• The https protocol.	
Dispatcher URI for external applications	WC_defaulthost_secure parameter in the	
Content Manager URIs	JazzSM_installation_dir\profile \properties\portdef.props file. The default value is 16311.	

- c) From the File menu, click Save.
- d) In the **informational** window, click **Close**.
- 9. Start IBM Cognos Analytics (content manager and application services), on Server B.

It might take Cognos Analytics a few minutes to start.

- a) While you are still in IBM Cognos Configuration, in the **Explorer** window, click **Local Configuration**.
- b) From the **Actions** menu, click **Test**.

Tip: If you are not configuring Cognos Analytics to send notifications, you can ignore the testing the mail server connection failure message.

- c) In the informational window, click Close.
- d) From the Actions menu, click Start.

It might take Cognos Analytics a few minutes to start.

- 10. Exit IBM Cognos Configuration, on Server B.
- 11. On *Server B*, copy the exported file that you created in Step 1 to the *Cognos_installation_dir* \deployment\ directory.
- 12. Import content into Cognos Analytics on Server B.
 - a) Open a web browser and enter either of the following URLs:

http://FQDN_0f_Your_Machine:port/bi

Or

https://FQDN_Of_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 8 (Optional). If you *did not* perform Step 8, the default port value is 9300.



Warning: At this point Cognos Analytics is configured with anonymous access so that anyone is able to access it.

- b) In the lower left-hand part of the page, select Manage > Administration console.
- c) In the IBM Cognos Administration GUI, select the **Configuration** tab.
- d) In the **Configuration** tab, select **Content Administration**.
- e) On the toolbar, click the **New Import** icon.

It is the fourth icon in the list.

- f) On the **Select a deployment archive** page, select the name of the file that you exported from Jazz for Service Management in Step 1 and click **Next**.
- g) On the **Enter the encryption password** page, enter the encryption password that you created in Step 1 and click **OK**.
- h) On the **Specify a name and description** page, enter a name for your import (or keep the default setting) and click **Next**.
- i) On the **Select the public folders, directory, and library content** page, select the following items to import:
 - Custom content that you exported.
 - IBM Spectrum Control Packages and (or the IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or the IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or the IBM Tivoli Storage Productivity Center Report Layouts).
- j) Accept the default settings in the **Options** section and click **Next**.

Tip: If you want to import your schedules with your IBM[®] Cognos[®] Business Intelligence content from Tivoli Common Reporting, complete the following steps:

- 1) In the **Options** section, verify that **Include schedules** is selected.
- 2) In the **Options** section, verify that **Conflict resolution** is set to **Replace existing entries**.
- 3) Click Next.
- k) On the Select directory content page, verify that Include data sources and connections and Include signons are selected and that Conflict resolution is set to Replace existing entries and click Next.
- l) On the **Specify the general options** page, click **Next**.
- m) On the **Review the summary** page, click **Next**.
- n) On the Select an action page, select Save and run once and click Finish.
- o) On the **Run with Options** page, select **Upgrade all report specifications to the latest version** and **Assign new IDs during import**.
- p) Click Run.
- q) On the **IBM Cognos software** page, select **View the details of this import after closing this dialog** and click **OK**.
- r) On the View run history details page, click Refresh.

Check the **Status** field to monitor that the job is executing. Do *not* log off from the IBM Cognos Administration GUI until the import job is complete.

Tip: The import job might take approximately 15 minutes or more to resolve. Click **Refresh** periodically to check the status.

The results of importing the reports and schedules into Cognos Analytics contain the following similar messages:

CM-REQ-4328 A problem was encountered while importing the object "/content/folder[@name="IBM Spectrum Control Predefined Reports"]/ folder[@name="Servers"]/report[@name="Servers Capacity"]/schedule". CM-REQ-4329 The following references cannot be resolved and were cleared: "credential: CAMID("VMMProvider:smadmin")/credential[@name='Credential '] ". CM-REQ-4328 A problem was encountered while importing the object

CM-REQ-4328 A problem was encountered while importing the object "/content/folder[@name="IBM Spectrum Control Predefined Reports"]/ folder[@name="Servers"]/report[@name="Servers Capacity"]/ schedule[@name="2018-04-27T18:03:22.638Z"]". CM-REQ-3282 The schedule will not run because the credential is missing.

You can safely ignore the messages as they are expected.

- s) After the import job is complete, check the **Completion time** and **Status** fields to verify that the job is complete. If it is complete, on the **View an import deployment record** page, click **Close**.
- t) To exit the IBM Cognos Administration GUI, close the browser tab.
- 13. Verify that the imported content is displayed in Cognos Analytics on Server B.
 - a) Return to the browser tab where the Cognos Analytics GUI is running. If it is not running, open a web browser and enter either of the following URLs:

http://FQDN_Of_Your_Machine:port/bi

Or

https://FQDN_Of_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 8 (Optional).

If you did perform Step 8, then you will use https. If you *did not* perform Step 8, then you use http.

If you *did not* perform Step 8, the default port value is 9300.

- b) On the IBM Cognos Analytics Welcome page, click Team content.
- c) Verify that the following content is listed:
 - Custom content that you saved to Public Folders before you ran this procedure.
 - IBM Spectrum Control Packages and (or IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or IBM Tivoli Storage Productivity Center Report Layouts).
- d) Optional: Attempt to generate a custom report or a predefined report and verify the contents.

Important: If you encounter APAR IT23800 or other problems when generating a predefined report in Cognos Analytics that was migrated from Tivoli Common Reporting, import the predefined reports package for the version of IBM Spectrum Control you are currently running on your system.

If you encounter APAR IT23800 or other problems when generating a custom report in Cognos Analytics that was migrated from Tivoli Common Reporting, you must update or recreate the custom report to use the predefined reports package for the version of IBM Spectrum Control you are currently running and remove references to tables that are no longer used in the IBM Spectrum Control database repository.

14. After you import the report content and schedules into Cognos Analytics, the schedules will not run due to missing credentials.

To update the schedules in Cognos Analytics with the correct credentials, complete the following steps:

a. Open a web browser and enter either of the following URLs:

http://FQDN_0f_Your_Machine:port/bi

Or

https://FQDN_Of_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 8 (Optional).

If you did perform Step 8, then you will use https. If you *did not* perform Step 8, then you use http.

If you *did not* perform Step 8, the default port value is 9300.

- b. On the IBM Cognos Analytics Welcome page, click Team content.
- c. Select a report that has an existing schedule.
- d. Select the **Properties** for the report.
- e. Select the **Schedule** tab.
- f. Select the > icon to open the schedule.
- g. Click **Update** on the schedule page.

Repeat steps c-g for each migrated report schedule you want to run in Cognos Analytics.

You migrated your custom IBM[®] Cognos[®] Business Intelligence reports and upgraded to the latest version of IBM Spectrum Control and are able to use Cognos[®] BI reports.

Change the configuration of IBM Cognos Analytics from anonymous access to authenticated access.

For more information, see Configuring an LDAP namespace for IBM Directory Server.

For more information, see Configuring an LDAP namespace for Active Directory Server.

For more information, see Managing user authentication.

Related tasks

"Importing IBM Spectrum Control pre-defined reports package " on page 96 Complete this procedure to import the IBM Spectrum Control predefined reports package into the IBM Cognos Analytics reporting tool.

Related information

APAR IT23800 Upgrading Db2 servers Upgrading a Db2 server (Windows) IBM Cognos Analytics server components Install and configure server components Installing server components on Windows operating system Installing Content Manager on Windows operating system Installing the Application services components on Windows operating system

Migrating Cognos BI reports to IBM Cognos Analytics in a multiple server Windows environment with remote Jazz for Service Management

If you do not have custom report content, you can skip this migration procedure. You can upgrade to IBM[®] Cognos[®] Analytics 11.0.9 or later when you upgrade to the latest version of IBM Spectrum Control. Complete this procedure in a multiple server environment to migrate your existing custom report content from Tivoli Common Reporting to Cognos Analytics.

Review the content of <u>Migrating reports to IBM Cognos Analytics during upgrade</u> before you start this procedure.

For this procedure, the terms *Server A* and *Server B* denote the two servers. *Server A* has DB2[®] Enterprise Server Edition and the IBM Spectrum Control database repository installed. *Server B* has DB2[®] Enterprise Server Edition, Jazz for Service Management, and Tivoli Common Reporting installed.

Important: Only reports in the Cognos Analytics Public Folders are exported from Tivoli Common Reporting. If you saved reports to Private Folders or My Folder, you *must* save them again in Public Folders before you export them.

If you plan to upgrade Db2 as part of your upgrade to the latest version of IBM Spectrum Control, upgrade Db2 on *Server A*, upgrade the IBM Spectrum Control database (TPCDB) on *Server A*, upgrade Db2 on *Server B* and then upgrade the Tivoli Common Reporting Content Store database (TCRDB) on *Server B*.

A high level overview on completing this upgrade:

- Export content from Tivoli Common Reporting on Server B.
- Upgrade IBM Spectrum Control on Server A.
- Uninstall IBM Spectrum Control from Server B.
- (Optional) Uninstall Tivoli Common Reporting, Jazz for Service Management, IBM[®] WebSphere[®] Application Server, and Installation Manager, from *Server B*.
- Install and configure Cognos Analytics on Server B.
- Import content into Cognos Analytics on Server B and then verify the content.
- 1. Log in to Jazz for Service Management and Tivoli Common Reporting on Server B to export content.
 - a) Open a web browser and enter the following URL:

https://FQDN_0f_Your_Machine:port/tarf/servlet/dispatch

Where https is the protocol, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*) and the *port* value is the secure HTTP port number that was specified during the installation of Jazz for Service Management.

To determine the secure HTTP port number for Jazz for Service Management, open the JazzSM_installation_dir\profile\properties\portdef.props file. The default JazzSM_installation_dir value is C:\Program Files\IBM\JazzSM. The port number is the value that is assigned to the **WC_defaulthost_secure** parameter. The default value is 16311.

If you receive a security certificate warning when you attempt to connect to the server, confirm the security exception and continue to the web page.

- b) Log in to the reporting interface using the Jazz for Service Management user name that was created when you installed Jazz for Service Management. The default value is smadmin.
- c) Select Launch > IBM Cognos Administration.
- d) In the IBM Cognos Administration GUI, select the **Configuration** tab.
- e) In the Configuration tab, select Content Administration.
- f) On the toolbar, click the New Export icon.

It is the third icon in the list.

- g) On the **Specify a name and description** page, enter a name for your export package and click **Next**.
- h) On the **Choose a deployment method** page, select **Select public folders and directory content** and click **Next**.
- i) On the Select the public folders content page, click the Add link.
- j) On the Select entries page, select the following items to export.
 - Custom content that you saved to Public Folders before running this procedure.
 - IBM Spectrum Control Packages and (or the IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or the IBM Tivoli Storage Productivity Center Predefined Reports).

- IBM Spectrum Control Report Layouts and (or the IBM Tivoli Storage Productivity Center Report Layouts).
- k) Click the **Green** arrow to transfer the content to the list.
- l) Click **OK**.
- m) On the Select the public folders content page, click Next.

Tip: If you want to export your schedules with your IBM[®] Cognos[®] Business Intelligence content from Tivoli Common Reporting, complete the following steps:

- 1) On the Select the public folders content page, select Include schedules.
- 2) Set Conflict resolution to Replace existing entries.
- 3) Click Next.
- n) On the **Select the directory content** page, select **Include data sources and connections** and **Include signons**.
- o) Set Conflict resolution to Replace existing entries and click Next.
- p) On the **Specify the general options** page, click **Next**.
- q) On the Specify a deployment archive page, click Set the encryption password.
- r) On the **Enter the encryption password** page, enter, and then confirm your password and click **OK**.

Tip: The encryption password is *not* an existing password in IBM Spectrum Control, Db2 or the operating system. The encryption password is a new password for the purpose of securing the content you are exporting from Jazz for Service Management and Tivoli Common Reporting.

Make note of your new password. You will need to provide it later in this procedure.

- s) On the **Specify a deployment archive** page, click **Next**.
- t) On the **Review the summary** page, click **Next**.
- u) On the Select an action page, select Save and run once and click Finish.
- v) On the **Run with options** page, click **Run**.
- w) On the **IBM Cognos software** page, select **View the details of this report after closing this dialog** and click **OK**.
- x) On the View run history details page, click Refresh.

Do not log off from the IBM Cognos Administration GUI until the export job is complete. You can click **Refresh** periodically to check the status of the export job.

- y) After the export job is complete, on the **View an export deployment record** page, click **Close**.
- z) Log off from the reporting interface.
- aa) Copy the exported file from the *JazzSM_installation_dir*\reporting\cognos \deployment\ directory to a directory that is outside of the Jazz for Service Management installation directory.

Make note of the name and location of this exported file. You will need this information in Step 11.

Tip: If you *do not* copy the exported file outside of the Jazz for Service Management installation directory, the exported file is deleted when you uninstall Tivoli Common Reporting.

2. Upgrade Server A to the latest version of IBM Spectrum Control.

For more information, see Upgrading from Tivoli Storage Productivity Center Version 5.2.0 and later with a remote database by using the installation program.

- 3. Upgrade *Server B* to the latest version of IBM Spectrum Control. You are then instructed to uninstall IBM Spectrum Control from *Server B*. Uninstall IBM Spectrum Control from *Server B*. For more information, see Uninstalling IBM Spectrum Control.
- 4. Optional: Uninstall Tivoli Common Reporting, Jazz for Service Management, WebSphere Application Server, and Installation Manager from *Server B*.

For more information, see Uninstalling Tivoli Common Reporting and Jazz for Service Management.

If you *did not* uninstall Tivoli Common Reporting, Jazz for Service Management, WebSphere Application Server, and Installation Manager, you *must* stop Jazz for Service Management and Tivoli Common Reporting before you proceed with the rest of this procedure.

a) To stop Jazz for Service Management and Tivoli Common Reporting, open a command prompt and enter the following command:

```
JazzSM_Installation_dir\profile\bin\stopServer.bat server_name
-username JazzSM_username -password JazzSM_password
```

For example:

```
C:\Program Files\IBM\JazzSM\profile\bin\stopServer.bat server1
-username smadmin -password abc123
```

- b) If you have a Windows Service named IBM WebSphere Application Server V8.5 -JazzSMProfile, you *must* change Startup Type from Automatic to Manual so that Jazz for Service Management and Tivoli Common Reporting do not start when you reboot the computer. For more information, see Accessing administration tools.
- 5. Install IBM Cognos Analytics 11.0.9 or later on Server B.
 - a) Log in to your Windows computer as a user with administrative privileges.
 - b) Start the IBM Cognos Analytics installation program.
 - c) Select the language to use for your installation and click **Next**.
 - d) On the **Product installation** page, select **IBM Cognos Analytics (IBM Bundler Edition)** and click **Next**.
 - e) On the License agreement page, accept the license agreement and click Next.
 - f) On the **Location** page, provide your installation location and name of the **Shortcut** folder and click **Next**.

Make note of your Cognos Analytics installation location. You will need to provide it later in this procedure.

Tip: If you want the Cognos Analytics installation to automatically create the installation location for you, click **Yes**.

g) On the Installation type page, select Custom and click Next.

The Custom option offers full flexibility to pick and choose the IBM Cognos Analytics components that you want to install.

- h) On the **Custom install** page, click **Next**.
- i) On the **Choose components** page, accept the default selections and click **Next**.
- j) On the **Pre-installation summary** page, review your information for accuracy and click **Install**.
- k) When the installation is complete, click **Done**.
- 6. On *Server B*, copy the following Db2 JDBC driver files from the C:\Program Files\IBM\SQLLIB \java\ directory to the *Cognos_installation_dir*\drivers\ directory:

The Cognos Analytics installation location is what you provided in the previous step.

- db2jcc.jar
- db2jcc_license_cu.jar
- db2jcc4.jar
- 7. Create the content store for Cognos Analytics on Server B.
 - a) From the Windows Start menu, select IBM Cognos Analytics > IBM Cognos Configuration.
 - b) In the **Explorer** window, expand **Data Access** > **Content Manager** and click **Content Store**.
 - c) In the Type property, enter DB2 database, if it is not already displayed.
 - d) In the **Database server and port number** property, enter localhost or the fully qualified domain name of the machine.

For example, localhost: 50000 or *FQDN_0f_Your_Machine*: 50000 where 50000 is the default port number that is used by Db2.

Tip: If you are using a different port number, ensure that you use that value. To determine the port that is used by Db2, examine the **varDBPort** parameter in the SC_installation_dir\config \InstallVariable.properties file.

e) In the **User ID and password** property, enter the user name of the owner of the Db2 instance where the content store database will be located and the password that is associated with that user name.

Typically, this user name is *db2admin*. If the user name is a Windows domain user name, enter the user name *without* a Windows domain name prefix or suffix.

- f) In the **Database name** property, verify that the default value is **cm**.
- g) From the **File** menu, click **Save**.

This step might take a few minutes to complete. Track the progress in the window.

- h) In the informational window, click Close.
- i) In the Explorer window, expand Data Access > Content Manager and click Content Store.
- j) Right-click Content Store and click Generate DDL.
- k) In the **informational** window, click **Close**.

Important: Do not exit IBM Cognos Configuration in this step. Wait until Step 10.

l) From the Windows Start menu, select IBM DB2 DB2COPY1 (Default) > DB2 Command Window - Administrator. Then, enter the following command:

db2 -tvf "Cognos_installation_dir\configuration\schemas\content\db2\createDb.sql"

On Windows, add quotes around the directory path if it contains spaces. For example:

db2 -tvf "C:\Program Files\IBM\Cognos\analytics\configuration\schemas\content\db2\createDb.sql"

This process might take a few minutes.

m) In IBM Cognos Configuration, from the **Actions** menu, click **Test**.

You are testing the connection between content manager and the content store database.

- n) In the **informational** window, click **Close**.
- 8. Optional: On *Server B*, you can change the IBM Cognos Analytics ports to match the ports that are used by Jazz for Service Management and Tivoli Common Reporting.

You would do this so that you do not have to get new firewall exceptions for the default Cognos Analytics ports.

- a) While you are still in IBM Cognos Configuration, in the Explorer window, click Environment.
- b) In the **Group Properties** window, select the **Value** next to the **URI** property and change the following properties (names):

Table 30. Group Property values	
Property	Change the value to
Gateway URI	Computer fully qualified domain name (for
External dispatcher URI	example, <i>myserver.mycompany.com</i>).
Internal dispatcher URI	• The https protocol.
Dispatcher URI for external applications	WC_defaulthost_secure parameter in the
Content Manager URIs	JazzSM_installation_dir\profile \properties\portdef.props file. The default value is 16311.

c) From the **File** menu, click **Save**.

- d) In the **informational** window, click **Close**.
- 9. Start IBM Cognos Analytics (content manager and application services), on Server B.

It might take Cognos Analytics a few minutes to start.

- a) While you are still in IBM Cognos Configuration, in the **Explorer** window, click **Local Configuration**.
- b) From the **Actions** menu, click **Test**.

Tip: If you are not configuring Cognos Analytics to send notifications, you can ignore the testing the mail server connection failure message.

- c) In the informational window, click Close.
- d) From the **Actions** menu, click **Start**.

It might take Cognos Analytics a few minutes to start.

- 10. Exit IBM Cognos Configuration, on Server B.
- 11. On *Server B*, copy the exported file that you created in Step 1 to the *Cognos_installation_dir* \deployment\ directory.
- 12. Import content into Cognos Analytics on Server B.
 - a) Open a web browser and enter either of the following URLs:

http://FQDN_Of_Your_Machine:port/bi

Or

```
https://FQDN_Of_Your_Machine:port/bi
```

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 8 (Optional). If you *did not* perform Step 8, the default port value is 9300.



Warning: At this point Cognos Analytics is configured with anonymous access so that anyone is able to access it.

- b) In the lower left-hand part of the page, select Manage > Administration console.
- c) In the IBM Cognos Administration GUI, select the **Configuration** tab.
- d) In the Configuration tab, select Content Administration.
- e) On the toolbar, click the **New Import** icon.

It is the fourth icon in the list.

- f) On the **Select a deployment archive** page, select the name of the file that you exported from Jazz for Service Management in Step 1 and click **Next**.
- g) On the **Enter the encryption password** page, enter the encryption password that you created in Step 1 and click **OK**.
- h) On the **Specify a name and description** page, enter a name for your import (or keep the default setting) and click **Next**.
- i) On the **Select the public folders, directory, and library content** page, select the following items to import:
 - Custom content that you exported.
 - IBM Spectrum Control Packages and (or the IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or the IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or the IBM Tivoli Storage Productivity Center Report Layouts).

j) Accept the default settings in the **Options** section and click **Next**.

Tip: If you want to import your schedules with your IBM[®] Cognos[®] Business Intelligence content from Tivoli Common Reporting, complete the following steps:

1) In the **Options** section, verify that **Include schedules** is selected.

2) In the **Options** section, verify that **Conflict resolution** is set to **Replace existing entries**.

3) Click Next.

- k) On the Select directory content page, verify that Include data sources and connections and Include signons are selected and that Conflict resolution is set to Replace existing entries and click Next.
- l) On the **Specify the general options** page, click **Next**.
- m) On the Review the summary page, click Next.
- n) On the Select an action page, select Save and run once and click Finish.
- o) On the **Run with Options** page, select **Upgrade all report specifications to the latest version** and **Assign new IDs during import**.
- p) Click **Run**.
- q) On the IBM Cognos software page, select View the details of this import after closing this dialog and click OK.
- r) On the View run history details page, click Refresh.

Check the **Status** field to monitor that the job is executing. Do *not* log off from the IBM Cognos Administration GUI until the import job is complete.

Tip: The import job might take approximately 15 minutes or more to resolve. Click **Refresh** periodically to check the status.

The results of importing the reports and schedules into Cognos Analytics contain the following similar messages:

```
CM-REQ-4328 A problem was encountered while importing the object
"/content/folder[@name="IBM Spectrum Control Predefined Reports"]/
folder[@name="Servers"]/report[@name="Servers Capacity"]/schedule".
CM-REQ-4329 The following references cannot be resolved and were cleared:
"credential: CAMID("VMMProvider:smadmin")/credential[@name='Credential '] "
CM-REQ-4328 A problem was encountered while importing the object
"/content/folder[@name="IBM Spectrum Control Predefined Reports"]/
folder[@name="Servers"]/report[@name="Servers Capacity"]/
schedule[@name="Servers"]/report[@name="Servers Capacity"]/
schedule[@name="2018-04-27T18:03:22.638Z"]".
CM-REQ-3282 The schedule will not run because the credential is missing.
```

You can safely ignore the messages as they are expected.

- s) After the import job is complete, check the **Completion time** and **Status** fields to verify that the job is complete. If it is complete, on the **View an import deployment record** page, click **Close**.
- t) To exit the IBM Cognos Administration GUI, close the browser tab.
- 13. Verify that the imported content is displayed in Cognos Analytics on Server B.
 - a) Return to the browser tab where the Cognos Analytics GUI is running. If it is not running, open a web browser and enter either of the following URLs:

http://FQDN_0f_Your_Machine:port/bi

Or

https://FQDN_0f_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 8 (Optional).

If you did perform Step 8, then you will use https. If you *did not* perform Step 8, then you use http.

If you *did not* perform Step 8, the default port value is 9300.

b) On the IBM Cognos Analytics Welcome page, click Team content.

- c) Verify that the following content is listed:
 - Custom content that you saved to Public Folders before you ran this procedure.
 - IBM Spectrum Control Packages and (or IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or IBM Tivoli Storage Productivity Center Report Layouts).
- d) Optional: Attempt to generate a custom report or a predefined report and verify the contents.

Important: If you encounter APAR IT23800 or other problems when generating a predefined report in Cognos Analytics that was migrated from Tivoli Common Reporting, import the predefined reports package for the version of IBM Spectrum Control you are currently running on your system.

If you encounter APAR IT23800 or other problems when generating a custom report in Cognos Analytics that was migrated from Tivoli Common Reporting, you must update or recreate the custom report to use the predefined reports package for the version of IBM Spectrum Control you are currently running and remove references to tables that are no longer used in the IBM Spectrum Control database repository.

14. After you import the report content and schedules into Cognos Analytics, the schedules will not run due to missing credentials.

To update the schedules in Cognos Analytics with the correct credentials, complete the following steps:

a. Open a web browser and enter either of the following URLs:

```
http://FQDN_Of_Your_Machine:port/bi
```

Or

https://FQDN_0f_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 8 (Optional).

If you did perform Step 8, then you will use https. If you *did not* perform Step 8, then you use http.

If you *did not* perform Step 8, the default port value is 9300.

- b. On the IBM Cognos Analytics Welcome page, click Team content.
- c. Select a report that has an existing schedule.
- d. Select the **Properties** for the report.
- e. Select the **Schedule** tab.
- f. Select the > icon to open the schedule.
- g. Click **Update** on the schedule page.

Repeat steps c-g for each migrated report schedule you want to run in Cognos Analytics.

You migrated your custom IBM[®] Cognos[®] Business Intelligence reports and upgraded to the latest version of IBM Spectrum Control and are able to use Cognos[®] BI reports.

Change the configuration of IBM Cognos Analytics from anonymous access to authenticated access.

For more information, see Configuring an LDAP namespace for IBM Directory Server.

For more information, see <u>Configuring an LDAP namespace for Active Directory Server</u>.
For more information, see Managing user authentication.

Related tasks

"Importing IBM Spectrum Control pre-defined reports package" on page 96 Complete this procedure to import the IBM Spectrum Control predefined reports package into the IBM Cognos Analytics reporting tool.

Related information

APAR IT23800 Upgrading Db2 servers Upgrading a Db2 server (Windows) IBM Cognos Analytics server components Install and configure server components Installing server components on Windows operating system Installing Content Manager on Windows operating system Installing the Application services components on Windows operating system

Migrating Cognos BI reports to IBM Cognos Analytics in a single Linux environment

If you do not have custom report content, you can skip this migration procedure. You can upgrade to IBM[®] Cognos[®] Analytics 11.0.9 or later when you upgrade to the latest version of IBM Spectrum Control. Complete this procedure to migrate your existing custom report content from Tivoli Common Reporting to Cognos Analytics.

Review the content of <u>Migrating reports to IBM Cognos Analytics during upgrade</u> before you start this procedure.

This procedure assumes that you installed Db2[®], IBM Spectrum Control 5.2.15 or earlier, IBM[®]Jazz for Service Management, IBM[®] Tivoli Common Reporting on a single Linux computer.

Important:

Only reports in the Cognos Analytics Public Folders are exported from Tivoli Common Reporting. If you saved reports to Private Folders or My Folder, you *must* save them again in Public Folders before you export them.

If you plan to upgrade Db2 as part of your upgrade to the latest version of IBM Spectrum Control, upgrade Db2, upgrade the IBM Spectrum Control database (TPCDB) and then upgrade the Tivoli Common Reporting Content Store database (TCRDB).

A high level overview of the migration:

- Export content from Tivoli Common Reporting.
- Upgrade IBM Spectrum Control.
- (Optional) Uninstall Tivoli Common Reporting, Jazz for Service Management, IBM[®] WebSphere[®] Application Server, and Installation Manager.
- Install and configure Cognos Analytics.
- Import content into Cognos Analytics and then verify the content.

Verify that you have the following prerequisite packages installed on a Linux computer for IBM Cognos Analytics 11.0.9 or later.

The prerequisite packages for Red Hat Enterprise Linux (RHEL) 6 versions are:

glibc-2.12-1.166.el6 or later (both i686 and x86_64 packages) libstdc++-4.4.7-16.el6 or later (both i686 and x86_64 packages) nspr-4.9.2-1.el6 or later (both i686 and x86_64 packages) nss-3.14.0.0-12.el6 or later (both i686 and x86_64 packages) openmotif-2.3.3-5.el6 or later (both i686 and x86_64 packages)

The prerequisite packages for Red Hat Enterprise Linux (RHEL) 7 versions are:

glibc-2.17-55.el7 or later (both i686 and x86_64 packages) libstdc++-4.8.2-16.el7 or later (both i686 and x86_64 packages) nspr-4.10.2-4.el7 or later (both i686 and x86_64 packages) nss-3.15.4-6.el7 or later (both i686 and x86_64 packages) motif-2.3.4-7.el7 or later (both i686 and x86_64 packages)

For more information, see Software Product Compatibility Reports.

You need to set the correct ulimit values in the /etc/security/limits.conf file for IBM Cognos Analytics 11.0.9 or later.

Here is an example of the entries you might need to add to the /etc/security/limits.conf file:

*	soft	nproc	unlimited
	hard	nproc	unlimited
*	soit	nofile	8192
	hard	nofile	8192
*	soft	stack	unlimited
*	hard	stack	unlimited

After you set and save your ulimit values, restart your computer and verify the correct ulimit values.

For more information, see Set the ulimit values on UNIX and Linux operating systems .

- 1. Log in to Jazz for Service Management and Tivoli Common Reporting to export content.
 - a) Open a web browser and enter the following URL:

https://FQDN_0f_Your_Machine:port/tarf/servlet/dispatch

Where https is the protocol, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*) and the *port* value is the secure HTTP port number that was specified during the installation of Jazz for Service Management.

To determine the secure HTTP port number for Jazz for Service Management, open the *JazzSM_installation_dir*/profile/properties/portdef.props file. The default *JazzSM_installation_dir* value is /opt/IBM/JazzSM. The port number is the value that is assigned to the **WC_defaulthost_secure** parameter. The default value is 16311.

If you receive a security certificate warning when you attempt to connect to the server, confirm the security exception and continue to the web page.

- b) Log in to the reporting interface using the Jazz for Service Management user name that was created when you installed Jazz for Service Management. The default value is smadmin.
- c) Select Launch > IBM Cognos Administration.
- d) In the IBM Cognos Administration GUI, select the **Configuration** tab.
- e) In the Configuration tab, select Content Administration.
- f) On the toolbar, click the **New Export** icon.

It is the third icon in the list.

- g) On the **Specify a name and description** page, enter a name for your export package and click **Next**.
- h) On the **Choose a deployment method** page, select **Select public folders and directory content** and click **Next**.
- i) On the Select the public folders content page, click the Add link.
- j) On the **Select entries** page, select the following items to export.
 - Custom content that you saved to Public Folders before running this procedure.
 - IBM Spectrum Control Packages and (or the IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or the IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or the IBM Tivoli Storage Productivity Center Report Layouts).

- k) Click the **Green** arrow to transfer the content to the list.
- l) Click **OK**.
- m) On the Select the public folders content page, click Next.

Tip: If you want to export your schedules with your IBM[®] Cognos[®] Business Intelligence content from Tivoli Common Reporting, complete the following steps:

- 1) On the Select the public folders content page, select Include schedules.
- 2) Set Conflict resolution to Replace existing entries.
- 3) Click Next.
- n) On the **Select the directory content** page, select **Include data sources and connections** and **Include signons**.
- o) Set Conflict resolution to Replace existing entries and click Next.
- p) On the **Specify the general options** page, click **Next**.
- q) On the Specify a deployment archive page, click Set the encryption password.
- r) On the **Enter the encryption password** page, enter, and then confirm your password and click **OK**.

Tip: The encryption password is *not* an existing password in IBM Spectrum Control, Db2 or the operating system. The encryption password is a new password for the purpose of securing the content you are exporting from Jazz for Service Management and Tivoli Common Reporting.

Make note of your new password. You will need to provide it later in this procedure.

- s) On the Specify a deployment archive page, click Next.
- t) On the **Review the summary** page, click **Next**.
- u) On the Select an action page, select Save and run once and click Finish.
- v) On the **Run with options** page, click **Run**.
- w) On the **IBM Cognos software** page, select **View the details of this report after closing this dialog** and click **OK**.
- x) On the View run history details page, click Refresh.

Do not log off from the IBM Cognos Administration GUI until the export job is complete. You can click **Refresh** periodically to check the status of the export job.

- y) After the export job is complete, on the View an export deployment record page, click Close.
- z) Log off from the reporting interface.
- aa) Copy the exported file from the JazzSM_installation_dir/reporting/cognos/ deployment/ directory to a directory that is outside of the Jazz for Service Management installation directory.

Make note of the name and location of this exported file. You will need this information in <u>"12" on</u> page 138.

Tip: If you *do not* copy the exported file outside of the Jazz for Service Management installation directory, the exported file is deleted when you uninstall Tivoli Common Reporting.

2. Upgrade your system to latest version of IBM Spectrum Control; this step uninstalls the IBM Spectrum Control Cognos BI Reports component.

For more information, see Upgrading IBM Spectrum Control in a single-server environment.

3. Optional: Uninstall Tivoli Common Reporting, Jazz for Service Management, WebSphere Application Server, and Installation Manager.

For more information, see Uninstalling Tivoli Common Reporting and Jazz for Service Management.

If you *did not* uninstall Tivoli Common Reporting, Jazz for Service Management, WebSphere Application Server, and Installation Manager, you *must* stop Jazz for Service Management and Tivoli Common Reporting before you proceed with the rest of this procedure.

To stop Jazz for Service Management and Tivoli Common Reporting, open a command prompt and enter the following command:

JazzSM_installation_dir/profile/bin/stopServer.sh server_name -username JazzSM_username -password JazzSM_password

For example:

/opt/IBM/JazzSM/profile/bin/stopServer.sh server1 -username smadmin -password abc123

4. Install IBM Cognos Analytics 11.0.9 or later.

Tip: You do not need to set the **JAVA_HOME** environment variable before you start the IBM Cognos Analytics 11.0.9 or later installation program.

- a) Log in to your computer as a user with root privileges.
- b) Start the IBM Cognos Analytics installation program.
- c) Select the language to use for your installation and click **Next**.
- d) On the **Product installation** page, select **IBM Cognos Analytics (IBM Bundler Edition)** and click **Next**.
- e) On the License agreement page, accept the License Agreement and click Next.
- f) On the **Location** page, provide your installation location and click **Next**.

Make note of your Cognos Analytics installation location. You will need to provide it later in this procedure.

Tip: If you want the IBM Cognos Analytics installation to automatically create the installation location for you, click **Yes**.

- g) On the Installation type page, select First install and click Next.
- h) On the **Choose components** page, accept the default selections, and click **Next**.
- i) On the Pre-installation summary page, review your information for accuracy and click Install.

j) When the installation is complete, click **Done**.

- 5. Copy the following Db2 JDBC driver files from the /opt/ibm/db2/version/java/ directory to the Cognos_installation_dir/drivers/ directory:
 - db2jcc.jar
 - db2jcc_license_cu.jar
 - db2jcc4.jar
- 6. Open a command prompt and enter the following command as the root user:

```
cd Cognos_installation_dir/drivers/
chmod +x db2jcc*.jar
```

7. Open a command prompt and enter the following command as the root user:

```
ln -s Db2_instance_owner_home_directory/sqllib/lib32/libdb2.so
Cognos_installation_dir/bin/
```

IBM Spectrum Control Predefined Reports use Compatibility Query Mode. IBM Cognos Analytics needs to use the 32-Bit Db2 library in order to connect to the IBM Spectrum Control database as a data source.

- 8. Create the content store for Cognos Analytics.
 - a) Open a command prompt and enter the following commands to start IBM Cognos Configuration:

```
cd Cognos_installation_dir/bin64/
. /home/db2inst1/sqllib/db2profile
./cogconfig.sh
```

Notice the space between the . and the / in the second command.

- b) In the Explorer window, expand Data Access > Content Manager and click Content Store.
- c) In the **Type** property, enter **DB2 database**, if it is not already displayed.
- d) In the **Database server and port number** property, enter localhost or the fully qualified domain name of the machine.

For example, localhost: 50000 or *FQDN_Of_Your_Machine*: 50000 where 50000 is the default port number that is used by Db2.

Tip: If you are using a different port number, ensure that you use that value. To determine the port that is used by Db2, examine the **varDBPort** parameter in the *SC_installation_dir/* config/InstallVariable.properties file.

e) In the **User ID and password** property, enter the user name of the owner of the Db2 instance where the content store database will be located and the password that is associated with that user name

Typically, this user name is *db2inst1*.

- f) In the **Database name** property, verify that the default value is **cm**.
- g) From the File menu, click Save.

This step might take a few minutes to complete. Track the progress in the window.

- h) In the **informational** window, click **Close**.
- i) In the Explorer window, expand Data Access > Content Manager and click Content Store.
- j) Right-click Content Store and click Generate DDL.
- k) In the **informational** window, click **Close**.

Important: Do not exit IBM Cognos Configuration in this step. Wait until "11" on page 138.

- l) While you are logged into the Linux operating system as the root user, switch to the user that is the Db2 instance owner (for example, *db2inst1*).
- m) Open a command prompt and enter the following Db2 command:

db2 -tvf Cognos_installation_dir/configuration/schemas/content/db2/createDb.sql

If the results of this command contain the following similar messages, you can safely ignore those messages because the Db2 instance owner already has the necessary privileges:

GRANT CREATETAB,BINDADD,CONNECT,IMPLICIT_SCHEMA ON DATABASE TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

GRANT CREATEIN, DROPIN, ALTERIN ON SCHEMA DB2COGNOS TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

GRANT USE OF TABLESPACE TSN_USR_cm TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

GRANT USE OF TABLESPACE TSN_REG_cm TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

- n) Go back to the root user.
- o) In IBM Cognos Configuration, from the Actions menu, click Test.

You are testing the connection between content manager and the content store database.

- p) In the **informational** window, click **Close**.
- 9. Optional: You can change the IBM Cognos Analytics ports to match the ports that are used by Jazz for Service Management and Tivoli Common Reporting.

You would do this so that you do not have to get new firewall exceptions for the default Cognos Analytics ports.

- a) While you are still in IBM Cognos Configuration, in the **Explorer** window, click **Environment**.
- b) In the **Group Properties** window, select the **Value** next to the **URI** property and change the following properties (names):

Table 31. Group Property values		
Property	Change the value to	
Gateway URI	 Computer fully qualified domain name (for example, myserver.mycompany.com). The https protocol. The 9300 port to the value of the WC_defaulthost_secure parameter in the 	
External dispatcher URI		
Internal dispatcher URI		
Dispatcher URI for external applications		
Content Manager URIs	JazzSM_installation_dir\profile \properties\portdef.props file. The default value is 16311.	

- c) From the **File** menu, click **Save**.
- d) In the informational window, click Close.
- 10. Start Cognos Analytics (content manager and application services).

It might take Cognos Analytics a few minutes to start.

- a) While you are still in IBM Cognos Configuration, in the **Explorer** window, click **Local Configuration**.
- b) From the **Actions** menu, click **Test**.

Tip: If you are not configuring Cognos Analytics to send notifications, you can ignore the testing the mail server connection failure message.

- c) In the **informational** window, click **Close**.
- d) From the Actions menu, click Start.

It might take Cognos Analytics a few minutes to start.

- 11. Exit IBM Cognos Configuration.
- 12. Copy the exported file that you created in <u>"1" on page 134</u> to the *Cognos_installation_dir/* deployment/ directory.
- 13. Import content into Cognos Analytics.
 - a) Open a web browser and enter either of the following URLs:

http://FQDN_0f_Your_Machine:port/bi

Or

```
https://FQDN_Of_Your_Machine:port/bi
```

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in <u>Step 9</u> (Optional). If you *did not* perform <u>Step 9</u>, the default port value is 9300.



Warning: At this point Cognos Analytics is configured with anonymous access so that anyone is able to access it.

- b) In the lower left-hand part of the page, select Manage > Administration console.
- c) In the IBM Cognos Administration GUI, select the ${\mbox{Configuration}}$ tab.
- d) In the **Configuration** tab, select **Content Administration**.

e) On the toolbar, click the New Import icon.

It is the fourth icon in the list.

- f) On the **Select a deployment archive** page, select the name of the file that you exported from Jazz for Service Management in Step 1 and click **Next**.
- g) On the **Enter the encryption password** page, enter the encryption password that you created in Step 1 and click **OK**.
- h) On the **Specify a name and description** page, enter a name for your import (or keep the default setting) and click **Next**.
- i) On the **Select the public folders, directory, and library content** page, select the following items to import:
 - Custom content that you exported.
 - IBM Spectrum Control Packages and (or the IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or the IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or the IBM Tivoli Storage Productivity Center Report Layouts).
- j) Accept the default settings in the **Options** section and click **Next**.

Tip: If you want to import your schedules with your IBM[®] Cognos[®] Business Intelligence content from Tivoli Common Reporting, complete the following steps:

- 1) In the **Options** section, verify that **Include schedules** is selected.
- 2) In the **Options** section, verify that **Conflict resolution** is set to **Replace existing entries**.
- 3) Click Next.
- k) On the Select directory content page, verify that Include data sources and connections and Include signons are selected and that Conflict resolution is set to Replace existing entries and click Next.
- l) On the Specify the general options page, click Next.
- m) On the **Review the summary** page, click **Next**.
- n) On the Select an action page, select Save and run once and click Finish.
- o) On the **Run with Options** page, select **Upgrade all report specifications to the latest version** and **Assign new IDs during import**.
- p) Click Run.
- q) On the IBM Cognos software page, select View the details of this import after closing this dialog and click OK.
- r) On the View run history details page, click Refresh.

Check the **Status** field to monitor that the job is executing. Do *not* log off from the IBM Cognos Administration GUI until the import job is complete.

Tip: The import job might take approximately 15 minutes or more to resolve. Click **Refresh** periodically to check the status.

The results of importing the reports and schedules into Cognos Analytics contain the following similar messages:

```
CM-REQ-4328 A problem was encountered while importing the object
"/content/folder[@name="IBM Spectrum Control Predefined Reports"]/
folder[@name="Servers"]/report[@name="Servers Capacity"]/schedule".
CM-REQ-4329 The following references cannot be resolved and were cleared:
"credential: CAMID("VMMProvider:smadmin")/credential[@name='Credential '] ".
CM-REQ-4328 A problem was encountered while importing the object
"/content/folder[@name="IBM Spectrum Control Predefined Reports"]/
folder[@name="Servers"]/report[@name="Servers Capacity"]/
schedule[@name="2018-04-27T18:03:22.638Z"]".
CM-REQ-3282 The schedule will not run because the credential is missing.
```

You can safely ignore the messages as they are expected.

- s) After the import job is complete, check the **Completion time** and **Status** fields to verify that the job is complete. If it is complete, on the **View an import deployment record** page, click **Close**.
- t) To exit the IBM Cognos Administration GUI, close the browser tab.
- 14. Verify that the imported content is displayed in Cognos Analytics.
 - a) Return to the browser tab where the Cognos Analytics GUI is running. If it is not running, open a web browser and enter either of the following URLs:

http://FQDN_0f_Your_Machine:port/bi

Or

https://FQDN_Of_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 9 (Optional).

If you did perform Step 9, then you will use https. If you *did not* perform Step 9, then you use http.

If you *did not* perform Step 9, the default port value is 9300.

- b) On the IBM Cognos Analytics Welcome page, click Team content.
- c) Verify that the following content is listed:
 - Custom content that you saved to Public Folders before you ran this procedure.
 - IBM Spectrum Control Packages and (or IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or IBM Tivoli Storage Productivity Center Report Layouts).
- d) Optional: Attempt to generate a custom report or a predefined report and verify the contents.

Important: If you encounter APAR IT23800 or other problems when generating a predefined report in Cognos Analytics that was migrated from Tivoli Common Reporting, import the predefined reports package for the version of IBM Spectrum Control you are currently running on your system.

If you encounter APAR IT23800 or other problems when generating a custom report in Cognos Analytics that was migrated from Tivoli Common Reporting, you must update or recreate the custom report to use the predefined reports package for the version of IBM Spectrum Control you are currently running and remove references to tables that are no longer used in the IBM Spectrum Control database repository.

15. After you import the report content and schedules into Cognos Analytics, the schedules will not run due to missing credentials.

To update the schedules in Cognos Analytics with the correct credentials, complete the following steps:

a. Return to the browser tab where the Cognos Analytics GUI is running. If it is not running, open a web browser and enter either of the following URLs:

http://FQDN_0f_Your_Machine:port/bi

Or

https://FQDN_Of_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 9 (Optional).

If you did perform Step 9, then you will use https. If you *did not* perform Step 9, then you use http.

If you *did not* perform Step 9, the default port value is 9300.

- b. On the IBM Cognos Analytics Welcome page, click Team content.
- c. Select a report that has an existing schedule.
- d. Select the **Properties** for the report.
- e. Select the **Schedule** tab.
- f. Select the > icon to open the schedule.
- g. Click **Update** on the schedule page.

Repeat steps c-g for each migrated report schedule you want to run in Cognos Analytics.

You migrated your custom IBM[®] Cognos[®] Business Intelligence reports and upgraded to the latest version of IBM Spectrum Control and are able to use Cognos[®] BI reports.

Change the configuration of IBM Cognos Analytics from anonymous access to authenticated access.

For more information, see Configuring an LDAP namespace for IBM Directory Server.

For more information, see Configuring an LDAP namespace for Active Directory Server.

For more information, see Managing user authentication.

Related tasks

<u>"Importing IBM Spectrum Control pre-defined reports package " on page 96</u> Complete this procedure to import the IBM Spectrum Control predefined reports package into the IBM Cognos Analytics reporting tool.

Related information

APAR IT23800 Upgrading Db2 servers Upgrading a Db2 server (Linux and UNIX) IBM Cognos Analytics server components Install and configure server components Installing server components on UNIX or Linux operating systems Installing Content Manager on UNIX or Linux operating systems Installing the Application services components on UNIX or Linux operating systems

Migrating Cognos BI reports to IBM Cognos Analytics in a multiple-server Linux environment with a remote database

If you do not have custom report content, you can skip this migration procedure. You can upgrade to IBM[®] Cognos[®] Analytics 11.0.9 or later when you upgrade to the latest version of IBM Spectrum Control. Complete this procedure to migrate your existing custom report content from Tivoli Common Reporting to Cognos Analytics.

Review the content of <u>Migrating reports to IBM Cognos Analytics during upgrade</u> before you start this procedure.

For this procedure, the terms *Server A* and *Server B* denote the two servers. *Server A* has DB2[®] Enterprise Server Edition and the IBM Spectrum Control database repository installed. *Server B* has all of the other IBM Spectrum Control components installed and DB2[®] Enterprise Server Edition, Jazz for Service Management, and Tivoli Common Reporting. **Important:** Only reports in the Cognos Analytics Public Folders are migrated to IBM[®] Cognos[®] Analytics 11.0.9 or later. If you saved reports to My Folder, you must save them again in Public Folders before you migrate them.

If you plan to upgrade Db2 as part of your upgrade to the latest version of IBM Spectrum Control, upgrade Db2 on *Server A*, upgrade the IBM Spectrum Control database (TPCDB) on *Server A*, upgrade Db2 on *Server B* and then upgrade the Tivoli Common Reporting Content Store database (TCRDB) on *Server B*.

A high level overview on completing this upgrade:

- Export content from Tivoli Common Reporting on Server B.
- Upgrade IBM Spectrum Control on Server A.
- Upgrade IBM Spectrum Control on Server B.
- (Optional) Uninstall Tivoli Common Reporting, Jazz for Service Management, IBM[®] WebSphere[®] Application Server, and Installation Manager, from *Server B*.
- Install and configure Cognos Analytics on Server B.
- Import content into IBM Cognos Analytics on Server B and then verify the content.

Verify that you have the following prerequisite packages installed on *Server B* for IBM Cognos Analytics 11.0.9 or later.

The prerequisite packages for Red Hat Enterprise Linux (RHEL) 6 are

glibc-2.12-1.166.el6 or later (both i686 and x86_64 packages) libstdc++-4.4.7-16.el6 or later (both i686 and x86_64 packages) nspr-4.9.2-1.el6 or later (both i686 and x86_64 packages) nss-3.14.0.0-12.el6 or later (both i686 and x86_64 packages) openmotif-2.3.3-5.el6 or later (both i686 and x86_64 packages)

The prerequisite packages for Red Hat Enterprise Linux (RHEL) 7 are:

glibc-2.17-55.el7 or later (both i686 and x86_64 packages) libstdc++-4.8.2-16.el7 or later (both i686 and x86_64 packages) nspr-4.10.2-4.el7 or later (both i686 and x86_64 packages) nss-3.15.4-6.el7 or later (both i686 and x86_64 packages) motif-2.3.4-7.el7 or later (both i686 and x86_64 packages)

For more information, see Software Product Compatibility Reports.

You need to set the correct ulimit values for *Server B* in the /etc/security/limits.conf file for Cognos Analytics.

Here is an example of the entries you might need to add to the /etc/security/limits.conf file:

*	soft	nproc	unlimited
*	hard	nproc	unlimited
*	soft	nofile	8192
*	hard	nofile	8192
*	soft	stack	unlimited
*	hard	stack	unlimited

After you set and save your ulimit values, restart your computer and verify the correct ulimit values.

For more information, see Set the ulimit values on UNIX and Linux operating systems .

- 1. Log in to Jazz for Service Management and Tivoli Common Reporting on Server B to export content.
 - a) Open a web browser and enter the following URL:

https://FQDN_0f_Your_Machine:port/tarf/servlet/dispatch

Where https is the protocol, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*) and the *port* value is the secure HTTP port number that was specified during the installation of Jazz for Service Management.

To determine the secure HTTP port number for Jazz for Service Management, open the JazzSM_installation_dir/profile/properties/portdef.props file. The default *JazzSM_installation_dir* value is /opt/IBM/JazzSM. The port number is the value that is assigned to the **WC_defaulthost_secure** parameter. The default value is 16311.

If you receive a security certificate warning when you attempt to connect to the server, confirm the security exception and continue to the web page.

- b) Log in to the reporting interface using the Jazz for Service Management user name that was created when you installed Jazz for Service Management. The default value is smadmin.
- c) Select Launch > IBM Cognos Administration.
- d) In the IBM Cognos Administration GUI, select the **Configuration** tab.
- e) In the **Configuration** tab, select **Content Administration**.
- f) On the toolbar, click the **New Export** icon.

It is the third icon in the list.

- g) On the **Specify a name and description** page, enter a name for your export package and click **Next**.
- h) On the **Choose a deployment method** page, select **Select public folders and directory content** and click **Next**.
- i) On the Select the public folders content page, click the Add link.
- j) On the Select entries page, select the following items to export.
 - Custom content that you saved to Public Folders before running this procedure.
 - IBM Spectrum Control Packages and (or the IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or the IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or the IBM Tivoli Storage Productivity Center Report Layouts).
- k) Click the **Green** arrow to transfer the content to the list.
- l) Click **OK**.
- m) On the Select the public folders content page, click Next.

Tip: If you want to export your schedules with your IBM[®] Cognos[®] Business Intelligence content from Tivoli Common Reporting, complete the following steps:

- 1) On the **Select the public folders** content page, select **Include schedules**.
- 2) Set Conflict resolution to Replace existing entries.
- 3) Click Next.
- n) On the **Select the directory content** page, select **Include data sources and connections** and **Include signons**.
- o) Set Conflict resolution to Replace existing entries and click Next.
- p) On the Specify the general options page, click Next.
- q) On the Specify a deployment archive page, click Set the encryption password.
- r) On the **Enter the encryption password** page, enter, and then confirm your password and click **OK**.

Tip: The encryption password is *not* an existing password in IBM Spectrum Control, Db2 or the operating system. The encryption password is a new password for the purpose of securing the content you are exporting from Jazz for Service Management and Tivoli Common Reporting.

Make note of your new password. You will need to provide it later in this procedure.

- s) On the Specify a deployment archive page, click Next.
- t) On the **Review the summary** page, click **Next**.
- u) On the Select an action page, select Save and run once and click Finish.
- v) On the ${\bf Run}$ with options page, click ${\bf Run}.$

- w) On the **IBM Cognos software** page, select **View the details of this report after closing this dialog** and click **OK**.
- x) On the View run history details page, click Refresh.

Do not log off from the IBM Cognos Administration GUI until the export job is complete. You can click **Refresh** periodically to check the status of the export job.

- y) After the export job is complete, on the **View an export deployment record** page, click **Close**.
- z) Log off from the reporting interface.
- aa) Copy the exported file from the JazzSM_installation_dir/reporting/cognos/ deployment/ directory to a directory that is outside of the Jazz for Service Management installation directory.

Make note of the name and location of this exported file. You will need this information in Step 13.

Tip: If you *do not* copy the exported file outside of the Jazz for Service Management installation directory, the exported file is deleted when you uninstall Tivoli Common Reporting.

2. Upgrade Server A to the latest version of IBM Spectrum Control.

For more information, see <u>Upgrading from Tivoli Storage Productivity Center Version 5.2.0 and later</u> with a remote database by using the installation program.

- 3. Upgrade *Server B* to the latest version of IBM Spectrum Control. For more information, see <u>Upgrading from Tivoli Storage Productivity Center Version 5.2.0 and later</u> with a remote database by using the installation program.
- 4. Optional: Uninstall Tivoli Common Reporting, Jazz for Service Management, WebSphere Application Server, and Installation Manager from *Server B*.

For more information, see Uninstalling Tivoli Common Reporting and Jazz for Service Management.

If you *did not* uninstall Tivoli Common Reporting, Jazz for Service Management, WebSphere Application Server, and Installation Manager, you *must* stop Jazz for Service Management and Tivoli Common Reporting before you proceed with the rest of this procedure.

To stop Jazz for Service Management and Tivoli Common Reporting, open a command prompt and enter the following command:

JazzSM_installation_dir/profile/bin/stopServer.sh server_name -username JazzSM_username -password JazzSM_password

For example:

/opt/IBM/JazzSM/profile/bin/stopServer.sh server1 -username smadmin -password abc123

5. Install IBM Cognos Analytics 11.0.9 or later on Server B.

Tip: You do not need to set the **JAVA_HOME** environment variable before you start the IBM Cognos Analytics Version 11.0.9 or later installation program.

- a) Log in to your computer as a user with root privileges.
- b) Start the IBM Cognos Analytics installation program.
- c) Select the language to use for your installation and click Next.
- d) On the **Product installation** page, select **IBM Cognos Analytics (IBM Bundler Edition)** and click **Next**.
- e) On the License agreement page, accept the License Agreement and click Next.
- f) On the **Location** page, provide your installation location and click **Next**.

Make note of your Cognos Analytics installation location. You will need to provide it later in this procedure.

Tip: If you want the IBM Cognos Analytics installation to automatically create the installation location for you, click **Yes**.

g) On the Installation type page, select First install and click Next.

h) On the **Choose components** page, accept the default selections, and click **Next**.

- i) On the **Pre-installation summary** page, review your information for accuracy and click **Install**.
- j) When the installation is complete, click **Done**.
- 6. On Server B, copy the following Db2 JDBC driver files from the /opt/ibm/db2/version/java/ directory to the Cognos_installation_dir/drivers/ directory :
 - db2jcc.jar
 - db2jcc_license_cu.jar
 - db2jcc4.jar
- 7. On Server B, open a command prompt and enter the following command as the root user:

```
cd Cognos_installation_dir/drivers/
chmod +x db2jcc*.jar
```

8. On Server B, open a command prompt and enter the following command as the root user:

```
ln -s Db2_instance_owner_home_directory/sqllib/lib32/libdb2.so
Cognos_installation_dir/bin/
```

IBM Spectrum Control Predefined Reports use Compatibility Query Mode. IBM Cognos Analytics needs to use the 32-Bit Db2 library in order to connect to the IBM Spectrum Control database as a data source.

- 9. Create the content store for Cognos Analytics on Server B.
 - a) Open a command prompt and enter the following commands to start IBM Cognos Configuration:

```
cd Cognos_installation_dir/bin64/
. /home/db2inst1/sqllib/db2profile
./cogconfig.sh
```

Notice the space between the . and the / in the second command.

- b) In the Explorer window, expand Data Access > Content Manager and click Content Store.
- c) In the **Type** property, enter **DB2 database**, if it is not already displayed.
- d) In the **Database server and port number** property, enter localhost or the fully qualified domain name of the machine.

For example, localhost: 50000 or *FQDN_0f_Your_Machine*: 50000 where 50000 is the default port number that is used by Db2.

Tip: If you are using a different port number, ensure that you use that value. To determine the port that is used by Db2, examine the **varDBPort** parameter in the SC_installation_dir/ config/InstallVariable.properties file.

e) In the **User ID and password** property, enter the user name of the owner of the Db2 instance where the content store database will be located and the password that is associated with that user name

Typically, this user name is *db2inst1*.

- f) In the **Database name** property, verify that the default value is **cm**.
- g) From the File menu, click Save.

This step might take a few minutes to complete. Track the progress in the window.

- h) In the **informational** window, click **Close**.
- i) In the Explorer window, expand Data Access > Content Manager and click Content Store.
- j) Right-click Content Store and click Generate DDL.
- k) In the informational window, click Close.

Important: Do not exit IBM Cognos Configuration in this step. Wait until Step 12.

- l) While you are logged into the Linux operating system as the root user, switch to the user that is the Db2 instance owner (for example, *db2inst1*).
- m) Open a command prompt and enter the following Db2 command:

 $db2 \ \text{-tvf} \ \textit{Cognos_installation_dir/configuration/schemas/content/db2/createDb.sql}$

If the results of this command contain the following similar messages, you can safely ignore those messages because the Db2 instance owner already has the necessary privileges:

GRANT CREATETAB,BINDADD,CONNECT,IMPLICIT_SCHEMA ON DATABASE TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

GRANT CREATEIN, DROPIN, ALTERIN ON SCHEMA DB2COGNOS TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

GRANT USE OF TABLESPACE TSN_USR_cm TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

GRANT USE OF TABLESPACE TSN_REG_cm TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

- n) Go back to the root user.
- o) In IBM Cognos Configuration, from the Actions menu, click Test.

You are testing the connection between content manager and the content store database.

- p) In the **informational** window, click **Close**.
- 10. Optional: On *Server B*, you can change the IBM Cognos Analytics ports to match the ports that are used by Jazz for Service Management and Tivoli Common Reporting.

You would do this so that you do not have to get new firewall exceptions for the default Cognos Analytics ports.

- a) While you are still in IBM Cognos Configuration, in the Explorer window, click Environment.
- b) In the **Group Properties** window, select the **Value** next to the **URI** property and change the following properties (names):

Table 32. Group Property values		
Property	Change the value to	
Gateway URI	Computer fully qualified domain name (for	
External dispatcher URI	example, <i>myserver.mycompany.com</i>).	
Internal dispatcher URI Dispatcher URI for external applications	 The https protocol. The 9300 port to the value of the WC_defaulthost_secure parameter in the 	
		Content Manager URIs

- c) From the **File** menu, click **Save**.
- d) In the informational window, click Close.
- 11. Start IBM Cognos Analytics (content manager and application services), on Server B.

It might take Cognos Analytics a few minutes to start.

- a) While you are still in IBM Cognos Configuration, in the **Explorer** window, click **Local Configuration**.
- b) From the **Actions** menu, click **Test**.

Tip: If you are not configuring Cognos Analytics to send notifications, you can ignore the testing the mail server connection failure message.

- c) In the informational window, click Close.
- d) From the **Actions** menu, click **Start**.

It might take Cognos Analytics a few minutes to start.

- 12. Exit IBM Cognos Configuration on Server B.
- 13. On *Server B*, copy the exported file that you created in Step 1 to the *Cognos_installation_dir/* deployment/ directory.
- 14. Import content into Cognos Analytics on Server B.
 - a) Open a web browser and enter either of the following URLs:

http://FQDN_0f_Your_Machine:port/bi

Or

https://FQDN_Of_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 10 (Optional). If you *did not* perform Step 10, the default port value is 9300.



Warning: At this point Cognos Analytics is configured with anonymous access so that anyone is able to access it.

- b) In the lower left-hand part of the page, select **Manage** > **Administration console**.
- c) In the IBM Cognos Administration GUI, select the **Configuration** tab.
- d) In the **Configuration** tab, select **Content Administration**.
- e) On the toolbar, click the **New Import** icon.

It is the fourth icon in the list.

- f) On the **Select a deployment archive** page, select the name of the file that you exported from Jazz for Service Management in Step 1 and click **Next**.
- g) On the **Enter the encryption password** page, enter the encryption password that you created in Step 1 and click **OK**.
- h) On the **Specify a name and description** page, enter a name for your import (or keep the default setting) and click **Next**.
- i) On the **Select the public folders, directory, and library content** page, select the following items to import:
 - Custom content that you exported.
 - IBM Spectrum Control Packages and (or the IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or the IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or the IBM Tivoli Storage Productivity Center Report Layouts).

j) Accept the default settings in the **Options** section and click **Next**.

Tip: If you want to import your schedules with your IBM[®] Cognos[®] Business Intelligence content from Tivoli Common Reporting, complete the following steps:

1) In the **Options** section, verify that **Include schedules** is selected.

2) In the Options section, verify that Conflict resolution is set to Replace existing entries.3) Click Next.

- 3) Click **Next**.
- k) On the Select directory content page, verify that Include data sources and connections and Include signons are selected and that Conflict resolution is set to Replace existing entries and click Next.
- l) On the **Specify the general options** page, click **Next**.
- m) On the Review the summary page, click Next.
- n) On the Select an action page, select Save and run once and click Finish.
- o) On the **Run with Options** page, select **Upgrade all report specifications to the latest version** and **Assign new IDs during import**.
- p) Click **Run**.
- q) On the IBM Cognos software page, select View the details of this import after closing this dialog and click OK.
- r) On the View run history details page, click Refresh.

Check the **Status** field to monitor that the job is executing. Do *not* log off from the IBM Cognos Administration GUI until the import job is complete.

Tip: The import job might take approximately 15 minutes or more to resolve. Click **Refresh** periodically to check the status.

The results of importing the reports and schedules into Cognos Analytics contain the following similar messages:

```
CM-REQ-4328 A problem was encountered while importing the object
"/content/folder[@name="IBM Spectrum Control Predefined Reports"]/
folder[@name="Servers"]/report[@name="Servers Capacity"]/schedule".
CM-REQ-4329 The following references cannot be resolved and were cleared:
"credential: CAMID("VMMProvider:smadmin")/credential[@name='Credential '] ".
CM-REQ-4328 A problem was encountered while importing the object
"/content/folder[@name="IBM Spectrum Control Predefined Reports"]/
folder[@name="Servers"]/report[@name="Servers Capacity"]/
schedule[@name="2018-04-27T18:03:22.638Z"]".
```

CM-REQ-3282 The schedule will not run because the credential is missing.

You can safely ignore the messages as they are expected.

- s) After the import job is complete, check the **Completion time** and **Status** fields to verify that the job is complete. If it is complete, on the **View an import deployment record** page, click **Close**.
- t) To exit the IBM Cognos Administration GUI, close the browser tab.
- 15. Verify that the imported content is displayed in Cognos Analytics on Server B.
 - a) Return to the browser tab where the Cognos Analytics GUI is running. If it is not running, open a web browser and enter either of the following URLs:

http://FQDN_Of_Your_Machine:port/bi

Or

https://FQDN_Of_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 10 (Optional).

If you did perform Step 10, then you will use https. If you *did not* perform Step 10, then you use http.

If you *did not* perform Step 10, the default port value is 9300.

- b) On the IBM Cognos Analytics Welcome page, click Team content.
- c) Verify that the following content is listed:

- Custom content that you saved to Public Folders before you ran this procedure.
- IBM Spectrum Control Packages and (or IBM Tivoli Storage Productivity Center Packages).
- IBM Spectrum Control Predefined Reports and (or IBM Tivoli Storage Productivity Center Predefined Reports).
- IBM Spectrum Control Report Layouts and (or IBM Tivoli Storage Productivity Center Report Layouts).
- d) Optional: Attempt to generate a custom report or a predefined report and verify the contents.

Important: If you encounter APAR IT23800 or other problems when generating a predefined report in Cognos Analytics that was migrated from Tivoli Common Reporting, import the predefined reports package for the version of IBM Spectrum Control you are currently running on your system.

If you encounter APAR IT23800 or other problems when generating a custom report in Cognos Analytics that was migrated from Tivoli Common Reporting, you must update or recreate the custom report to use the predefined reports package for the version of IBM Spectrum Control you are currently running and remove references to tables that are no longer used in the IBM Spectrum Control database repository.

16. After you import the report content and schedules into Cognos Analytics, the schedules will not run due to missing credentials.

To update the schedules in Cognos Analytics with the correct credentials, complete the following steps:

a. Return to the browser tab where the Cognos Analytics GUI is running. If it is not running, open a web browser and enter either of the following URLs:

http://FQDN_0f_Your_Machine:port/bi

Or

https://FQDN_Of_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 10 (Optional).

If you did perform Step 10, then you will use https. If you *did not* perform Step 10, then you use http.

If you *did not* perform Step 10, the default port value is 9300.

- b. On the IBM Cognos Analytics Welcome page, click Team content.
- c. Select a report that has an existing schedule.
- d. Select the **Properties** for the report.
- e. Select the **Schedule** tab.
- f. Select the > icon to open the schedule.
- g. Click **Update** on the schedule page.

Repeat steps c-g for each migrated report schedule you want to run in Cognos Analytics.

You migrated your custom IBM[®] Cognos[®] Business Intelligence reports and upgraded to the latest version of IBM Spectrum Control and are able to use Cognos[®] BI reports.

Change the configuration of IBM Cognos Analytics from anonymous access to authenticated access.

For more information, see Configuring an LDAP namespace for IBM Directory Server.

For more information, see Configuring an LDAP namespace for Active Directory Server.

For more information, see Managing user authentication.

Related tasks

<u>"Importing IBM Spectrum Control pre-defined reports package " on page 96</u> Complete this procedure to import the IBM Spectrum Control predefined reports package into the IBM Cognos Analytics reporting tool.

Related information

APAR IT23800 Upgrading Db2 servers Upgrading a Db2 server (Linux and UNIX) IBM Cognos Analytics server components Install and configure server components Installing server components on UNIX or Linux operating systems Installing Content Manager on UNIX or Linux operating systems Installing the Application services components on UNIX or Linux operating systems

Migrating Cognos BI reports to IBM Cognos Analytics in a multiple server Linux environment with remote Jazz for Service Management

If you do not have custom report content, you can skip this migration procedure. You can upgrade to IBM[®] Cognos[®] Analytics 11.0.9 or later when you upgrade to the latest version of IBM Spectrum Control. Complete this procedure to migrate your existing custom report content from Tivoli Common Reporting to Cognos Analytics.

Review the content of <u>Migrating reports to IBM Cognos Analytics during upgrade</u> before you start this procedure.

For this procedure, the terms *Server A* and *Server B* denote the two servers. *Server A* has DB2[®] Enterprise Server Edition, IBM Spectrum Control database repository, and the IBM Spectrum Control servers installed. *Server B* has DB2[®] Enterprise Server Edition, Jazz for Service Management, and Cognos Analytics installed.

Important: Only reports in the Cognos Analytics Public Folders are migrated to IBM[®] Cognos[®] Analytics 11.0.9 or later. If you saved reports to My Folder, you must save them again in Public Folders before you migrate them.

If you plan to upgrade Db2 as part of your upgrade to the latest version of IBM Spectrum Control, upgrade Db2 on *Server A*, upgrade the IBM Spectrum Control database (TPCDB) on *Server A*, upgrade Db2 on *Server B* and then upgrade the Tivoli Common Reporting Content Store database (TCRDB) on *Server B*.

A high level overview on completing this upgrade:

- Export content from Tivoli Common Reporting on Server B.
- Upgrade IBM Spectrum Control on Server A.
- Uninstall IBM Spectrum Control on Server B.
- (Optional) Uninstall Tivoli Common Reporting, Jazz for Service Management, IBM[®] WebSphere[®] Application Server, and Installation Manager, from *Server B*.
- Install and configure Cognos Analytics on Server B.
- Import content into IBM Cognos Analytics on Server B and then verify the content.

Verify that you have the following prerequisite packages installed on *Server B* for IBM Cognos Analytics 11.0.9 or later.

The prerequisite packages for Red Hat Enterprise Linux (RHEL) 6 are:

glibc-2.12-1.166.el6 or later (both i686 and x86_64 packages) libstdc++-4.4.7-16.el6 or later (both i686 and x86_64 packages) nspr-4.9.2-1.el6 or later (both i686 and x86_64 packages) nss-3.14.0.0-12.el6 or later (both i686 and x86_64 packages) openmotif-2.3.3-5.el6 or later (both i686 and x86_64 packages)

The prerequisite packages for Red Hat Enterprise Linux (RHEL) 7 are:

glibc-2.17-55.el7 or later (both i686 and x86_64 packages) libstdc++-4.8.2-16.el7 or later (both i686 and x86_64 packages) nspr-4.10.2-4.el7 or later (both i686 and x86_64 packages) nss-3.15.4-6.el7 or later (both i686 and x86_64 packages) motif-2.3.4-7.el7 or later (both i686 and x86_64 packages)

For more information, see Software Product Compatibility Reports.

You need to set the correct ulimit values for *Server B* in the /etc/security/limits.conf file for Cognos Analytics.

Here is an example of the entries you might need to add to the /etc/security/limits.conf file:

*	soft hard	nproc	unlimited unlimited
*	soft	nofile	8192
* *	nard soft	noiile stack	8192 unlimited
*	hard	stack	unlimited

After you set and save your ulimit values, restart your computer and verify the correct ulimit values.

For more information, see Set the ulimit values on UNIX and Linux operating systems .

- 1. Log in to Jazz for Service Management and Tivoli Common Reporting on Server B to export content.
 - a) Open a web browser and enter the following URL:

https://FQDN_0f_Your_Machine:port/tarf/servlet/dispatch

Where https is the protocol, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*) and the *port* value is the secure HTTP port number that was specified during the installation of Jazz for Service Management.

To determine the secure HTTP port number for Jazz for Service Management, open the *JazzSM_installation_dir*/profile/properties/portdef.props file. The default *JazzSM_installation_dir* value is /opt/IBM/JazzSM. The port number is the value that is assigned to the **WC_defaulthost_secure** parameter. The default value is 16311.

If you receive a security certificate warning when you attempt to connect to the server, confirm the security exception and continue to the web page.

- b) Log in to the reporting interface using the Jazz for Service Management user name that was created when you installed Jazz for Service Management. The default value is smadmin.
- c) Select Launch > IBM Cognos Administration.
- d) In the IBM Cognos Administration GUI, select the **Configuration** tab.
- e) In the Configuration tab, select Content Administration.
- f) On the toolbar, click the **New Export** icon.

It is the third icon in the list.

- g) On the **Specify a name and description** page, enter a name for your export package and click **Next**.
- h) On the **Choose a deployment method** page, select **Select public folders and directory content** and click **Next**.
- i) On the Select the public folders content page, click the Add link.
- j) On the **Select entries** page, select the following items to export.
 - Custom content that you saved to Public Folders before running this procedure.
 - IBM Spectrum Control Packages and (or the IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or the IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or the IBM Tivoli Storage Productivity Center Report Layouts).

- k) Click the **Green** arrow to transfer the content to the list.
- l) Click **OK**.
- m) On the Select the public folders content page, click Next.

Tip: If you want to export your schedules with your IBM[®] Cognos[®] Business Intelligence content from Tivoli Common Reporting, complete the following steps:

- 1) On the Select the public folders content page, select Include schedules.
- 2) Set Conflict resolution to Replace existing entries.
- 3) Click Next.
- n) On the **Select the directory content** page, select **Include data sources and connections** and **Include signons**.
- o) Set Conflict resolution to Replace existing entries and click Next.
- p) On the **Specify the general options** page, click **Next**.
- q) On the Specify a deployment archive page, click Set the encryption password.
- r) On the **Enter the encryption password** page, enter, and then confirm your password and click **OK**.

Tip: The encryption password is *not* an existing password in IBM Spectrum Control, Db2 or the operating system. The encryption password is a new password for the purpose of securing the content you are exporting from Jazz for Service Management and Tivoli Common Reporting.

Make note of your new password. You will need to provide it later in this procedure.

- s) On the Specify a deployment archive page, click Next.
- t) On the **Review the summary** page, click **Next**.
- u) On the Select an action page, select Save and run once and click Finish.
- v) On the **Run with options** page, click **Run**.
- w) On the **IBM Cognos software** page, select **View the details of this report after closing this dialog** and click **OK**.
- x) On the View run history details page, click Refresh.

Do not log off from the IBM Cognos Administration GUI until the export job is complete. You can click **Refresh** periodically to check the status of the export job.

- y) After the export job is complete, on the View an export deployment record page, click Close.
- z) Log off from the reporting interface.
- aa) Copy the exported file from the JazzSM_installation_dir/reporting/cognos/ deployment/ directory to a directory that is outside of the Jazz for Service Management installation directory.

Make note of the name and location of this exported file. You will need this information in Step 13.

Tip: If you *do not* copy the exported file outside of the Jazz for Service Management installation directory, the exported file is deleted when you uninstall Tivoli Common Reporting.

2. Upgrade Server A to the latest version of IBM Spectrum Control.

For more information, see Upgrading from Tivoli Storage Productivity Center Version 5.2.0 and later with a remote database by using the installation program.

- 3. Upgrade *Server B* to the latest version of IBM Spectrum Control. You are then instructed to uninstall IBM Spectrum Control from *Server B*. Uninstall IBM Spectrum Control from *Server B*. For more information, see Uninstalling IBM Spectrum Control.
- 4. Optional: Uninstall Tivoli Common Reporting, Jazz for Service Management, WebSphere Application Server, and Installation Manager from *Server B*.

For more information, see Uninstalling Tivoli Common Reporting and Jazz for Service Management.

If you *did not* uninstall Tivoli Common Reporting, Jazz for Service Management, WebSphere Application Server, and Installation Manager, you *must* stop Jazz for Service Management and Tivoli Common Reporting before you proceed with the rest of this procedure.

To stop Jazz for Service Management and Tivoli Common Reporting, open a command prompt and enter the following command:

JazzSM_installation_dir/profile/bin/stopServer.sh server_name -username JazzSM_username -password JazzSM_password

For example:

/opt/IBM/JazzSM/profile/bin/stopServer.sh server1 -username smadmin -password abc123

5. Install IBM Cognos Analytics 11.0.9 or later on Server B.

Tip: You do not need to set the **JAVA_HOME** environment variable before you start the IBM Cognos Analytics Version 11.0.9 or later installation program.

- a) Log in to your computer as a user with root privileges.
- b) Start the IBM Cognos Analytics installation program.
- c) Select the language to use for your installation and click **Next**.
- d) On the **Product installation** page, select **IBM Cognos Analytics (IBM Bundler Edition)** and click **Next**.
- e) On the License agreement page, accept the License Agreement and click Next.
- f) On the Location page, provide your installation location and click Next.

Make note of your Cognos Analytics installation location. You will need to provide it later in this procedure.

Tip: If you want the IBM Cognos Analytics installation to automatically create the installation location for you, click **Yes**.

- g) On the Installation type page, select First install and click Next.
- h) On the **Choose components** page, accept the default selections, and click **Next**.
- i) On the Pre-installation summary page, review your information for accuracy and click Install.
- j) When the installation is complete, click **Done**.
- 6. On Server B, copy the following Db2 JDBC driver files from the /opt/ibm/db2/version/java/ directory to the Cognos_installation_dir/drivers/ directory :
 - db2jcc.jar
 - db2jcc_license_cu.jar
 - db2jcc4.jar
- 7. On Server B, open a command prompt and enter the following command as the root user:

```
cd Cognos_installation_dir/drivers/
chmod +x db2jcc*.jar
```

8. On Server B, open a command prompt and enter the following command as the root user:

```
ln -s Db2_instance_owner_home_directory/sqllib/lib32/libdb2.so
Cognos_installation_dir/bin/
```

IBM Spectrum Control Predefined Reports use Compatibility Query Mode. IBM Cognos Analytics needs to use the 32-Bit Db2 library in order to connect to the IBM Spectrum Control database as a data source.

- 9. Create the content store for Cognos Analytics on Server B.
 - a) Open a command prompt and enter the following commands to start IBM Cognos Configuration:

```
cd Cognos_installation_dir/bin64/
. /home/db2inst1/sqllib/db2profile
```

./cogconfig.sh

Notice the space between the . and the / in the second command.

- b) In the **Explorer** window, expand **Data Access** > **Content Manager** and click **Content Store**.
- c) In the Type property, enter DB2 database, if it is not already displayed.
- d) In the **Database server and port number** property, enter localhost or the fully qualified domain name of the machine.

For example, localhost: 50000 or *FQDN_0f_Your_Machine*: 50000 where 50000 is the default port number that is used by Db2.

Tip: If you are using a different port number, ensure that you use that value. To determine the port that is used by Db2, examine the **varDBPort** parameter in the *SC_installation_dir/* config/InstallVariable.properties file.

e) In the **User ID and password** property, enter the user name of the owner of the Db2 instance where the content store database will be located and the password that is associated with that user name

Typically, this user name is *db2inst1*.

- f) In the **Database name** property, verify that the default value is **cm**.
- g) From the File menu, click Save.

This step might take a few minutes to complete. Track the progress in the window.

- h) In the informational window, click Close.
- i) In the Explorer window, expand Data Access > Content Manager and click Content Store.
- j) Right-click Content Store and click Generate DDL.
- k) In the informational window, click Close.

Important: Do not exit IBM Cognos Configuration in this step. Wait until Step 12.

- l) While you are logged into the Linux operating system as the root user, switch to the user that is the Db2 instance owner (for example, *db2inst1*).
- m) Open a command prompt and enter the following Db2 command:

 $db2 \ \text{-tvf} \ \textit{Cognos_installation_dir/configuration/schemas/content/db2/createDb.sql}$

If the results of this command contain the following similar messages, you can safely ignore those messages because the Db2 instance owner already has the necessary privileges:

GRANT CREATETAB,BINDADD,CONNECT,IMPLICIT_SCHEMA ON DATABASE TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

GRANT CREATEIN, DROPIN, ALTERIN ON SCHEMA DB2COGNOS TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

GRANT USE OF TABLESPACE TSN_USR_cm TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

GRANT USE OF TABLESPACE TSN_REG_cm TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

- n) Go back to the root user.
- o) In IBM Cognos Configuration, from the **Actions** menu, click **Test**.

You are testing the connection between content manager and the content store database.

p) In the informational window, click Close.

10. Optional: On *Server B*, you can change the IBM Cognos Analytics ports to match the ports that are used by Jazz for Service Management and Tivoli Common Reporting.

You would do this so that you do not have to get new firewall exceptions for the default Cognos Analytics ports.

- a) While you are still in IBM Cognos Configuration, in the **Explorer** window, click **Environment**.
- b) In the **Group Properties** window, select the **Value** next to the **URI** property and change the following properties (names):

Table 33. Group Property values		
Property	Change the value to	
Gateway URI	• Computer fully qualified domain name (for	
External dispatcher URI	example, <i>myserver.mycompany.com</i>).	
Internal dispatcher URI	 The https protocol. The 9300 port to the value of the WC_defaulthost_secure parameter in the 	
Dispatcher URI for external applications		
Content Manager URIs	JazzSM_installation_dir\profile \properties\portdef.props file. The default value is 16311.	

- c) From the **File** menu, click **Save**.
- d) In the informational window, click Close.
- 11. Start IBM Cognos Analytics (content manager and application services), on Server B.

It might take Cognos Analytics a few minutes to start.

- a) While you are still in IBM Cognos Configuration, in the **Explorer** window, click **Local Configuration**.
- b) From the Actions menu, click Test.

Tip: If you are not configuring Cognos Analytics to send notifications, you can ignore the testing the mail server connection failure message.

- c) In the **informational** window, click **Close**.
- d) From the Actions menu, click Start.

It might take Cognos Analytics a few minutes to start.

- 12. Exit IBM Cognos Configuration on Server B.
- 13. On *Server B*, copy the exported file that you created in Step 1 to the *Cognos_installation_dir/* deployment/ directory.
- 14. Import content into Cognos Analytics on Server B.
 - a) Open a web browser and enter either of the following URLs:

```
http://FQDN_0f_Your_Machine:port/bi
```

Or

```
https://FQDN_Of_Your_Machine:port/bi
```

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 10 (Optional). If you *did not* perform Step 10, the default port value is 9300.



Warning: At this point Cognos Analytics is configured with anonymous access so that anyone is able to access it.

- b) In the lower left-hand part of the page, select Manage > Administration console.
- c) In the IBM Cognos Administration GUI, select the **Configuration** tab.
- d) In the Configuration tab, select Content Administration.
- e) On the toolbar, click the **New Import** icon.

It is the fourth icon in the list.

- f) On the Select a deployment archive page, select the name of the file that you exported from Jazz for Service Management in Step 1 and click Next.
- g) On the **Enter the encryption password** page, enter the encryption password that you created in Step 1 and click **OK**.
- h) On the **Specify a name and description** page, enter a name for your import (or keep the default setting) and click **Next**.
- i) On the Select the public folders, directory, and library content page, select the following items to import:
 - Custom content that you exported.
 - IBM Spectrum Control Packages and (or the IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or the IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or the IBM Tivoli Storage Productivity Center Report Layouts).

j) Accept the default settings in the **Options** section and click **Next**.

Tip: If you want to import your schedules with your IBM[®] Cognos[®] Business Intelligence content from Tivoli Common Reporting, complete the following steps:

- 1) In the **Options** section, verify that **Include schedules** is selected.
- 2) In the **Options** section, verify that **Conflict resolution** is set to **Replace existing entries**.

3) Click Next.

- k) On the Select directory content page, verify that Include data sources and connections and Include signons are selected and that Conflict resolution is set to Replace existing entries and click Next.
- l) On the **Specify the general options** page, click **Next**.
- m) On the **Review the summary** page, click **Next**.
- n) On the Select an action page, select Save and run once and click Finish.
- o) On the **Run with Options** page, select **Upgrade all report specifications to the latest version** and **Assign new IDs during import**.
- p) Click Run.
- q) On the IBM Cognos software page, select View the details of this import after closing this dialog and click OK.
- r) On the View run history details page, click Refresh.

Check the **Status** field to monitor that the job is executing. Do *not* log off from the IBM Cognos Administration GUI until the import job is complete.

Tip: The import job might take approximately 15 minutes or more to resolve. Click **Refresh** periodically to check the status.

The results of importing the reports and schedules into Cognos Analytics contain the following similar messages:

CM-REQ-4328 A problem was encountered while importing the object "/content/folder[@name="IBM Spectrum Control Predefined Reports"]/ folder[@name="Servers"]/report[@name="Servers Capacity"]/schedule". CM-REQ-4329 The following references cannot be resolved and were cleared: "credential: CAMID("VMMProvider:smadmin")/credential[@name='Credential '] ". CM-REQ-4328 A problem was encountered while importing the object "/content/folder[@name="IBM Spectrum Control Predefined Reports"]/ folder[@name="Servers"]/report[@name="Servers Capacity"]/ schedule[@name="2018-04-27T18:03:22.638Z"]". CM-REQ-3282 The schedule will not run because the credential is missing.

You can safely ignore the messages as they are expected.

- s) After the import job is complete, check the **Completion time** and **Status** fields to verify that the job is complete. If it is complete, on the **View an import deployment record** page, click **Close**.
- t) To exit the IBM Cognos Administration GUI, close the browser tab.
- 15. Verify that the imported content is displayed in Cognos Analytics on Server B.
 - a) Return to the browser tab where the Cognos Analytics GUI is running. If it is not running, open a web browser and enter either of the following URLs:

http://FQDN_0f_Your_Machine:port/bi

Or

https://FQDN_Of_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 10 (Optional).

If you did perform Step 10, then you will use https. If you *did not* perform Step 10, then you use http.

If you *did not* perform Step 10, the default port value is 9300.

- b) On the IBM Cognos Analytics Welcome page, click Team content.
- c) Verify that the following content is listed:
 - Custom content that you saved to Public Folders before you ran this procedure.
 - IBM Spectrum Control Packages and (or IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or IBM Tivoli Storage Productivity Center Report Layouts).
- d) Optional: Attempt to generate a custom report or a predefined report and verify the contents.

Important: If you encounter APAR IT23800 or other problems when generating a predefined report in Cognos Analytics that was migrated from Tivoli Common Reporting, import the predefined reports package for the version of IBM Spectrum Control you are currently running on your system.

If you encounter APAR IT23800 or other problems when generating a custom report in Cognos Analytics that was migrated from Tivoli Common Reporting, you must update or recreate the custom report to use the predefined reports package for the version of IBM Spectrum Control you are currently running and remove references to tables that are no longer used in the IBM Spectrum Control database repository.

16. After you import the report content and schedules into Cognos Analytics, the schedules will not run due to missing credentials.

To update the schedules in Cognos Analytics with the correct credentials, complete the following steps:

a. Return to the browser tab where the Cognos Analytics GUI is running. If it is not running, open a web browser and enter either of the following URLs:

http://FQDN_Of_Your_Machine:port/bi

https://FQDN_Of_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 10 (Optional).

If you did perform Step 10, then you will use https. If you *did not* perform Step 10, then you use http.

If you *did not* perform Step 10, the default port value is 9300.

- b. On the IBM Cognos Analytics Welcome page, click Team content.
- c. Select a report that has an existing schedule.
- d. Select the **Properties** for the report.
- e. Select the **Schedule** tab.
- f. Select the > icon to open the schedule.
- g. Click **Update** on the schedule page.

Repeat steps c-g for each migrated report schedule you want to run in Cognos Analytics.

You migrated your custom IBM[®] Cognos[®] Business Intelligence reports and upgraded to the latest version of IBM Spectrum Control and are able to use Cognos[®] BI reports.

Change the configuration of IBM Cognos Analytics from anonymous access to authenticated access.

For more information, see Configuring an LDAP namespace for IBM Directory Server.

For more information, see Configuring an LDAP namespace for Active Directory Server.

For more information, see Managing user authentication.

Related tasks

"Importing IBM Spectrum Control pre-defined reports package " on page 96 Complete this procedure to import the IBM Spectrum Control predefined reports package into the IBM Cognos Analytics reporting tool.

Related information

APAR IT23800 Upgrading Db2 servers Upgrading a Db2 server (Linux and UNIX) IBM Cognos Analytics server components Install and configure server components Installing server components on UNIX or Linux operating systems Installing Content Manager on UNIX or Linux operating systems Installing the Application services components on UNIX or Linux operating systems

Migrating Cognos BI reports to IBM Cognos Analytics in a single AIX environment

If you do not have custom report content, you can skip this migration procedure. You can upgrade to IBM[®] Cognos[®] Analytics 11.0.9 or later when you upgrade to the latest version of IBM Spectrum Control. Complete this procedure to migrate your existing custom report content from Tivoli Common Reporting to Cognos Analytics.

Review the content of <u>Migrating reports to IBM Cognos Analytics during upgrade</u> before you start this procedure.

This procedure assumes that you installed Db2[®], IBM Spectrum Control 5.2.15 or earlier, IBM[®]Jazz for Service Management, IBM[®] Tivoli Common Reporting on a single AIX[®] computer.

Important:

Only reports in the Cognos Analytics Public Folders are exported from Tivoli Common Reporting. If you saved reports to Private Folders or My Folder, you *must* save them again in Public Folders before you export them.

If you plan to upgrade Db2 as part of your upgrade to the latest version of IBM Spectrum Control, upgrade Db2, upgrade the IBM Spectrum Control database (TPCDB) and then upgrade the Tivoli Common Reporting Content Store database (TCRDB).

A high level overview of the migration:

- Export content from Tivoli Common Reporting.
- Upgrade IBM Spectrum Control.
- (Optional) Uninstall Tivoli Common Reporting, Jazz for Service Management, IBM® WebSphere® Application Server, and Installation Manager.
- Install and configure Cognos Analytics.
- Import content into Cognos Analytics and then verify the content.

Verify that you have the following prerequisite packages installed on a AIX computer for IBM Cognos Analytics 11.0.9 or later.

The prerequisites for AIX 6.1 are:

- TL7
- SP05 (6100-07-05-1228)
- IBM XL C/C++ for AIX, 12.1 Runtime Environment
- bos.pmapi.lib

The prerequisites for AIX 7.1 are:

- IBM XL C/C++ for AIX, 12.1 Runtime Environment
- bos.pmapi.lib

For more information, see Software Product Compatibility Reports.

You need to set the correct ulimit values in the /etc/security/limits file for IBM Cognos Analytics Version 11.0.9 or later.

Here is an example of the entries you might need to add to the /etc/security/limits file:

```
default:
fsize = -1
cpu = -1
rss = -1
stack = 16384
nofiles = 8192
```

After you set and save your ulimit values, restart your computer and verify the correct ulimit values.

For more information, see Set the ulimit values on UNIX and Linux operating systems .

- 1. Log in to Jazz for Service Management and Tivoli Common Reporting to export content.
 - a) Open a web browser and enter the following URL:

https://FQDN_0f_Your_Machine:port/tarf/servlet/dispatch

Where https is the protocol, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*) and the *port* value is the secure HTTP port number that was specified during the installation of Jazz for Service Management.

To determine the secure HTTP port number for Jazz for Service Management, open the JazzSM_installation_dir/profile/properties/portdef.props file. The default JazzSM_installation_dir value is /opt/IBM/JazzSM. The port number is the value that is assigned to the **WC_defaulthost_secure** parameter. The default value is 16311. If you receive a security certificate warning when you attempt to connect to the server, confirm the security exception and continue to the web page.

- b) Log in to the reporting interface using the Jazz for Service Management user name that was created when you installed Jazz for Service Management. The default value is smadmin.
- c) Select Launch > IBM Cognos Administration.
- d) In the IBM Cognos Administration GUI, select the **Configuration** tab.
- e) In the Configuration tab, select Content Administration.
- f) On the toolbar, click the **New Export** icon.

It is the third icon in the list.

- g) On the **Specify a name and description** page, enter a name for your export package and click **Next**.
- h) On the **Choose a deployment method** page, select **Select public folders and directory content** and click **Next**.
- i) On the Select the public folders content page, click the Add link.
- j) On the **Select entries** page, select the following items to export.
 - Custom content that you saved to Public Folders before running this procedure.
 - IBM Spectrum Control Packages and (or the IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or the IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or the IBM Tivoli Storage Productivity Center Report Layouts).
- k) Click the **Green** arrow to transfer the content to the list.
- l) Click **OK**.
- m) On the Select the public folders content page, click Next.

Tip: If you want to export your schedules with your IBM[®] Cognos[®] Business Intelligence content from Tivoli Common Reporting, complete the following steps:

- 1) On the Select the public folders content page, select Include schedules.
- 2) Set Conflict resolution to Replace existing entries.
- 3) Click Next.
- n) On the **Select the directory content** page, select **Include data sources and connections** and **Include signons**.
- o) Set Conflict resolution to Replace existing entries and click Next.
- p) On the Specify the general options page, click Next.
- q) On the Specify a deployment archive page, click Set the encryption password.
- r) On the **Enter the encryption password** page, enter, and then confirm your password and click **OK**.

Tip: The encryption password is *not* an existing password in IBM Spectrum Control, Db2 or the operating system. The encryption password is a new password for the purpose of securing the content you are exporting from Jazz for Service Management and Tivoli Common Reporting.

Make note of your new password. You will need to provide it later in this procedure.

- s) On the Specify a deployment archive page, click Next.
- t) On the **Review the summary** page, click **Next**.
- u) On the Select an action page, select Save and run once and click Finish.
- v) On the **Run with options** page, click **Run**.
- w) On the **IBM Cognos software** page, select **View the details of this report after closing this dialog** and click **OK**.

x) On the View run history details page, click Refresh.

Do not log off from the IBM Cognos Administration GUI until the export job is complete. You can click **Refresh** periodically to check the status of the export job.

- y) After the export job is complete, on the **View an export deployment record** page, click **Close**.
- z) Log off from the reporting interface.
- aa) Copy the exported file from the JazzSM_installation_dir/reporting/cognos/ deployment/ directory to a directory that is outside of the Jazz for Service Management installation directory.

Make note of the name and location of this exported file. You will need this information in Step 12.

Tip: If you *do not* copy the exported file outside of the Jazz for Service Management installation directory, the exported file is deleted when you uninstall Tivoli Common Reporting.

2. Upgrade your system to latest version of IBM Spectrum Control; this step uninstalls the IBM Spectrum Control Cognos BI Reports component.

For more information, see Upgrading IBM Spectrum Control in a single-server environment.

3. Optional: Uninstall Tivoli Common Reporting, Jazz for Service Management, WebSphere Application Server, and Installation Manager.

For more information, see Uninstalling Tivoli Common Reporting and Jazz for Service Management.

If you *did not* uninstall Tivoli Common Reporting, Jazz for Service Management, WebSphere Application Server, and Installation Manager, you *must* stop Jazz for Service Management and Tivoli Common Reporting before you proceed with the rest of this procedure.

To stop Jazz for Service Management and Tivoli Common Reporting, open a command prompt and enter the following command:

```
JazzSM_installation_dir/profile/bin/stopServer.sh server_name
-username JazzSM_username -password JazzSM_password
```

For example:

/opt/IBM/JazzSM/profile/bin/stopServer.sh server1 -username smadmin -password abc123

4. Install IBM Cognos Analytics 11.0.9 or later.

Tip: You do not need to set the **JAVA_HOME** environment variable before you start the IBM Cognos Analytics 11.0.9 or later installation program.

- a) Log in to your computer as a user with root privileges.
- b) Start the IBM Cognos Analytics installation program.
- c) Select the language to use for your installation and click **Next**.
- d) On the **Product installation** page, select **IBM Cognos Analytics (IBM Bundler Edition)** and click **Next**.
- e) On the **License agreement** page, accept the License Agreement and click **Next**.
- f) On the Location page, provide your installation location and click Next.

Make note of your Cognos Analytics installation location. You will need to provide it later in this procedure.

Tip: If you want the IBM Cognos Analytics installation to automatically create the installation location for you, click **Yes**.

- g) On the Installation type page, select First install and click Next.
- h) On the **Choose components** page, accept the default selections, and click **Next**.
- i) On the **Pre-installation summary** page, review your information for accuracy and click **Install**.
- j) When the installation is complete, click **Done**.
- 5. Copy the following Db2 JDBC driver files from the /opt/IBM/db2/version/java/ directory to the Cognos_installation_dir/drivers/ directory :

- db2jcc.jar
- db2jcc_license_cu.jar
- db2jcc4.jar

6. Open a command prompt and enter the following command as the root user:

cd Cognos_installation_dir/drivers/
chmod +x db2jcc*.jar

7. Open a command prompt and enter the following command as the root user:

ln -s Db2_instance_owner_home_directory/sqllib/lib32/libdb2.a Cognos_installation_dir/bin/

IBM Spectrum Control Predefined Reports use Compatibility Query Mode. Cognos Analytics needs to use the 32-Bit Db2 library in order to connect to the IBM Spectrum Control database as a data source.

8. Create the content store for Cognos Analytics.

a) Open a command prompt and enter the following commands to start IBM Cognos Configuration:

```
cd Cognos_installation_dir/bin64/
. /home/db2inst1/sqllib/db2profile
./cogconfig.sh
```

Notice the space between the . and the / in the second command.

- b) In the Explorer window, expand Data Access > Content Manager and click Content Store.
- c) In the Type property, enter DB2 database, if it is not already displayed.
- d) In the **Database server and port number** property, enter localhost or the fully qualified domain name of the machine.

For example, localhost: 50000 or *FQDN_Of_Your_Machine*: 50000 where 50000 is the default port number that is used by Db2.

Tip: If you are using a different port number, ensure that you use that value. To determine the port that is used by Db2, examine the **varDBPort** parameter in the SC_installation_dir/ config/InstallVariable.properties file.

e) In the **User ID and password** property, enter the user name of the owner of the Db2 instance where the content store database will be located and the password that is associated with that user name

Typically, this user name is *db2inst1*.

- f) In the Database name property, verify that the default value is cm.
- g) From the File menu, click Save.

This step might take a few minutes to complete. Track the progress in the window.

- h) In the informational window, click Close.
- i) In the Explorer window, expand Data Access > Content Manager and click Content Store.
- j) Right-click Content Store and click Generate DDL.
- k) In the **informational** window, click **Close**.

Important: Do not exit IBM Cognos Configuration in this step. Wait until Step 11.

- l) While you are logged into the AIX operating system as the root user, switch to the user that is the Db2 instance owner (for example, *db2inst1*).
- m) Open a command prompt and enter the following Db2 command:

 $db2 \ \text{-tvf} \ \textit{Cognos_installation_dir/configuration/schemas/content/db2/createDb.sql}$

If the results of this command contain the following similar messages, you can safely ignore those messages because the Db2 instance owner already has the necessary privileges:

GRANT CREATETAB,BINDADD,CONNECT,IMPLICIT_SCHEMA ON DATABASE TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

GRANT CREATEIN, DROPIN, ALTERIN ON SCHEMA DB2COGNOS TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

GRANT USE OF TABLESPACE TSN_USR_cm TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

GRANT USE OF TABLESPACE TSN_REG_cm TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

- n) Go back to the root user.
- o) In IBM Cognos Configuration, from the Actions menu, click Test.

You are testing the connection between content manager and the content store database.

- p) In the **informational** window, click **Close**.
- 9. Optional: You can change the IBM Cognos Analytics ports to match the ports that are used by Jazz for Service Management and Tivoli Common Reporting.

You would do this so that you do not have to get new firewall exceptions for the default Cognos Analytics ports.

- a) While you are still in IBM Cognos Configuration, in the Explorer window, click Environment.
- b) In the **Group Properties** window, select the **Value** next to the **URI** property and change the following properties (names):

Table 34. Group Property values		
Property	Change the value to	
Gateway URI	• Computer fully qualified domain name (for	
External dispatcher URI	example, <i>myserver.mycompany.com</i>).	
Internal dispatcher URI Dispatcher URI for external applications	 The https protocol. The 9300 port to the value of the WC_defaulthost_secure parameter in the 	
		Content Manager URIs

- c) From the **File** menu, click **Save**.
- d) In the informational window, click Close.
- 10. Start Cognos Analytics (content manager and application services).

It might take Cognos Analytics a few minutes to start.

- a) While you are still in IBM Cognos Configuration, in the **Explorer** window, click **Local Configuration**.
- b) From the Actions menu, click Test.

Tip: If you are not configuring Cognos Analytics to send notifications, you can ignore the testing the mail server connection failure message.

- c) In the **informational** window, click **Close**.
- d) From the Actions menu, click Start.

It might take Cognos Analytics a few minutes to start.

- 11. Exit IBM Cognos Configuration.
- 12. Copy the exported file that you created in <u>Step 1</u> to the *Cognos_installation_dir/* deployment/ directory.
- 13. Import content into Cognos Analytics.
 - a) Open a web browser and enter either of the following URLs:

http://FQDN_Of_Your_Machine:port/bi

Or

https://FQDN_0f_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in <u>Step 9</u> (Optional). If you *did not* perform <u>Step 9</u>, the default port value is 9300.



Warning: At this point Cognos Analytics is configured with anonymous access so that anyone is able to access it.

- b) In the lower left-hand part of the page, select Manage > Administration console.
- c) In the IBM Cognos Administration GUI, select the **Configuration** tab.
- d) In the Configuration tab, select Content Administration.
- e) On the toolbar, click the **New Import** icon.

It is the fourth icon in the list.

- f) On the **Select a deployment archive** page, select the name of the file that you exported from Jazz for Service Management in Step 1 and click **Next**.
- g) On the **Enter the encryption password** page, enter the encryption password that you created in <u>Step 1</u> and click **OK**.
- h) On the **Specify a name and description** page, enter a name for your import (or keep the default setting) and click **Next**.
- i) On the **Select the public folders, directory, and library content** page, select the following items to import:
 - Custom content that you exported.
 - IBM Spectrum Control Packages and (or the IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or the IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or the IBM Tivoli Storage Productivity Center Report Layouts).
- j) Accept the default settings in the **Options** section and click **Next**.

Tip: If you want to import your schedules with your IBM[®] Cognos[®] Business Intelligence content from Tivoli Common Reporting, complete the following steps:

1) In the **Options** section, verify that **Include schedules** is selected.

2) In the Options section, verify that Conflict resolution is set to Replace existing entries.3) Click Next.

- k) On the Select directory content page, verify that Include data sources and connections and Include signons are selected and that Conflict resolution is set to Replace existing entries and click Next.
- l) On the **Specify the general options** page, click **Next**.
- m) On the **Review the summary** page, click **Next**.
- n) On the Select an action page, select Save and run once and click Finish.

- o) On the **Run with Options** page, select **Upgrade all report specifications to the latest version** and **Assign new IDs during import**.
- p) Click Run.
- q) On the IBM Cognos software page, select View the details of this import after closing this dialog and click OK.
- r) On the View run history details page, click Refresh.

Check the **Status** field to monitor that the job is executing. Do *not* log off from the IBM Cognos Administration GUI until the import job is complete.

Tip: The import job might take approximately 15 minutes or more to resolve. Click **Refresh** periodically to check the status.

The results of importing the reports and schedules into Cognos Analytics contain the following similar messages:

```
CM-REQ-4328 A problem was encountered while importing the object
"/content/folder[@name="IBM Spectrum Control Predefined Reports"]/
folder[@name="Servers"]/report[@name="Servers Capacity"]/schedule".
CM-REQ-4329 The following references cannot be resolved and were cleared:
"credential: CAMID("VMMProvider:smadmin")/credential[@name='Credential '] ".
CM-REQ-4328 A problem was encountered while importing the object
"/content/folder[@name="IBM Spectrum Control Predefined Reports"]/
folder[@name="Servers"]/report[@name="Servers Capacity"]/
schedule[@name="2018-04-27T18:03:22.638Z"]".
CM-REQ-3282 The schedule will not run because the credential is missing.
```

You can safely ignore the messages as they are expected.

- s) After the import job is complete, check the **Completion time** and **Status** fields to verify that the job is complete. If it is complete, on the **View an import deployment record** page, click **Close**.
- t) To exit the IBM Cognos Administration GUI, close the browser tab.
- 14. Verify that the imported content is displayed in Cognos Analytics.
 - a) Return to the browser tab where the Cognos Analytics GUI is running. If it is not running, open a web browser and enter either of the following URLs:

http://FQDN_0f_Your_Machine:port/bi

Or

https://FQDN_Of_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 9 (Optional).

If you did perform Step 9, then you will use https. If you *did not* perform Step 9, then you use http.

If you *did not* perform Step 9, the default port value is 9300.

- b) On the IBM Cognos Analytics Welcome page, click Team content.
- c) Verify that the following content is listed:
 - Custom content that you saved to Public Folders before you ran this procedure.
 - IBM Spectrum Control Packages and (or IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or IBM Tivoli Storage Productivity Center Report Layouts).
- d) Optional: Attempt to generate a custom report or a predefined report and verify the contents.

Important: If you encounter APAR IT23800 or other problems when generating a predefined report in Cognos Analytics that was migrated from Tivoli Common Reporting, import the predefined reports package for the version of IBM Spectrum Control you are currently running on your system.

If you encounter APAR IT23800 or other problems when generating a custom report in Cognos Analytics that was migrated from Tivoli Common Reporting, you must update or recreate the custom report to use the predefined reports package for the version of IBM Spectrum Control you are currently running and remove references to tables that are no longer used in the IBM Spectrum Control database repository.

15. After you import the report content and schedules into Cognos Analytics, the schedules will not run due to missing credentials.

To update the schedules in Cognos Analytics with the correct credentials, complete the following steps:

a. Return to the browser tab where the Cognos Analytics GUI is running. If it is not running, open a web browser and enter either of the following URLs:

http://FQDN_Of_Your_Machine:port/bi

Or

https://FQDN_Of_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 9 (Optional).

If you did perform Step 9, then you will use https. If you *did not* perform Step 9, then you use http.

If you *did not* perform Step 9, the default port value is 9300.

- b. On the IBM Cognos Analytics Welcome page, click Team content.
- c. Select a report that has an existing schedule.
- d. Select the **Properties** for the report.
- e. Select the Schedule tab.
- f. Select the > icon to open the schedule.
- g. Click **Update** on the schedule page.

Repeat steps c-g for each migrated report schedule you want to run in Cognos Analytics.

You migrated your custom IBM[®] Cognos[®] Business Intelligence reports and upgraded to the latest version of IBM Spectrum Control and are able to use Cognos[®] BI reports.

Change the configuration of IBM Cognos Analytics from anonymous access to authenticated access.

For more information, see Configuring an LDAP namespace for IBM Directory Server.

For more information, see Configuring an LDAP namespace for Active Directory Server.

For more information, see <u>Managing user authentication</u>.

Related tasks

<u>"Importing IBM Spectrum Control pre-defined reports package " on page 96</u> Complete this procedure to import the IBM Spectrum Control predefined reports package into the IBM Cognos Analytics reporting tool.

Related information

APAR IT23800 Upgrading DB2 servers Upgrading a DB2 server (Linux and UNIX) IBM Cognos Analytics server components Install and configure server components Installing server components on UNIX or Linux operating systems Installing Content Manager on UNIX or Linux operating systems Installing the Application services components on UNIX or Linux operating systems

Migrating Cognos BI reports to IBM Cognos Analytics in a multiple server AIX environment with a remote database

If you do not have custom report content, you can skip this migration procedure. You can upgrade to IBM[®] Cognos[®] Analytics 11.0.9 or later when you upgrade to the latest version of IBM Spectrum Control. Complete this procedure to migrate your existing custom report content from Tivoli Common Reporting to Cognos Analytics.

Review the content of <u>Migrating reports to IBM Cognos Analytics during upgrade</u> before you start this procedure.

For this procedure, the terms *Server A* and *Server B* denote the two servers. *Server A* has DB2[®] Enterprise Server Edition and the IBM Spectrum Control database repository installed. *Server B* has all of the other IBM Spectrum Control components installed and DB2[®] Enterprise Server Edition, Jazz for Service Management, and Tivoli Common Reporting.

Important: Only reports in the Cognos Analytics Public Folders are migrated to IBM[®] Cognos[®] Analytics 11.0.9 or later. If you saved reports to My Folder, you must save them again in Public Folders before you migrate them.

If you plan to upgrade Db2 as part of your upgrade to the latest version of IBM Spectrum Control, upgrade Db2 on *Server A*, upgrade the IBM Spectrum Control database (TPCDB) on *Server A*, upgrade Db2 on *Server B* and then upgrade the Tivoli Common Reporting Content Store database (TCRDB) on *Server B*.

A high level overview on completing this upgrade:

- Export content from Tivoli Common Reporting on Server B.
- Upgrade IBM Spectrum Control on Server A.
- Upgrade IBM Spectrum Control on Server B.
- (Optional) Uninstall Tivoli Common Reporting, Jazz for Service Management, IBM[®] WebSphere[®] Application Server, and Installation Manager, from *Server B*.
- Install and configure Cognos Analytics on Server B.
- Import content into Cognos Analytics on Server B and then verify the content.

Verify that you have the following prerequisite packages installed on *Server B* for IBM Cognos Analytics 11.0.9 or later.

The prerequisites for AIX Version 6.1 are:

- TL7
- SP05 (6100-07-05-1228)
- IBM XL C/C++ for AIX, 12.1 Runtime Environment
- bos.pmapi.lib

The prerequisites for AIX 7.1 are:

- IBM XL C/C++ for AIX, 12.1 Runtime Environment
- bos.pmapi.lib

For more information, see Software Product Compatibility Reports.

You need to set the correct ulimit values for *Server B* in the /etc/security/limits file for Cognos Analytics.

Here is an example of the entries you might need to add to the /etc/security/limits file:

default: fsize = -1 core = -1 rss = -1 stack = 16384 nofiles = 8192

After you set and save your ulimit values, restart your computer and verify the correct ulimit values.

For more information, see Set the ulimit values on UNIX and Linux operating systems .

- 1. Log in to Jazz for Service Management and Tivoli Common Reporting on Server B to export content.
 - a) Open a web browser and enter the following URL:

https://FQDN_0f_Your_Machine:port/tarf/servlet/dispatch

Where https is the protocol, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*) and the *port* value is the secure HTTP port number that was specified during the installation of Jazz for Service Management.

To determine the secure HTTP port number for Jazz for Service Management, open the *JazzSM_installation_dir*/profile/properties/portdef.props file. The default *JazzSM_installation_dir* value is /opt/IBM/JazzSM. The port number is the value that is assigned to the **WC_defaulthost_secure** parameter. The default value is 16311.

If you receive a security certificate warning when you attempt to connect to the server, confirm the security exception and continue to the web page.

- b) Log in to the reporting interface using the Jazz for Service Management user name that was created when you installed Jazz for Service Management. The default value is smadmin.
- c) Select Launch > IBM Cognos Administration.
- d) In the IBM Cognos Administration GUI, select the **Configuration** tab.
- e) In the Configuration tab, select Content Administration.
- f) On the toolbar, click the **New Export** icon.

It is the third icon in the list.

- g) On the **Specify a name and description** page, enter a name for your export package and click **Next**.
- h) On the **Choose a deployment method** page, select **Select public folders and directory content** and click **Next**.
- i) On the Select the public folders content page, click the Add link.

j) On the Select entries page, select the following items to export.

- Custom content that you saved to Public Folders before running this procedure.
- IBM Spectrum Control Packages and (or the IBM Tivoli Storage Productivity Center Packages).
- IBM Spectrum Control Predefined Reports and (or the IBM Tivoli Storage Productivity Center Predefined Reports).
- IBM Spectrum Control Report Layouts and (or the IBM Tivoli Storage Productivity Center Report Layouts).
- k) Click the **Green** arrow to transfer the content to the list.
- l) Click **OK**.
- m) On the Select the public folders content page, click Next.

Tip: If you want to export your schedules with your IBM[®] Cognos[®] Business Intelligence content from Tivoli Common Reporting, complete the following steps:

1) On the **Select the public folders** content page, select **Include schedules**.
2) Set Conflict resolution to Replace existing entries.

3) Click Next.

- n) On the **Select the directory content** page, select **Include data sources and connections** and **Include signons**.
- o) Set Conflict resolution to Replace existing entries and click Next.
- p) On the Specify the general options page, click Next.
- q) On the Specify a deployment archive page, click Set the encryption password.
- r) On the **Enter the encryption password** page, enter, and then confirm your password and click **OK**.

Tip: The encryption password is *not* an existing password in IBM Spectrum Control, Db2 or the operating system. The encryption password is a new password for the purpose of securing the content you are exporting from Jazz for Service Management and Tivoli Common Reporting.

Make note of your new password. You will need to provide it later in this procedure.

- s) On the **Specify a deployment archive** page, click **Next**.
- t) On the **Review the summary** page, click **Next**.
- u) On the Select an action page, select Save and run once and click Finish.
- v) On the Run with options page, click Run.
- w) On the **IBM Cognos software** page, select **View the details of this report after closing this dialog** and click **OK**.
- x) On the View run history details page, click Refresh.

Do not log off from the IBM Cognos Administration GUI until the export job is complete. You can click **Refresh** periodically to check the status of the export job.

- y) After the export job is complete, on the View an export deployment record page, click Close.
- z) Log off from the reporting interface.
- aa) Copy the exported file from the JazzSM_installation_dir/reporting/cognos/ deployment/ directory to a directory that is outside of the Jazz for Service Management installation directory.

Make note of the name and location of this exported file. You will need this information in Step 13.

Tip: If you *do not* copy the exported file outside of the Jazz for Service Management installation directory, the exported file is deleted when you uninstall Tivoli Common Reporting.

2. Upgrade Server A to the latest version of IBM Spectrum Control.

For more information, see <u>Upgrading from Tivoli Storage Productivity Center Version 5.2.0 and later</u> with a remote database by using the installation program.

- 3. Upgrade *Server B* to the latest version of IBM Spectrum Control. For more information, see <u>Upgrading from Tivoli Storage Productivity Center Version 5.2.0 and later</u> with a remote database by using the installation program.
- 4. Optional: Uninstall Tivoli Common Reporting, Jazz for Service Management, WebSphere Application Server, and Installation Manager from *Server B*.

For more information, see Uninstalling Tivoli Common Reporting and Jazz for Service Management.

If you *did not* uninstall Tivoli Common Reporting, Jazz for Service Management, WebSphere Application Server, and Installation Manager, you *must* stop Jazz for Service Management and Tivoli Common Reporting before you proceed with the rest of this procedure.

To stop Jazz for Service Management and Tivoli Common Reporting, open a command prompt and enter the following command:

```
JazzSM_installation_dir/profile/bin/stopServer.sh server_name -username JazzSM_username -password JazzSM_password
```

For example:

/opt/IBM/JazzSM/profile/bin/stopServer.sh server1 -username smadmin -password abc123

5. Install IBM Cognos Analytics 11.0.9 or later on Server B.

Tip: You do not need to set the **JAVA_HOME** environment variable before you start the IBM Cognos Analytics 11.0.9 or later installation program.

- a) Log in to your computer as a user with root privileges.
- b) Start the IBM Cognos Analytics installation program.
- c) Select the language to use for your installation and click Next.
- d) On the **Product installation** page, select **IBM Cognos Analytics (IBM Bundler Edition)** and click **Next**.
- e) On the **License agreement** page, accept the License Agreement and click **Next**.
- f) On the Location page, provide your installation location and click Next.

Make note of your Cognos Analytics installation location. You will need to provide it later in this procedure.

Tip: If you want the IBM Cognos Analytics installation to automatically create the installation location for you, click **Yes**.

- g) On the Installation type page, select First install and click Next.
- h) On the **Choose components** page, accept the default selections, and click **Next**.
- i) On the Pre-installation summary page, review your information for accuracy and click Install.
- j) When the installation is complete, click **Done**.
- 6. On Server B, copy the following Db2 JDBC driver files from the /opt/IBM/db2/version/java/ directory to the Cognos_installation_dir/drivers/ directory :
 - db2jcc.jar
 - db2jcc_license_cu.jar
 - db2jcc4.jar

7. On Server B, open a command prompt and enter the following command as the root user:

```
cd Cognos_installation_dir/drivers/
chmod +x db2jcc*.jar
```

8. On Server B, open a command prompt and enter the following command as the root user:

```
ln -s Db2_instance_owner_home_directory/sqllib/lib32/libdb2.a Cognos_installation_dir/bin/
```

IBM Spectrum Control Predefined Reports use Compatibility Query Mode. Cognos Analytics needs to use the 32-Bit Db2 library in order to connect to the IBM Spectrum Control database as a data source.

- 9. Create the content store for Cognos Analytics on Server B.
 - a) Open a command prompt and enter the following commands to start IBM Cognos Configuration:

```
cd Cognos_installation_dir/bin64/
. /home/db2inst1/sqllib/db2profile
./cogconfig.sh
```

Notice the space between the . and the / in the second command.

- b) In the **Explorer** window, expand **Data Access** > **Content Manager** and click **Content Store**.
- c) In the **Type** property, enter **DB2 database**, if it is not already displayed.
- d) In the **Database server and port number** property, enter localhost or the fully qualified domain name of the machine.

For example, localhost: 50000 or *FQDN_Of_Your_Machine*: 50000 where 50000 is the default port number that is used by Db2.

Tip: If you are using a different port number, ensure that you use that value. To determine the port that is used by Db2, examine the **varDBPort** parameter in the SC_installation_dir/ config/InstallVariable.properties file.

e) In the **User ID and password** property, enter the user name of the owner of the Db2 instance where the content store database will be located and the password that is associated with that user name

Typically, this user name is *db2inst1*.

- f) In the Database name property, verify that the default value is cm.
- g) From the File menu, click Save.
 - This step might take a few minutes to complete. Track the progress in the window.
- h) In the **informational** window, click **Close**.
- i) In the Explorer window, expand Data Access > Content Manager and click Content Store.
- j) Right-click Content Store and click Generate DDL.
- k) In the informational window, click Close.

Important: Do not exit IBM Cognos Configuration in this step. Wait until Step 12.

- l) While you are logged into the AIX operating system as the root user, switch to the user that is the Db2 instance owner (for example, *db2inst1*).
- m) Open a command prompt and enter the following Db2 command:

db2 -tvf Cognos_installation_dir/configuration/schemas/content/db2/createDb.sql

If the results of this command contain the following similar messages, you can safely ignore those messages because the Db2 instance owner already has the necessary privileges:

GRANT CREATETAB,BINDADD,CONNECT,IMPLICIT_SCHEMA ON DATABASE TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

GRANT CREATEIN, DROPIN, ALTERIN ON SCHEMA DB2COGNOS TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

GRANT USE OF TABLESPACE TSN_USR_cm TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

GRANT USE OF TABLESPACE TSN_REG_cm TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

- n) Go back to the root user.
- o) In IBM Cognos Configuration, from the Actions menu, click Test.
 - You are testing the connection between content manager and the content store database.
- p) In the **informational** window, click **Close**.
- 10. Optional: On *Server B*, you can change the IBM Cognos Analytics ports to match the ports that are used by Jazz for Service Management and Tivoli Common Reporting.

You would do this so that you do not have to get new firewall exceptions for the default Cognos Analytics ports.

- a) While you are still in IBM Cognos Configuration, in the **Explorer** window, click **Environment**.
- b) In the **Group Properties** window, select the **Value** next to the **URI** property and change the following properties (names):

Table 35. Group Property values		
Property	Change the value to	
Gateway URI	Computer fully qualified domain name (for	
External dispatcher URI	example, <i>myserver.mycompany.com</i>).	
Internal dispatcher URI	• The https protocol.	
Dispatcher URI for external applications	WC_defaulthost_secure parameter in the	
Content Manager URIs	JazzSM_installation_dir\profile \properties\portdef.props file. The default value is 16311.	

c) From the **File** menu, click **Save**.

d) In the **informational** window, click **Close**.

11. Start IBM Cognos Analytics (content manager and application services), on Server B.

It might take Cognos Analytics a few minutes to start.

- a) While you are still in IBM Cognos Configuration, in the **Explorer** window, click **Local Configuration**.
- b) From the **Actions** menu, click **Test**.

Tip: If you are not configuring Cognos Analytics to send notifications, you can ignore the testing the mail server connection failure message.

- c) In the informational window, click Close.
- d) From the **Actions** menu, click **Start**.

It might take Cognos Analytics a few minutes to start.

- 12. Exit IBM Cognos Configuration on Server B.
- 13. On *Server B*, copy the exported file that you created in Step 1 to the *Cognos_installation_dir/* deployment/ directory.
- 14. Import content into Cognos Analytics on Server B.
 - a) Open a web browser and enter either of the following URLs:

```
http://FQDN_0f_Your_Machine:port/bi
```

Or

```
https://FQDN_Of_Your_Machine:port/bi
```

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 10 (Optional). If you *did not* perform Step 10, the default port value is 9300.



Warning: At this point Cognos Analytics is configured with anonymous access so that anyone is able to access it.

- b) In the lower left-hand part of the page, select **Manage** > **Administration console**.
- c) In the IBM Cognos Administration GUI, select the **Configuration** tab.
- d) In the **Configuration** tab, select **Content Administration**.
- e) On the toolbar, click the **New Import** icon.

It is the fourth icon in the list.

f) On the **Select a deployment archive** page, select the name of the file that you exported from Jazz for Service Management in Step 1 and click **Next**.

- g) On the **Enter the encryption password** page, enter the encryption password that you created in Step 1 and click **OK**.
- h) On the **Specify a name and description** page, enter a name for your import (or keep the default setting) and click **Next**.
- i) On the **Select the public folders, directory, and library content** page, select the following items to import:
 - Custom content that you exported.
 - IBM Spectrum Control Packages and (or the IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or the IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or the IBM Tivoli Storage Productivity Center Report Layouts).
- j) Accept the default settings in the **Options** section and click **Next**.

Tip: If you want to import your schedules with your IBM[®] Cognos[®] Business Intelligence content from Tivoli Common Reporting, complete the following steps:

- 1) In the **Options** section, verify that **Include schedules** is selected.
- 2) In the **Options** section, verify that **Conflict resolution** is set to **Replace existing entries**.
- 3) Click Next.
- k) On the Select directory content page, verify that Include data sources and connections and Include signons are selected and that Conflict resolution is set to Replace existing entries and click Next.
- l) On the **Specify the general options** page, click **Next**.
- m) On the **Review the summary** page, click **Next**.
- n) On the Select an action page, select Save and run once and click Finish.
- o) On the **Run with Options** page, select **Upgrade all report specifications to the latest version** and **Assign new IDs during import**.
- p) Click Run.
- q) On the IBM Cognos software page, select View the details of this import after closing this dialog and click OK.
- r) On the View run history details page, click Refresh.

Check the **Status** field to monitor that the job is executing. Do *not* log off from the IBM Cognos Administration GUI until the import job is complete.

Tip: The import job might take approximately 15 minutes or more to resolve. Click **Refresh** periodically to check the status.

The results of importing the reports and schedules into Cognos Analytics contain the following similar messages:

```
CM-REQ-4328 A problem was encountered while importing the object
"/content/folder[@name="IBM Spectrum Control Predefined Reports"]/
folder[@name="Servers"]/report[@name="Servers Capacity"]/schedule".
CM-REQ-4329 The following references cannot be resolved and were cleared:
"credential: CAMID("VMMProvider:smadmin")/credential[@name='Credential '] ".
CM-REQ-4328 A problem was encountered while importing the object
"/content/folder[@name="IBM Spectrum Control Predefined Reports"]/
folder[@name="Servers"]/report[@name="Servers Capacity"]/
schedule[@name="2018-04-27T18:03:22.638Z"]".
CM-REQ-3282 The schedule will not run because the credential is missing.
```

You can safely ignore the messages as they are expected.

- s) After the import job is complete, check the **Completion time** and **Status** fields to verify that the job is complete. If it is complete, on the **View an import deployment record** page, click **Close**.
- t) To exit the IBM Cognos Administration GUI, close the browser tab.

- 15. Verify that the imported content is displayed in Cognos Analytics on Server B.
 - a) Return to the browser tab where the Cognos Analytics GUI is running. If it is not running, open a web browser and enter either of the following URLs:

http://FQDN_Of_Your_Machine:port/bi

Or

https://FQDN_0f_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 10 (Optional).

If you did perform Step 10, then you will use https. If you *did not* perform Step 10, then you use http.

If you *did not* perform Step 10, the default port value is 9300.

- b) On the IBM Cognos Analytics Welcome page, click Team content.
- c) Verify that the following content is listed:
 - Custom content that you saved to Public Folders before you ran this procedure.
 - IBM Spectrum Control Packages and (or IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or IBM Tivoli Storage Productivity Center Report Layouts).
- d) Optional: Attempt to generate a custom report or a predefined report and verify the contents.

Important: If you encounter APAR IT23800 or other problems when generating a predefined report in Cognos Analytics that was migrated from Tivoli Common Reporting, import the predefined reports package for the version of IBM Spectrum Control you are currently running on your system.

If you encounter APAR IT23800 or other problems when generating a custom report in Cognos Analytics that was migrated from Tivoli Common Reporting, you must update or recreate the custom report to use the predefined reports package for the version of IBM Spectrum Control you are currently running and remove references to tables that are no longer used in the IBM Spectrum Control database repository.

16. After you import the report content and schedules into Cognos Analytics, the schedules will not run due to missing credentials.

To update the schedules in Cognos Analytics with the correct credentials, complete the following steps:

a. Return to the browser tab where the Cognos Analytics GUI is running. If it is not running, open a web browser and enter either of the following URLs:

http://FQDN_Of_Your_Machine:port/bi

Or

https://FQDN_Of_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 10 (Optional).

If you did perform Step 10, then you will use https. If you *did not* perform Step 10, then you use http.

If you *did not* perform Step 10, the default port value is 9300.

- b. On the IBM Cognos Analytics Welcome page, click Team content.
- c. Select a report that has an existing schedule.
- d. Select the **Properties** for the report.
- e. Select the **Schedule** tab.
- f. Select the > icon to open the schedule.
- g. Click **Update** on the schedule page.

Repeat steps c-g for each migrated report schedule you want to run in Cognos Analytics.

You migrated your custom IBM[®] Cognos[®] Business Intelligence reports and upgraded to the latest version of IBM Spectrum Control and are able to use Cognos[®] BI reports.

Change the configuration of IBM Cognos Analytics from anonymous access to authenticated access.

For more information, see Configuring an LDAP namespace for IBM Directory Server.

For more information, see Configuring an LDAP namespace for Active Directory Server.

For more information, see Managing user authentication.

Related tasks

"Importing IBM Spectrum Control pre-defined reports package" on page 96 Complete this procedure to import the IBM Spectrum Control predefined reports package into the IBM Cognos Analytics reporting tool.

Related information

APAR IT23800 Upgrading DB2 servers Upgrading a DB2 server (Linux and UNIX) IBM Cognos Analytics server components Install and configure server components Installing server components on UNIX or Linux operating systems Installing Content Manager on UNIX or Linux operating systems Installing the Application services components on UNIX or Linux operating systems

Migrating Cognos BI reports to IBM Cognos Analytics in a multiple server AIX environment with remote Jazz for Service Management

If you do not have custom report content, you can skip this migration procedure. You can upgrade to IBM® Cognos® Analytics 11.0.9 or later when you upgrade to the latest version of IBM Spectrum Control. Complete this procedure to migrate your existing custom report content from Tivoli Common Reporting to Cognos Analytics.

Review the content of "Configuring IBM Cognos Analytics" on page 88 before you start this procedure.

For this procedure, the terms *Server A* and *Server B* denote the two servers. *Server A* has DB2[®] Enterprise Server Edition, IBM Spectrum Control database repository, and the IBM Spectrum Control servers installed. *Server B* has DB2[®] Enterprise Server Edition, Jazz for Service Management and Tivoli Common Reporting installed.

Important: Only reports in the Cognos Analytics Public Folders are migrated to IBM[®] Cognos[®] Analytics 11.0.9 or later. If you saved reports to My Folder, you must save them again in Public Folders before you migrate them.

If you plan to upgrade Db2 as part of your upgrade to the latest version of IBM Spectrum Control, upgrade Db2 on *Server A*, upgrade the IBM Spectrum Control database (TPCDB) on *Server A*, upgrade Db2 on *Server B* and then upgrade the Tivoli Common Reporting Content Store database (TCRDB) on *Server B*.

A high level overview on completing this upgrade:

• Export content from Tivoli Common Reporting on Server B.

- Upgrade IBM Spectrum Control on Server A.
- Uninstall IBM Spectrum Control on Server B.
- (Optional) Uninstall Tivoli Common Reporting, Jazz for Service Management, IBM[®] WebSphere[®] Application Server, and Installation Manager, from *Server B*.
- Install and configure Cognos Analytics on Server B.
- Import content into Cognos Analytics on Server B and then verify the content.

Verify that you have the following prerequisite packages installed on *Server B* for IBM Cognos Analytics Version or later.

The prerequisites for AIX 6.1 are:

- TL7
- SP05 (6100-07-05-1228)
- IBM XL C/C++ for AIX, 12.1 Runtime Environment
- bos.pmapi.lib

The prerequisites for AIX 7.1 are:

- IBM XL C/C++ for AIX, 12.1 Runtime Environment
- bos.pmapi.lib

For more information, see Software Product Compatibility Reports.

You need to set the correct ulimit values on *Server B* in the /etc/security/limits file for Cognos Analytics.

Here is an example of the entries you might need to add to the /etc/security/limits file:

default: fsize = -1 core = -1 rss = -1 stack = 16384 nofiles = 8192

After you set and save your ulimit values, restart your computer and verify the correct ulimit values.

For more information, see Set the ulimit values on UNIX and Linux operating systems .

- 1. Log in to Jazz for Service Management and Tivoli Common Reporting on Server B to export content.
 - a) Open a web browser and enter the following URL:

https://FQDN_Of_Your_Machine:port/tarf/servlet/dispatch

Where https is the protocol, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*) and the *port* value is the secure HTTP port number that was specified during the installation of Jazz for Service Management.

To determine the secure HTTP port number for Jazz for Service Management, open the *JazzSM_installation_dir*/profile/properties/portdef.props file. The default *JazzSM_installation_dir* value is /opt/IBM/JazzSM. The port number is the value that is assigned to the **WC_defaulthost_secure** parameter. The default value is 16311.

If you receive a security certificate warning when you attempt to connect to the server, confirm the security exception and continue to the web page.

- b) Log in to the reporting interface using the Jazz for Service Management user name that was created when you installed Jazz for Service Management. The default value is smadmin.
- c) Select Launch > IBM Cognos Administration.
- d) In the IBM Cognos Administration GUI, select the **Configuration** tab.
- e) In the **Configuration** tab, select **Content Administration**.

- f) On the toolbar, click the **New Export** icon.
 - It is the third icon in the list.
- g) On the **Specify a name and description** page, enter a name for your export package and click **Next**.
- h) On the **Choose a deployment method** page, select **Select public folders and directory content** and click **Next**.
- i) On the Select the public folders content page, click the Add link.
- j) On the **Select entries** page, select the following items to export.
 - Custom content that you saved to Public Folders before running this procedure.
 - IBM Spectrum Control Packages and (or the IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or the IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or the IBM Tivoli Storage Productivity Center Report Layouts).
- k) Click the **Green** arrow to transfer the content to the list.
- l) Click **OK**.
- m) On the Select the public folders content page, click Next.

Tip: If you want to export your schedules with your IBM[®] Cognos[®] Business Intelligence content from Tivoli Common Reporting, complete the following steps:

- 1) On the Select the public folders content page, select Include schedules.
- 2) Set Conflict resolution to Replace existing entries.
- 3) Click Next.
- n) On the **Select the directory content** page, select **Include data sources and connections** and **Include signons**.
- o) Set Conflict resolution to Replace existing entries and click Next.
- p) On the Specify the general options page, click Next.
- q) On the Specify a deployment archive page, click Set the encryption password.
- r) On the **Enter the encryption password** page, enter, and then confirm your password and click **OK**.

Tip: The encryption password is *not* an existing password in IBM Spectrum Control, Db2 or the operating system. The encryption password is a new password for the purpose of securing the content you are exporting from Jazz for Service Management and Tivoli Common Reporting.

Make note of your new password. You will need to provide it later in this procedure.

- s) On the Specify a deployment archive page, click Next.
- t) On the **Review the summary** page, click **Next**.
- u) On the Select an action page, select Save and run once and click Finish.
- v) On the **Run with options** page, click **Run**.
- w) On the **IBM Cognos software** page, select **View the details of this report after closing this dialog** and click **OK**.
- x) On the View run history details page, click Refresh.

Do not log off from the IBM Cognos Administration GUI until the export job is complete. You can click **Refresh** periodically to check the status of the export job.

- y) After the export job is complete, on the View an export deployment record page, click Close.
- z) Log off from the reporting interface.

aa) Copy the exported file from the JazzSM_installation_dir/reporting/cognos/ deployment/ directory to a directory that is outside of the Jazz for Service Management installation directory.

Make note of the name and location of this exported file. You will need this information in Step 13.

Tip: If you *do not* copy the exported file outside of the Jazz for Service Management installation directory, the exported file is deleted when you uninstall Tivoli Common Reporting.

2. Upgrade Server A to the latest version of IBM Spectrum Control.

For more information, see Upgrading from Tivoli Storage Productivity Center Version 5.2.0 and later with a remote database by using the installation program.

3. Upgrade *Server B* to the latest version of IBM Spectrum Control. You are then instructed to uninstall IBM Spectrum Control from *Server B*.

For more information, see <u>Uninstalling IBM Spectrum Control</u>.

4. Optional: Uninstall Tivoli Common Reporting, Jazz for Service Management, WebSphere Application Server, and Installation Manager from *Server B*.

For more information, see Uninstalling Tivoli Common Reporting and Jazz for Service Management.

If you *did not* uninstall Tivoli Common Reporting, Jazz for Service Management, WebSphere Application Server, and Installation Manager, you *must* stop Jazz for Service Management and Tivoli Common Reporting before you proceed with the rest of this procedure.

To stop Jazz for Service Management and Tivoli Common Reporting, open a command prompt and enter the following command:

JazzSM_installation_dir/profile/bin/stopServer.sh server_name -username JazzSM_username -password JazzSM_password

For example:

```
/opt/IBM/JazzSM/profile/bin/stopServer.sh server1 -username smadmin -password abc123
```

5. Install IBM Cognos Analytics 11.0.9 or later on Server B.

Tip: You do not need to set the **JAVA_HOME** environment variable before you start the IBM Cognos Analytics 11.0.9 or later installation program.

- a) Log in to your computer as a user with root privileges.
- b) Start the IBM Cognos Analytics installation program.
- c) Select the language to use for your installation and click **Next**.
- d) On the **Product installation** page, select **IBM Cognos Analytics (IBM Bundler Edition)** and click **Next**.
- e) On the **License agreement** page, accept the License Agreement and click **Next**.
- f) On the Location page, provide your installation location and click Next.

Make note of your Cognos Analytics installation location. You will need to provide it later in this procedure.

Tip: If you want the IBM Cognos Analytics installation to automatically create the installation location for you, click **Yes**.

- g) On the Installation type page, select First install and click Next.
- h) On the **Choose components** page, accept the default selections, and click **Next**.
- i) On the **Pre-installation summary** page, review your information for accuracy and click **Install**.
- j) When the installation is complete, click **Done**.
- 6. On *Server B*, copy the following Db2 JDBC driver files from the /opt/IBM/db2/version/java/ directory to the *Cognos_installation_dir*/drivers/ directory :
 - db2jcc.jar
 - db2jcc_license_cu.jar

db2jcc4.jar

7. On Server B, open a command prompt and enter the following command as the root user:

```
cd Cognos_installation_dir/drivers/
chmod +x db2jcc*.jar
```

8. On Server B, open a command prompt and enter the following command as the root user:

ln -s Db2_instance_owner_home_directory/sqllib/lib32/libdb2.a Cognos_installation_dir/bin/

IBM Spectrum Control Predefined Reports use Compatibility Query Mode. Cognos Analytics needs to use the 32-Bit Db2 library in order to connect to the IBM Spectrum Control database as a data source.

9. Create the content store for Cognos Analytics on Server B.

a) Open a command prompt and enter the following commands to start IBM Cognos Configuration:

```
cd Cognos_installation_dir/bin64/
. /home/db2inst1/sqllib/db2profile
./cogconfig.sh
```

Notice the space between the . and the / in the second command.

- b) In the Explorer window, expand Data Access > Content Manager and click Content Store.
- c) In the **Type** property, enter **DB2 database**, if it is not already displayed.
- d) In the **Database server and port number** property, enter localhost or the fully qualified domain name of the machine.

For example, localhost: 50000 or *FQDN_Of_Your_Machine*: 50000 where 50000 is the default port number that is used by Db2.

Tip: If you are using a different port number, ensure that you use that value. To determine the port that is used by Db2, examine the **varDBPort** parameter in the *SC_installation_dir/* config/InstallVariable.properties file.

e) In the **User ID and password** property, enter the user name of the owner of the Db2 instance where the content store database will be located and the password that is associated with that user name

Typically, this user name is *db2inst1*.

- f) In the **Database name** property, verify that the default value is **cm**.
- g) From the **File** menu, click **Save**.

This step might take a few minutes to complete. Track the progress in the window.

- h) In the **informational** window, click **Close**.
- i) In the **Explorer** window, expand **Data Access** > **Content Manager** and click **Content Store**.
- j) Right-click Content Store and click Generate DDL.
- k) In the informational window, click Close.

Important: Do not exit IBM Cognos Configuration in this step. Wait until Step 12.

- l) While you are logged into the AIX operating system as the root user, switch to the user that is the Db2 instance owner (for example, *db2inst1*).
- m) Open a command prompt and enter the following Db2 command:

 $db2 \ \text{-tvf} \ \textit{Cognos_installation_dir/configuration/schemas/content/db2/createDb.sql}$

If the results of this command contain the following similar messages, you can safely ignore those messages because the Db2 instance owner already has the necessary privileges:

GRANT CREATETAB,BINDADD,CONNECT,IMPLICIT_SCHEMA ON DATABASE TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

GRANT CREATEIN,DROPIN,ALTERIN ON SCHEMA DB2COGNOS TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502

GRANT USE OF TABLESPACE TSN_USR_cm TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself. SQLSTATE=42502 GRANT USE OF TABLESPACE TSN_REG_cm TO USER db2inst1 DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0554N An authorization ID cannot grant a privilege or authority to itself.

n) Go back to the root user.

SQLSTATE=42502

o) In IBM Cognos Configuration, from the Actions menu, click Test.

You are testing the connection between content manager and the content store database.

p) In the informational window, click Close.

10. Optional: On *Server B*, you can change the IBM Cognos Analytics ports to match the ports that are used by Jazz for Service Management and Tivoli Common Reporting.

You would do this so that you do not have to get new firewall exceptions for the default Cognos Analytics ports.

- a) While you are still in IBM Cognos Configuration, in the **Explorer** window, click **Environment**.
- b) In the Group Properties window, select the Value next to the URI property and change the following properties (names):

Table 36. Group Property values		
Property	Change the value to	
Gateway URI	Computer fully qualified domain name (for	
External dispatcher URI	example, <i>myserver.mycompany.com</i>).	
Internal dispatcher URI	The https protocol. The 0200 part to the value of the	
Dispatcher URI for external applications	WC_defaulthost_secure parameter in the	
Content Manager URIs	JazzSM_installation_dir\profile \properties\portdef.props file. The default value is 16311.	

- c) From the File menu, click Save.
- d) In the **informational** window, click **Close**.
- 11. Start IBM Cognos Analytics (content manager and application services), on Server B.

It might take Cognos Analytics a few minutes to start.

- a) While you are still in IBM Cognos Configuration, in the **Explorer** window, click **Local Configuration**.
- b) From the **Actions** menu, click **Test**.

Tip: If you are not configuring Cognos Analytics to send notifications, you can ignore the testing the mail server connection failure message.

- c) In the **informational** window, click **Close**.
- d) From the Actions menu, click Start.

It might take Cognos Analytics a few minutes to start.

12. Exit IBM Cognos Configuration on Server B.

- 13. On *Server B*, copy the exported file that you created in Step 1 to the *Cognos_installation_dir/* deployment/ directory.
- 14. Import content into Cognos Analytics on Server B.
 - a) Open a web browser and enter either of the following URLs:

http://FQDN_0f_Your_Machine:port/bi

Or

https://FQDN_Of_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 10 (Optional). If you *did not* perform Step 10, the default port value is 9300.



Warning: At this point Cognos Analytics is configured with anonymous access so that anyone is able to access it.

- b) In the lower left-hand part of the page, select **Manage** > **Administration console**.
- c) In the IBM Cognos Administration GUI, select the **Configuration** tab.
- d) In the **Configuration** tab, select **Content Administration**.
- e) On the toolbar, click the **New Import** icon.

It is the fourth icon in the list.

- f) On the **Select a deployment archive** page, select the name of the file that you exported from Jazz for Service Management in Step 1 and click **Next**.
- g) On the **Enter the encryption password** page, enter the encryption password that you created in Step 1 and click **OK**.
- h) On the **Specify a name and description** page, enter a name for your import (or keep the default setting) and click **Next**.
- i) On the **Select the public folders, directory, and library content** page, select the following items to import:
 - Custom content that you exported.
 - IBM Spectrum Control Packages and (or the IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or the IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or the IBM Tivoli Storage Productivity Center Report Layouts).
- j) Accept the default settings in the **Options** section and click **Next**.

Tip: If you want to import your schedules with your IBM[®] Cognos[®] Business Intelligence content from Tivoli Common Reporting, complete the following steps:

- 1) In the **Options** section, verify that **Include schedules** is selected.
- 2) In the **Options** section, verify that **Conflict resolution** is set to **Replace existing entries**.
- 3) Click Next.
- k) On the Select directory content page, verify that Include data sources and connections and Include signons are selected and that Conflict resolution is set to Replace existing entries and click Next.
- l) On the Specify the general options page, click Next.
- m) On the **Review the summary** page, click **Next**.
- n) On the Select an action page, select Save and run once and click Finish.

- o) On the **Run with Options** page, select **Upgrade all report specifications to the latest version** and **Assign new IDs during import**.
- p) Click Run.
- q) On the IBM Cognos software page, select View the details of this import after closing this dialog and click OK.
- r) On the View run history details page, click Refresh.

Check the **Status** field to monitor that the job is executing. Do *not* log off from the IBM Cognos Administration GUI until the import job is complete.

Tip: The import job might take approximately 15 minutes or more to resolve. Click **Refresh** periodically to check the status.

The results of importing the reports and schedules into Cognos Analytics contain the following similar messages:

```
CM-REQ-4328 A problem was encountered while importing the object
"/content/folder[@name="IBM Spectrum Control Predefined Reports"]/
folder[@name="Servers"]/report[@name="Servers Capacity"]/schedule".
CM-REQ-4329 The following references cannot be resolved and were cleared:
"credential: CAMID("VMMProvider:smadmin")/credential[@name='Credential '] ".
CM-REQ-4328 A problem was encountered while importing the object
"/content/folder[@name="IBM Spectrum Control Predefined Reports"]/
folder[@name="Servers"]/report[@name="Servers Capacity"]/
schedule[@name="2018-04-27T18:03:22.638Z"]".
CM-REQ-3282 The schedule will not run because the credential is missing.
```

You can safely ignore the messages as they are expected.

- s) After the import job is complete, check the **Completion time** and **Status** fields to verify that the job is complete. If it is complete, on the **View an import deployment record** page, click **Close**.
- t) To exit the IBM Cognos Administration GUI, close the browser tab.
- 15. Verify that the imported content is displayed in Cognos Analytics on Server B.
 - a) Return to the browser tab where the Cognos Analytics GUI is running. If it is not running, open a web browser and enter either of the following URLs:

http://FQDN_0f_Your_Machine:port/bi

Or

https://FQDN_Of_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 10 (Optional).

If you did perform Step 10, then you will use https. If you *did not* perform Step 10, then you use http.

If you *did not* perform Step 10, the default port value is 9300.

- b) On the IBM Cognos Analytics Welcome page, click Team content.
- c) Verify that the following content is listed:
 - Custom content that you saved to Public Folders before you ran this procedure.
 - IBM Spectrum Control Packages and (or IBM Tivoli Storage Productivity Center Packages).
 - IBM Spectrum Control Predefined Reports and (or IBM Tivoli Storage Productivity Center Predefined Reports).
 - IBM Spectrum Control Report Layouts and (or IBM Tivoli Storage Productivity Center Report Layouts).
- d) Optional: Attempt to generate a custom report or a predefined report and verify the contents.

Important: If you encounter APAR IT23800 or other problems when generating a predefined report in Cognos Analytics that was migrated from Tivoli Common Reporting, import the predefined reports package for the version of IBM Spectrum Control you are currently running on your system.

If you encounter APAR IT23800 or other problems when generating a custom report in Cognos Analytics that was migrated from Tivoli Common Reporting, you must update or recreate the custom report to use the predefined reports package for the version of IBM Spectrum Control you are currently running and remove references to tables that are no longer used in the IBM Spectrum Control database repository.

16. After you import the report content and schedules into Cognos Analytics, the schedules will not run due to missing credentials.

To update the schedules in Cognos Analytics with the correct credentials, complete the following steps:

a. Return to the browser tab where the Cognos Analytics GUI is running. If it is not running, open a web browser and enter either of the following URLs:

http://FQDN_0f_Your_Machine:port/bi

Or

https://FQDN_Of_Your_Machine:port/bi

Where http or https are protocols, *FQDN_Of_Your_Machine* is your fully qualified domain name, (for example, *myserver.mycompany.com*), and the *port* value is the value that you set when you updated Cognos Analytics, in Step 10 (Optional).

If you did perform Step 10, then you will use https. If you *did not* perform Step 10, then you use http.

If you *did not* perform Step 10, the default port value is 9300.

- b. On the IBM Cognos Analytics Welcome page, click Team content.
- c. Select a report that has an existing schedule.
- d. Select the **Properties** for the report.
- e. Select the **Schedule** tab.
- f. Select the > icon to open the schedule.
- g. Click **Update** on the schedule page.

Repeat steps c-g for each migrated report schedule you want to run in Cognos Analytics.

You migrated your custom IBM[®] Cognos[®] Business Intelligence report s and upgraded to the latest version of IBM Spectrum Control and are able to use Cognos[®] BI report s.

Change the configuration of IBM Cognos Analytics from anonymous access to authenticated access.

For more information, see Configuring an LDAP namespace for IBM Directory Server.

For more information, see Configuring an LDAP namespace for Active Directory Server.

For more information, see <u>Managing user authentication</u>.

Related tasks

"Importing IBM Spectrum Control pre-defined reports package " on page 96 Complete this procedure to import the IBM Spectrum Control predefined reports package into the IBM Cognos Analytics reporting tool.

Related information

APAR IT23800 Upgrading DB2 servers Upgrading a DB2 server (Linux and UNIX) IBM Cognos Analytics server components Install and configure server components Installing server components on UNIX or Linux operating systems Installing Content Manager on UNIX or Linux operating systems Installing the Application services components on UNIX or Linux operating systems

Upgrading IBM Spectrum Control in a single-server environment

You can upgrade IBM Spectrum Control by using the installation program or silent mode.

In a single-server environment, to upgrade IBM Spectrum Control, see the following topics:

- <u>"Upgrading IBM Spectrum Control in a single-server Windows environment by using the installation</u> program" on page 184
- "Upgrading IBM Spectrum Control in a single-server environment by using silent mode " on page 187

Upgrading IBM Spectrum Control in a single-server Windows environment by using the installation program

You can upgrade IBM Spectrum Control by using the installation program.

Before you upgrade, you must back up the entire IBM Spectrum Control system.

To upgrade IBM Spectrum Control in a single-server Windows environment, complete the following steps:

- 1. Log on to the IBM Spectrum Control computer with the appropriate user privileges.
- 2. If you are upgrading from Tivoli Storage Productivity Center 5.2.0 or later, start the Web server.

For more information about starting the services, see 🖙 Starting the IBM Spectrum Control services.

- 3. Start the IBM Spectrum Control installation program.
 - a) Download the image into a directory.
 - b) Extract the image files.
 - c) Enter the following command: cd *image_directory*\SC and then enter setup.bat.
- 4. Follow the prompts in the installation program to upgrade IBM Spectrum Control.
- 5. After the upgrade is finished, review the message log to ensure that no errors occurred.

Related concepts

"Backups" on page 105

Before you upgrade, you must back up the entire IBM Spectrum Control system.

Related reference

"Preparing for an upgrade" on page 101

You can use the following information to help prepare for your upgrade of IBM Spectrum Control. Good planning helps you avoid delays and problems when you upgrade your system.

"Reviewing the log files to resolve installation issues" on page 77

If an error occurs during IBM Spectrum Control installation, you can review the error log files to resolve issues and continue the installation.

"Planning for installation" on page 1

You can install IBM Spectrum Control by using the installation program or the command line in silent mode. Installing IBM Spectrum Control by using console mode is not supported. Also, upgrading the operating system of a server where IBM Spectrum Control is installed is not supported. If you must upgrade the server, contact the IBM Support team for IBM Spectrum Control Support to discuss your options.

"Starting the installation programs" on page 51

There are various methods to start the IBM Spectrum Control installation programs and on various operating systems.

Upgrading IBM Spectrum Control in a single-server AIX or Linux environment by using the installation program

You can upgrade IBM Spectrum Control as a root user or non-root user on an AIX or Linux operating system by using the IBM Spectrum Control installation program. To upgrade IBM Spectrum Control as a non-root user, you must have sudo privileges on the target AIX or Linux server.

Before you upgrade, you must back up the entire IBM Spectrum Control system.

Ensure that X Window System is installed on the target AIX or Linux server. The X Window System is required to upgrade IBM Spectrum Control by using the installation program.

If you want to upgrade IBM Spectrum Control as a non-root user, have your system administrator complete the following tasks on the target server before you begin the upgrade:

• If you are upgrading IBM Spectrum Control on an AIX server, install sudo on the server. The default AIX

distribution does not include sudo privileges. To get the sudo installation package, go to <u>http://</u>www.ibm.com/systems/power/software/aix/linux/toolbox/date.html</u>. Find **sudo-version** in the **Package** column, and click **RPM** to download the package.

- Ensure that the non-root user has sudo privileges for the following commands on the server:
 - xauth (Enables the non-root user to provide access to their X Window System display for the root user.)
 - **setup.bin** (Enables the non-root user to launch the IBM Spectrum Control installation program.)

You must enter the full path to the commands when you configure the sudo privileges. For example:

username ALL=(root) SETENV: /usr/bin/xauth, /home/username/Downloads/IBMSC/SC/setup.bin

- If the sudo environment on the server uses the secure_path option, ensure that the following directories are included in the secure_path value for the non-root user who is upgrading IBM Spectrum Control:
 - DB2_instance_owner_home_directory/sqllib/bin (Example: /home/db2inst1/sqllib/ bin)
 - DB2_instance_owner_home_directory/sqllib/adm(Example:/home/db2inst1/sqllib/ adm)
 - DB2_instance_owner_home_directory/sqllib/misc (Example: /home/db2inst1/sqllib/ misc)
- Ensure that the following requirements are met to enable the upgrade of IBM Spectrum Control by using the installation program:
 - The non-root user is able to use the X Window System on the target server and the X Window System DISPLAY environment variable is set correctly for the not-root user.
 - The DISPLAY environment variable is preserved in the sudo environment.
 - The root user has access to the X Window System display that is owned by the non-root user.

These display requirements do not apply if you upgrade IBM Spectrum Control in silent mode.

- If you are upgrading IBM Spectrum Control on an AIX server, ensure that the ODMDIR environment variable is preserved in the sudo environment.
- 1. Log on to the IBM Spectrum Control computer as the root user or as the non-root user who has sudo privileges.
- 2. If you are upgrading from Tivoli Storage Productivity Center 5.2.0 or later, start the Web server.
- For more information about starting the services, see 🖻 Starting the IBM Spectrum Control services.
- 3. Start the IBM Spectrum Control installation program.

a) Create a directory. Enter:

mkdir /SpectrumControl

- b) Download the image into the SpectrumControl directory.
- c) Enter the following command to extract the image files:

tar -xzvf filename.tar.gz

d) Ensure that the user name that you plan to use as the IBM Spectrum Control common user is in the system group and the db2iadm1 group.

If the user name is not in a group, you can add the user as shown in the following command example. In this example, the user name is db2inst1:

usermod -G system db2inst1

Tip: If the user is already a member of secondary groups, the **usermod** command removes the db2inst1 user name from all the secondary groups except for the system group. To preserve the existing secondary group memberships, provide a comma separated list of secondary groups after the -G flag. For more information, enter man usermod at the command prompt.

e) Go to the /SpectrumControl/SC directory:

cd /SpectrumControl/SC

f) Set up your shell environment to point to the instance where the database repository is installed. Source the db2profile for the instance that you want. For example, if the Db2 instance is db2inst1, you can source the db2profile by entering:

. /home/db2inst1/sqllib/db2profile

Remember: There is a space between . and /home.

- g) Start the installation program by running the **./setup.bin** or **sudo -E ./setup.bin** command from the same command shell that you used in the previous step.
- 4. Follow the prompts in the installation program to upgrade IBM Spectrum Control.
- 5. After the upgrade is finished, review the message log to ensure that no errors occurred.

Related concepts

"Backups" on page 105

Before you upgrade, you must back up the entire IBM Spectrum Control system.

Related reference

"Preparing for an upgrade" on page 101

You can use the following information to help prepare for your upgrade of IBM Spectrum Control. Good planning helps you avoid delays and problems when you upgrade your system.

"Reviewing the log files to resolve installation issues" on page 77

If an error occurs during IBM Spectrum Control installation, you can review the error log files to resolve issues and continue the installation.

"Planning for installation" on page 1

You can install IBM Spectrum Control by using the installation program or the command line in silent mode. Installing IBM Spectrum Control by using console mode is not supported. Also, upgrading the operating system of a server where IBM Spectrum Control is installed is not supported. If you must upgrade the server, contact the IBM Support team for IBM Spectrum Control Support to discuss your options.

"Starting the installation programs" on page 51

There are various methods to start the IBM Spectrum Control installation programs and on various operating systems.

Upgrading IBM Spectrum Control in a single-server environment by using silent mode

You can upgrade IBM Spectrum Control by using silent mode. This upgrade method is useful if your computer cannot display graphics.

Before you upgrade, you must back up the entire IBM Spectrum Control system.

To upgrade IBM Spectrum Control in a single-server environment by using silent mode, complete the following steps:

- 1. Log on to the IBM Spectrum Control computer with the appropriate user privileges.
- 2. If you are upgrading from Tivoli Storage Productivity Center 5.2.0 or later, start the Web server. For more information about starting the services, see 🖙 Starting the IBM Spectrum Control services.
- 3. Edit and save the appropriate response file.
 - Edit the silent_Upgrade.properties file and set the following parameters:
 - LICENSE_ACCEPTED=true
 - CHOSEN_INSTALL_TYPE="Upgrade"
 - CONFIRM_REPLICATION_UNINSTALL=true
 - CONFIRM_REPORTS_UNINSTALL=true
- 4. Run the silent mode installation program.
 - On Windows operating systems, run the following command:

```
setup.bat -l language -i silent -f absolute_path_to_response_file
```

where *language* can be one of the following values:

- Czech cs
- English en
- French fr
- German de
- Hungarian hu
- Italian it
- Japanese ja
- Korean ko
- Polish pl
- Brazilian Portuguese pt_BR
- Russian ru
- Spanish es
- Chinese (Simplified) zh_CN
- Chinese (Traditional) zh_TW

absolute_path_to_response_file is the absolute path to the response file. For example, the following command specifies the language and the path:

```
setup.bat -1 fr -i silent -f
c:\SpectrumControl\silent_Upgrade.properties
```

• On the AIX or Linux operating system, you must source the Db2 profile, db2profile, for the instance owner of the Db2 database. The following text is an example of the command you run to source the user profile:

. /home/db2inst1/sqllib/db2profile

• On AIX or Linux operating systems, run the following command:

./setup.bin -1 language -i silent -f /absolute_path_to_response_file

Where absolute_path_to_response_file is the absolute path to the response file. For example, the following command specifies the language and the path:

./setup.bin -l de -i silent -f /SpectrumControl/silent_Upgrade.properties

If you do not specify a language or if the language is not specified correctly, the installation program uses the English language as the default.

- 5. Monitor the progress of the upgrade.
 - To view the progress of the silent mode installation on Windows operating systems, check the trace log in the following path:

```
installation_dir\logs\traceTPCInstall.log
```

• To view the progress of the silent mode installation on AIX or Linux operating systems, check the trace log in the following path:

```
installation_dir/logs/traceTPCInstall.log
```

Related concepts

"Backups" on page 105

Before you upgrade, you must back up the entire IBM Spectrum Control system.

Related reference

"Planning for IBM Spectrum Control authentication and authorization" on page 17 An operating system user name is required to install and log on to IBM Spectrum Control for the first time. After you install IBM Spectrum Control, you can assign roles to users. Roles determine the product functions that are available to users.

"Editing the upgrade response file" on page 188 When you upgrade using the silent mode, use the silent_Upgrade.properties file.

<u>"Reviewing the log files to resolve installation issues" on page 77</u> If an error occurs during IBM Spectrum Control installation, you can review the error log files to resolve issues and continue the installation.

Editing the upgrade response file

When you upgrade using the silent mode, use the silent_Upgrade.properties file.

Parameters in the silent_Upgrade.properties file

The silent_Upgrade.properties file contains the following parameters:

LICENSE_ACCEPTED=false

Specifies whether you accept the IBM Spectrum Control license agreement. The options are:

true

You accept all the terms and conditions of the IBM Spectrum Control license agreement.

false or any other value

You do not accept the IBM Spectrum Control license agreement. The installation program exits.

CHOSEN_INSTALL_TYPE="Upgrade"

Specifies the upgrade type.

Important: Do not change the value for this parameter.

CONFIRM_REPLICATION_UNINSTALL=false

Acknowledges the uninstall of the Replication server during the upgrade.

The options are:

false

You do not acknowledge the uninstall of the Replication server and the upgrade does not proceed.

true

You do acknowledge the uninstall of the Replication server and the upgrade does proceed.

varAlertKeystorePW=default varDeviceKeystorePW=default varWebKeystorePW=default

Specify the password for the Alert server, Device server, and Web server keystore files.

The default keystore password is *default*. If any of the specified keystore passwords are incorrect, the upgrade exits.

Related tasks

"Upgrading IBM Spectrum Control in a single-server environment by using silent mode " on page 187 You can upgrade IBM Spectrum Control by using silent mode. This upgrade method is useful if your computer cannot display graphics.

Upgrading IBM Spectrum Control in a multiple-server environment

To upgrade IBM Spectrum Control in a multiple-server environment, start the installation program on the server on which the database repository is installed. After you complete the installation program on this server, you can start the start the installation program on the other server.

In a multiple-server environment, to upgrade IBM Spectrum Control, see the following topic:

• <u>"Upgrading from Tivoli Storage Productivity Center Version 5.2.0 and later with a remote database by</u> using the installation program" on page 189

Upgrading from Tivoli Storage Productivity Center Version 5.2.0 and later with a remote database by using the installation program

You can upgrade from Tivoli Storage Productivity Center Version 5.2.0 and later to IBM Spectrum Control with a remote database by using the installation program.

Before you upgrade, you must back up the entire Tivoli Storage Productivity Center system.

For this procedure, the terms *Server A* and *Server B* denote the two servers. Server A has DB2 Enterprise Server Edition and the Tivoli Storage Productivity Center database repository installed. Server B has all of the other TPC components installed.

To upgrade using the installation program, complete the following steps:

- 1. Complete the following steps on Server B:
 - a) Log on to Server B with the appropriate user privileges.
 - b) On Server B, stop all Tivoli Storage Productivity Center services.

For more information on stopping the services, see <u>Stopping the Tivoli Storage Productivity</u> Center servers.

- 2. Complete the following steps on Server A:
 - a) Log on to Server A with the appropriate user privileges.
 - b) If necessary, upgrade DB2 on Server A to a version that is supported by IBM Spectrum Control.

For more information about the supported DB2 versions, see <a>http://www.ibm.com/support/

docview.wss?uid=ibm10719187#DB.. For more information about upgrading DB2, see Upgrading DB2 servers.

Before you start the IBM Spectrum Control installation program on AIX or Linux operating systems, you must source the user profile, db2profile, for the instance owner of the DB2 database. The following text is an example of the command to source the user profile:

. /home/db2inst1/sqllib/db2profile

- c) Start the IBM Spectrum Control installation program on Server A.
- d) Follow the prompts in the installation program to upgrade the database repository on Server A.
- e) After the upgrade is finished on Server A, review the message log to ensure that no errors occurred.
- 3. Complete the following steps on Server B:
 - a) Log on to Server B with the appropriate user privileges.
 - b) On Server B, start the Web Server. For more information about starting the services, see <u>Starting</u> the IBM Spectrum Control services.
 - c) Start the IBM Spectrum Control installation program on Server B.
 - d) Follow the prompts in the installation program to upgrade the IBM Spectrum Control components on Server B.
 - e) After the upgrade is finished, review the message log file on Server B to ensure that no errors occurred.

Related concepts

"Backups" on page 105

Before you upgrade, you must back up the entire IBM Spectrum Control system.

Related reference

"Preparing for an upgrade" on page 101

You can use the following information to help prepare for your upgrade of IBM Spectrum Control. Good planning helps you avoid delays and problems when you upgrade your system.

"Planning for IBM Spectrum Control authentication and authorization" on page 17

An operating system user name is required to install and log on to IBM Spectrum Control for the first time. After you install IBM Spectrum Control, you can assign roles to users. Roles determine the product functions that are available to users.

"Reviewing the log files to resolve installation issues" on page 77

If an error occurs during IBM Spectrum Control installation, you can review the error log files to resolve issues and continue the installation.

Upgrading from Tivoli Storage Productivity Center Version 5.2.0 and later with remote Jazz for Service Management by using the installation program

You can upgrade Tivoli Storage Productivity Center Version 5.2.0 and later with remote Jazz for Service Management to IBM Spectrum Control, on a single machine by using the installation program.

Before you upgrade, you must back up the entire Tivoli Storage Productivity Center system.

For this procedure, the terms *Server A* and *Server B* denote the two servers. Server A has DB2 Enterprise Server Edition, the Tivoli Storage Productivity Center database repository and the Tivoli Storage Productivity Center servers installed. Server B has DB2 Enterprise Server Edition, Jazz for Service Management, and Cognos Analytics reports installed.

The IBM Cognos BI reports component is no longer part of the IBM Spectrum Control product. The upgrade on Server B will instruct you to uninstall IBM Spectrum Control from Server B. Therefore, after you complete this upgrade procedure, all of the IBM Spectrum Control components will be on Server A and no part of IBM Spectrum Control will be on Server B.

To upgrade IBM Spectrum Control by using the installation program, complete the following steps:

- 1. On Server A, complete the following steps:
 - a) Log on to Server A with the appropriate user privileges.
 - b) Before you start the IBM Spectrum Control installation program on the AIX or Linux operating systems, you must source the user profile (db2profile) for the instance owner of the DB2 database.

The following text is an example of the command to source the user profile:

. /home/db2inst1/sqllib/db2profile

- c) Start the IBM Spectrum Control installation program.
- d) Follow the prompts in the installation program to upgrade the IBM Spectrum Control database repository and the IBM Spectrum Control servers.
- e) After the upgrade is finished, review the message log on Server A to ensure that no errors occurred.
- 2. On Server B, complete the following steps:
 - a) Log on to Server B with the appropriate user privileges.
 - b) Before you start the IBM Spectrum Control installation program on the AIX or Linux operating systems, you must source the user profile (db2profile) for the instance owner of the DB2 database.

The following text is an example of the command to source the user profile:

. /home/db2inst1/sqllib/db2profile

c) Start the IBM Spectrum Control installation program on Server B.

- d) The upgrade will instruct you to uninstall IBM Spectrum Control from Server B. Quit the IBM Spectrum Control installation program.
- e) Uninstall IBM Spectrum Control from Server B.

After you complete this upgrade procedure, all of the IBM Spectrum Control components will be on Server A and no part of IBM Spectrum Control will be on Server B.

Related concepts

<u>"Backups" on page 105</u> Before you upgrade, you must back up the entire IBM Spectrum Control system.

Related tasks

"Db2" on page 43

You can install the most recent version of Db2 that IBM Spectrum Control supports on the Linux, AIX, or Windows operating systems.

Related reference

"Preparing for an upgrade" on page 101

You can use the following information to help prepare for your upgrade of IBM Spectrum Control. Good planning helps you avoid delays and problems when you upgrade your system.

<u>"Planning for IBM Spectrum Control authentication and authorization" on page 17</u> An operating system user name is required to install and log on to IBM Spectrum Control for the first time. After you install IBM Spectrum Control, you can assign roles to users. Roles determine the product functions that are available to users.

"Reviewing the log files to resolve installation issues" on page 77

If an error occurs during IBM Spectrum Control installation, you can review the error log files to resolve issues and continue the installation.

Upgrading IBM Spectrum Control with a remote database by using silent mode

You can upgrade IBM Spectrum Control in a multiple-server environment with a remote database by using silent mode.

Before you upgrade, you must back up the entire IBM Spectrum Control system.

For this procedure, the terms *Server A* and *Server B* denote the two servers. Server A has Db2 and the IBM Spectrum Control database repository installed. Server B has all of the other IBM Spectrum Control components installed.

To upgrade IBM Spectrum Control by using silent mode, complete the following steps:

- 1. Complete the following steps on Server B:
 - a) Log on to Server B with the appropriate user privileges.
 - b) On Server B, stop all of the IBM Spectrum Control services.
 - See 🖙 Stopping the IBM Spectrum Control servers by using the GUI.
- 2. Complete the following steps on Server A:
 - a) Log on to Server A with the appropriate user privileges.
 - b) If necessary, upgrade Db2 on Server A to a version that is supported by IBM Spectrum Control.

For more information about the supported Db2 versions, see <u>http://www.ibm.com/support/</u> <u>docview.wss?uid=ibm10719187#DB</u>. For more information about upgrading Db2, see <u>Upgrading DB2 servers</u>.

- c) Edit and save the appropriate response file.
 - Edit the silent_Upgrade.properties file and set the following parameters:
 - LICENSE_ACCEPTED=true
 - CHOSEN_INSTALL_TYPE="Upgrade"
- d) On AIX or Linux operating systems, source the user profile (db2profile) for the instance owner of the Db2 database.

For example:

```
. /home/db2inst1/sqllib/db2profile
```

- e) Run the silent mode installation program on Server A.
 - For Windows operating systems, run the following command:

setup.bat -l language -i silent -f absolute_path_to_response_file

where *language* can be one of the following values:

- Czech cs
- English en
- French fr
- German de
- Hungarian hu
- Italian it
- Japanese ja
- Korean ko
- Polish pl
- Brazilian Portuguese pt_BR

- Russian ru
- Spanish es
- Chinese (Simplified) zh_CN
- Chinese (Traditional) zh_TW

absolute_path_to_response_file is the absolute path to the response file. For example, the following command specifies the language and the path:

setup.bat -1 fr -i silent -f
c:\SpectrumControl\silent_Upgrade.properties

• For AIX or Linux operating systems, run the following command:

./setup.bin -1 language -i silent -f /absolute_path_to_response_file

For example, the following command specifies the language and the path:

./setup.bin -1 de -i silent -f /SpectrumControl/silent_Upgrade.properties

If you do not specify a language or if the language is not specified correctly, the installation program uses the English language as the default.

- f) Monitor the progress of the upgrade on Server A.
 - To view the progress of the silent mode installation on Windows operating systems, check the trace log in the following path:

```
installation_dir\logs\traceTPCInstall.log
```

• To view the progress of the silent mode installation on AIX or Linux operating systems, check the trace log in the following path:

```
installation_dir/logs/traceTPCInstall.log
```

- 3. Complete the following steps on Server B:
 - a) Log on to Server B with the appropriate user privileges.
 - b) If you are upgrading from Tivoli Storage Productivity Center 5.2.0 or later, start the Web server. For more information about starting the services, see 🖙 Starting the IBM Spectrum Control services.
 - c) Edit and save the appropriate response file on Server B.
 - Edit the silent_Upgrade.properties file and set the following parameters:
 - LICENSE_ACCEPTED=true
 - CHOSEN_INSTALL_TYPE="Upgrade"
 - CONFIRM_REPORTS_UNINSTALL=true
 - CONFIRM_REPLICATION_UNINSTALL=true
 - d) Run the silent mode installation program on Server B.
 - For Windows operating systems, run the following command:

```
setup.bat -1 language -i silent -f absolute_path_to_response_file
```

where *language* can be one of the following values:

- Czech cs
- English en
- French fr
- German de
- Hungarian hu

- Italian it
- Japanese ja
- Korean ko
- Polish pl
- Brazilian Portuguese pt_BR
- Russian ru
- Spanish es
- Chinese (Simplified) zh_CN
- Chinese (Traditional) zh_TW

absolute_path_to_response_file is the absolute path to the response file. For example, the following command specifies the language and the path:

```
setup.bat -1 fr -i silent -f
c:\SpectrumControl\silent_Upgrade.properties.properties
```

• For AIX or Linux operating systems, run the following command:

./setup.bin -1 language -i silent -f /absolute_path_to_response_file

For example, the following command specifies the language and the path:

./setup.bin -1 de -i silent -f /SpectrumControl/silent_Upgrade.properties

If you do not specify a language or if the language is not specified correctly, the installation program uses the English language as the default.

- e) Monitor the progress of the upgrade on Server B.
 - To view the progress of the silent mode installation on Windows operating systems, check the trace log in the following path:

```
installation_dir\logs\traceTPCInstall.log
```

• To view the progress of the silent mode installation on AIX or Linux operating systems, check the trace log in the following path:

```
installation_dir/logs/traceTPCInstall.log
```

Related concepts

"Backups" on page 105

Before you upgrade, you must back up the entire IBM Spectrum Control system.

Related reference

"Preparing for an upgrade" on page 101

You can use the following information to help prepare for your upgrade of IBM Spectrum Control. Good planning helps you avoid delays and problems when you upgrade your system.

"Editing the upgrade response file" on page 188

When you upgrade using the silent mode, use the silent_Upgrade.properties file.

"Planning for IBM Spectrum Control authentication and authorization" on page 17 An operating system user name is required to install and log on to IBM Spectrum Control for the first time.

After you install IBM Spectrum Control, you can assign roles to users. Roles determine the product functions that are available to users.

"Reviewing the log files to resolve installation issues" on page 77

If an error occurs during IBM Spectrum Control installation, you can review the error log files to resolve issues and continue the installation.

Upgrading Storage Resource agents

Upgrade Storage Resource agents to ensure that they are at the same release level as the IBM Spectrum Control server.

When you apply maintenance to IBM Spectrum Control, you can upgrade Storage Resource agents immediately or at a later time. To ensure that all your agents are at the current release level and to manage your network load, schedule upgrades regularly.

If a Storage Resource agent is not at the same level as the IBM Spectrum Control server, the following limitations occur:

- New functions in the current release might not be available for the resources that are monitored by the agent.
- Problem fixes are not applied to the agent.

You can upgrade Storage Resource agents by using the following methods:

- Use the Modify Agents > Upgrade action on the Servers page in the GUI.
- Use a Storage Resource agent command.

To determine if a Storage Resource agent must be upgraded, complete the following steps:

- 1. In the menu bar, go to **Servers** > **Servers**.
- 2. View the values in the Agent State column.

If the state of the agent is **Upgraded needed**, the Storage Resource agent for the related server must be upgraded.

Starting agent upgrades

Upgrade a Storage Resource agent to the same release level as the IBM Spectrum Control server.

The ability to start the upgrade process for a Storage Resource agent is available when the following conditions are met:

- A Storage Resource agent must be deployed on the server that you want IBM Spectrum Control to monitor.
- An agent upgrade is not currently running for the server.
- The version of the agent that is deployed on the server is earlier than the IBM Spectrum Control server version.

Restriction: It is not possible to run a scheduled upgrade from versions of a Windows Storage Resource agent deployed in non-daemon mode when you upgrade from IBM Spectrum Control version 5.2.8, 5.2.9, 5.2.10 or 5.2.11 to IBM Spectrum Control version 5.2.13 or later versions.

To upgrade a Storage Resource agent that was not upgraded at maintenance time, complete the following steps:

- 1. In the menu bar, go to **Servers** > **Servers**.
- 2. On the **Servers** page, right-click the server that contains the Storage Resource agent to upgrade and select **Modify Agents > Upgrade**.
- 3. Select Immediate from the Agent Upgrade list on the Upgrade Agent window.
- 4. Click **Upgrade** to start the upgrade process.

Scheduling agent upgrades

Schedule the upgrade process for a Storage Resource agent.

You can schedule the upgrade process for a Storage Resource agent when the following conditions are met:

- A Storage Resource agent must be deployed on the server that you want IBM Spectrum Control to monitor.
- An agent upgrade is not currently running for the server.
- The version of the agent that is deployed on the server is earlier than the IBM Spectrum Control server version.

Tips:

- To manage the workload for a server and the network, schedule the agent upgrade for a time when the server and network are not busy.
- The scheduled time for an agent upgrade is based on the time zone of the IBM Spectrum Control server, not the time zone of the server where the Storage Resource agent is installed. For example, if an agent is installed on a server in the Central (CST) time zone, but the IBM Spectrum Control server is in the Pacific (PST) time zone, the time that is shown in the web-based GUI when you schedule the upgrade is PST.

Restriction: It is not possible to run a scheduled upgrade from versions of a Windows Storage Resource agent deployed in non-daemon mode when you upgrade from IBM Spectrum Control version 5.2.8, 5.2.9, 5.2.10 or 5.2.11 to IBM Spectrum Control version 5.2.13 or later versions.

To schedule the upgrade of a Storage Resource agent that was not upgraded at maintenance time, complete the following steps:

- 1. In the menu bar, go to **Servers** > **Servers**.
- 2. On the **Servers** page, right-click the server that contains the Storage Resource agent to upgrade and select **Modify Agents > Upgrade**.
- 3. Select Scheduled from the Agent Upgrade list on the Upgrade Agent window.
- 4. Select the date and time and click **Upgrade** to schedule the agent upgrade.

Upgrading Storage Resource agents by using a command

You can manually upgrade Storage Resource agents.

To manually upgrade the Storage Resource agent, complete the following steps:

1. Go to the DVD location of the installation program (by using the Storage Resource Agent image) and go to the bin directory:

cd DVD_image_location/data/sra/operating_system_name

Where DVD_image_location is the location of the installation image for the Storage Resource agent.

2. Run the upgrade command:

```
▶ bin/Agent — -upgrade — -installLoc — agent_install_directory →
```

-commType Daemon

Notes:

¹ Parameter when the agent is run as a daemon service.

The parameters are:

-installLoc "agent_install_directory"

Location where the agent is installed. Enclose the directory name in quotation marks, for example, "C:\Program Files\IBM\TPC_SRA\".

-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 by using the default location:

```
bin/Agent -upgrade
-installLoc "/opt/IBM/TPC/"
-commType Daemon
```

Here is an example for a non-daemon service by using a non-default location:

```
bin/Agent
-upgrade -installLoc "C:\Program Files\IBM\TPC_SRA\"
```

Tip: If you run the upgrade program outside of the *DVD_image_location* installation directory, then you must specify the full path.

Upgrading Windows Storage Resource agents from previous versions to 5.2.13 or later

To upgrade a Windows Storage Resource agent in non-daemon mode from versions 5.2.8, 5.2.9, 5.2.10 and 5.2.11 of IBM Spectrum Control to version 5.2.13 or later, require a different process from the standard upgrade steps.

You can use two procedures for upgrading a Windows Storage Resource agent to version 5.2.13 or later.

The manual upgrade procedure from the command prompt preserves the historical data for the Storage Resource agent.

The procedure that uses the IBM Spectrum Control GUI requires creating a new agent and losing the historical data.

Option	Description	
Upgrade by using command prompt	1. Download the latest version of IBM Spectrum Control Agent refresh pack from Fix Central. You can access Fix Central at <u>http://</u> www.ibm.com/support/fixcentral/	
	Open a Windows command prompt in the directory where you downloaded the refresh pack.	
	3. Run the following command from the command line:	
	Agent.exe -UPGRADE -INSTALLLOC <sra install="" location=""></sra>	
Upgrade steps by using the GUI	 1. Remove the server that the Storage Resource agent is deployed to. 2. Deploy a new Storage Resource agent. 	
	CAUTION: If you use this option, historical data for the Storage Resource agent is lost.	

Upgrading SMI-S providers for storage systems

Before you upgrade an SMI-S provider (also called the CIM agent or CIMOM agent), ensure that IBM Spectrum Control supports the SMI-S provider that you want and that the provider is compatible with the firmware versions of your storage systems.

To ensure that an SMI-S provider is supported, review the supported products list for the current release of IBM Spectrum Control. For more information about the products that are supported by IBM Spectrum Control Version 5.2 (or later), see see It http://www.ibm.com/support/docview.wss?uid=swg21386446.

Under Storage, click the link for the appropriate release. If you are uncertain about the SMI-S provider support, contact IBM customer support to help you with your upgrade plans.

Upgrading CIM agents

To upgrade a Common Information Model (CIM) agent, you must have the upgrade instructions that are supplied by the provider of the agent.

To upgrade the CIM agent, follow these steps:

- 1. Stop all IBM Spectrum Control server activity that might be dependent on the CIM agent (for example, performance monitor jobs, and discovery or probe jobs).
- 2. Stop the IBM Spectrum Control server services.
- 3. If any IBM Spectrum Control server processes remain, shut down the IBM Spectrum Control server for the duration of the CIM agent upgrade. If it is not possible to shut down the IBM Spectrum Control server, stop or kill the running processes.
- 4. Upgrade the CIM agent.
 - a. Refer to the instructions supplied by the CIM agent 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 IBM Spectrum Control are still in place, and that all devices managed by the CIM agent are still listed.
- 5. Restart the IBM Spectrum Control server and IBM Spectrum Control server services.
- 6. Open the IBM Spectrum Control GUI.
- 7. Run a CIM object manager (CIMOM) discovery job.
- 8. Run a probe job for each storage system that is managed by the CIM agent.

Migrating alert definitions from Tivoli Storage Productivity Center 5.2.7

When you upgrade from Tivoli Storage Productivity Center 5.2.7 and earlier to IBM Spectrum Control 5.2.10 or later, all the alert definitions for performance and configuration conditions are automatically migrated.

Important: Before you upgrade to IBM Spectrum Control and migrate alert definitions, ensure that you back up the product database. If the upgrade and migration is interrupted, the database might be left in an incomplete state and unusable. This situation might occur because of a power failure or memory issues during the upgrade. If an upgrade is interrupted, use the backups to restore the database to its original state and rerun the upgrade process.

For more information about backing up the product database, see <u>"Backups" on page 105</u>.

For more information about restoring the database, see http://www.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.admin.ha.doc/doc/t0006242.html

Performance alerts

Alert definitions that contain performance thresholds are automatically migrated during the upgrade process. Violations of those thresholds will be detected as they were in previous versions of the product.

The names of the alert definitions are converted to matching names in IBM Spectrum Control. For example, if you defined a *Total I/O Rate Threshold* alert for a storage system in Version 5.2.7, that definition is migrated to version 5.2.10 and is shown as *Total I/O Rate - overall* for that storage system.

Example names of 5.2.7 and earlier performance alerts	Example names of 5.2.8 and later performance alerts
Peak Back-end Write Response Time Threshold	Disk: Response Times
Total I/O Rate Threshold	Peak Back-end Write Response Time
	Volume: I/O Rates
	Total I/O Rate - overall

Configuration alerts

Alert definitions that contain configuration conditions are automatically migrated during the upgrade process. Violations of those conditions will be detected as they were in previous versions of the product. Examples of configuration alerts include Probe Failed, *resource* Missing, and *resource* Discovered.

The names of the alert definitions are converted to matching names in IBM Spectrum Control. For example, if you defined a *Probe Failed* alert for a storage system in Version 5.2.7, that definition is migrated to version 5.2.10 and is shown as *Probe Status* with a condition of *Error* for that storage system.

Example names of 5.2.7 and earlier configuration alerts	lier configuration alerts Example names of 5.2.8 and later configuration alerts		
Probe Failed	Probe Status	Error	~
Performance Monitor Failed	Performance Monitor Status	Error	\sim

Restriction for alert log entries: The existing entries for configuration alerts in the alert log are not migrated to IBM Spectrum Control 5.2.10 and later.

Alert notification settings

The global alert notification settings for alerts were consolidated in IBM Spectrum Control. Instead of separate notification settings for performance and configuration alerts, there is a single setting for all types of alerts. During the upgrade process, global alert notification settings are migrated in the following way:

- If alert notification settings were defined for performance alerts only, those settings are used as the global setting for all alerts.
- If alert notification settings were defined for configuration alerts only, those settings are used as the global setting for all alerts.
- If alert notification settings were defined for both performance and configuration alerts, the setting for performance alerts is used as the global setting for all alerts.

To view the global alert notification settings for all alerts, go to **Settings** > **Alert Notifications**.

Additionally, the alert notification settings that you can define at the resource level were consolidated. In previous releases, you had to define notifications for performance and configuration alerts separately. In IBM Spectrum Control, the notification settings that you define for a resource are automatically applied to both types of alerts. To view the alert notification settings for a specific resource, go to a resource list page, right-click a resource, and click **Edit Alert Notification Settings**.

Alert suppression settings

In IBM Spectrum Control 5.2.10 and later, you can customize how often you receive notifications for configuration and performance alerts. In previous versions, you could only suppress notifications for performance alerts. During an upgrade, any existing suppression settings in alert definitions are migrated. In alert definitions where suppression settings are not specified, or the settings can't be migrated, a default suppression setting is automatically selected for those definitions.

The following suppression settings are available for performance and configuration alerts in IBM Spectrum Control:

Do not suppress alerts

Receive alert notifications whenever an alert violation is detected.

Only alert once until problem clears

Receive one notification for an alert violation, even if the condition is violated multiple times.

Only generate alerts every

Receive one notification when an alert is initially violated. The alert is suppressed and no notifications are sent until both the specified time has passed and the alert is triggered again.

Do not alert until the condition is violated for more than

Do not receive notifications for an alert unless the violation is not cleared for longer than the specified time.

The next steps

After an upgrade to IBM Spectrum Control 5.2.10 or later is complete, the ability to define alerts and be notified of changes and conditions on resources is significantly enhanced. You can define alerts for all the key attributes of a resource, including attributes for status, configuration, capacity, and performance. These new alert definitions include criteria that you can customize to determine when alerts are generated.

For example, for a capacity attribute such as Available Drive Capacity, you can specify that an alert is generated when the amount of available capacity on a resource's disks is less than or equal to 50 GiB. The operator (less than or equal to) + a specified capacity (50) + the unit of measurement (GiB) is the criteria that determines if an alert is generated. For a configuration alert such as Firmware, you can generate alerts when the firmware version changes, when it is a specific version, or when it contains certain values.

Tip: Because of these enhancements and the overall streamlining of alerting capabilities, a number of configuration alerts in Tivoli Storage Productivity Center 5.2.7 and earlier were either removed, renamed, or consolidated into other alerts in IBM Spectrum Control. For information about the conditions that are

available for triggering alerts in IBM Spectrum Control, see 🖙 Triggering conditions for alerts

Important note about NetApp Filers: When you upgrade from a previous version to IBM Spectrum Control 5.2.10 or later, the alert definitions for NetApp filers will be migrated. However, to generate alerts for those filers, you must monitor them through direct connections rather than through Storage Resource agents.

In Tivoli Storage Productivity Center 5.2.7 and earlier, you could monitor NetApp filers by using Storage Resource agents. In IBM Spectrum Control, you must add those NetApp filers again and enter the credentials for connecting to them directly. After you add the NetApp filers, the previous entries for the filers are automatically removed and alerts will be generated for the alert definitions that were migrated.

For information about to how to add NetApp filers, see 🖙 Adding and configuring NetApp devices

Dell EMC VMAX storage systems: In IBM Spectrum Control 5.2.12 or earlier, VMAX disk groups were represented as pools within the SMI-S model. When you upgrade from a previous version to IBM Spectrum Control 5.2.13 or later, the alert definitions for VMAX storage systems will be migrated. If disk groups were represented as pools, the following alerts are migrated:

VMAX Pool alerts in 5.2.12 and earlier	VMAX Disk Group alerts in 5.2.13 and later
Status Deleted Pool New Pool	Status Removed Disk Group New Disk Group

Migrating alert definitions to alert policies

When you upgrade to IBM Spectrum Control V5.3.2 or later, all of your monitored resources retain their existing alert definitions and are not included in an alert policy. However, at any time, you can place resources into an alert policy or create a policy based on a resource.

Use alert policies to manage the alert definitions and notification settings that apply to different sets of resources. Here are some reasons to place resources in an alert policy:

- You want to manage alert conditions and notification settings for a group of resources of the same type. For example, if you have several SAN Volume Controller storage systems in your environment, you can create an alert policy so that the alert definitions are the same for all of the SAN Volume Controller systems. Note that alert policies manage one type of resource only.
- You want to use one alert policy for the storage systems in your test environment, and another for the storage systems in your production environment.

Tips:

- Alert policies manage one type of resource only.
- A resource can be managed by only one alert policy.
- If a resource is managed by a policy, the resource cannot have alert definitions and notification settings that are independent of the policy. The alert definitions and notification settings that apply to the resource come from the policy.

It is not a requirement for resources to be managed by an alert policy. You can define alert conditions and notification settings for individual resources.

You can also define alerts and notification settings for applications and general groups to manage alerts for groups of resource components such as volumes or pools.

Migrating alert definitions from resources to alert policies

If you want to create a new alert policy that uses the alert definitions from one of your resources, complete the following steps:

- 1. Go to the details page for the resource from which you want to create the policy. For example, to create an alert policy from a FlashSystem 9100, click **Storage** > **Block Storage Systems**.
- 2. Right-click the resource, then click **View Alert Definitions**.
- 3. Click Create Policy from the Policy Actions menu.
- 4. Type a name for the policy.
- 5. Make sure that the **Use alert definitions and notification settings from** *resource_name* option is selected.
- 6. Select any other resources that you want to add to the policy from the table of resources. Alert definitions in the policy are automatically applied to the resources you select. You can also choose to add resources later.

Migrating groups

When you upgrade to IBM Spectrum Control V5.2.10 or later, the reporting, monitoring, and storage resource groups that were created in IBM Tivoli Storage Productivity Center V5.2.7 or earlier are automatically migrated.

Reporting groups and monitoring groups

Reporting groups and monitoring groups were available in the stand-alone GUI of IBM Tivoli Storage Productivity Center Version 5.2.7 and earlier, as the following types of groups:

Server groups

- File system groups
- Storage system groups, including storage virtualizers
- Fabric monitoring groups

These groups are deprecated since IBM Spectrum Control Version 5.2.8. After you upgrade, copies of the groups are available as general groups in the IBM Spectrum Control GUI, and as storage resource groups in the Cognos Analytics reporting tool.

If your reporting groups and monitoring groups have more than two hierarchical levels, the hierarchical structure of the groups is changed during migration. For example, if group B is a member of group A, then members of group B become members of group A. Members of group B also remain members of group B. Group B is removed as a member of group A. After migration, you can use subgroups of general groups to organize resources into a hierarchical group.

Restrictions: The following types of reporting groups and monitoring groups are not migrated:

- Groups that are related to databases, directories, OS groups, tapes, and users.
- Default reporting and monitoring groups that were created by IBM Tivoli Storage Productivity Center but never modified.

Storage resource groups

After you upgrade, storage resource groups are available as general groups in the IBM Spectrum Control GUI. The hierarchical structure of storage resource groups is not changed during migration.

Accessing general groups and storage resource groups

Click Groups > General Groups to access general groups in the IBM Spectrum Control GUI.

You can access the storage resource groups in the Cognos Analytics reporting tool under the Capacity and Relationships package. Any updates to the general groups are reflected in the corresponding storage resource groups, but not in the deprecated reporting and monitoring groups.

Scenario: Changing from LDAP and Local OS authentication to only LDAP or Local OS authentication after an upgrade

In this scenario, you change from LDAP and Local OS authentication to only LDAP or Local OS authentication.

You were running an earlier version of IBM Spectrum Control with both LDAP and Local OS authentication configured. You upgraded to the latest version of IBM Spectrum Control. The preferred method of authentication is to select either LDAP or Local OS authentication.

- 1. Back up the ldapregistry.xml file in the *installation_dir/wlp/usr/servers/webServer/* registry/ directory.
- 2. Log on as an administrator to the IBM Spectrum Control GUI.
- 3. Click **Settings** > **User Management**.

Use	r Management
Authentication: LDAP and Local OS Your system is currently configured with LDAP and Local OS authentication. The preferred method is to select a single authentication configuration. Edit Authentication	
I≡ Actions + Add	Group
Name	Role
LocalGroup	Administrator
🚇 root	Administrator
SCTestGroup	Administrator

- 4. Click Edit Authentication.
 - a) On the **Authentication Configuration** page, uncheck **LDAP**, if you want to change from LDAP and Local OS authentication to *only* Local OS authentication, and click **Save**.
 - b) On the Authentication Configuration page, uncheck Local OS, if you want to change from LDAP and Local OS authentication to only LDAP authentication and you do not want to alter your LDAP settings, and click Save.
 - c) On the **Authentication Configuration** page, uncheck **Local OS**, if you want to change from LDAP and Local OS authentication to *only* LDAP authentication and you **do** want to alter your LDAP settings, then start with Step 6 in

Adding an LDAP repository to the federated repositories for IBM Spectrum Control
Chapter 4. Uninstalling

You can uninstall IBM Spectrum Control by using the uninstallation program or by using silent mode from the command line.

To uninstall IBM Spectrum Control, uninstall these components and related software:

- Uninstall any Storage Resource agents installed on your remote systems.
- If all IBM Spectrum Control components are installed on one server, uninstall all components.
- If the database repository is installed on a separate server, uninstall the IBM Spectrum Control components on the first server, and then uninstall the database repository on the second server.
- Uninstall IBM[®] Db2[®].

Note: On the Windows operating system, before you uninstall IBM Spectrum Control, if you installed the Monitoring Agent service, stop the **Monitoring Agent for Windows OS - Primary** and **Monitoring Agent for Windows OS - Watchdog** services.

Uninstalling IBM Spectrum Control in a single-server environment

In a single-server environment, you can uninstall IBM Spectrum Control by using the uninstallation program. The uninstallation process requires minimal user interaction.

To uninstall the software in a single-server environment:

- 1. Log on to the IBM Spectrum Control host server with the appropriate user privileges.
- 2. Start the IBM Spectrum Control uninstallation program for your operating system.
 - For the Windows operating system:
 - a. Click Start > Control Panel > Programs > Programs and Features.
 - b. Highlight IBM Spectrum Control and click Uninstall/Change.
 - For the AIX or Linux operating systems:

Run the following command from the root directory:

installation_dir/_uninst/uninstall

where *installation_dir* is where IBM Spectrum Control is installed.

- 3. Review the message that indicates that all the installed IBM Spectrum Control components are uninstalled.
- 4. Click Uninstall and click Next.

You cannot cancel the uninstallation process after it starts.

5. Restart the system if needed.

For the Windows operating system, you can restart the system now or later. You must restart the system to reinstall IBM Spectrum Control.

For the AIX or Linux operating system, you *do not* have to restart the system.

6. If an error occurred during the uninstallation process, review the installation log files.

Related reference

"Planning for IBM Spectrum Control authentication and authorization" on page 17 An operating system user name is required to install and log on to IBM Spectrum Control for the first time. After you install IBM Spectrum Control, you can assign roles to users. Roles determine the product functions that are available to users.

"Reviewing the log files to resolve installation issues" on page 77

If an error occurs during IBM Spectrum Control installation, you can review the error log files to resolve issues and continue the installation.

Uninstalling IBM Spectrum Control in a multiple-server environment

You can uninstall IBM Spectrum Control by using the uninstallation program. This uninstallation process requires minimal user interaction.

For this procedure, the terms *Server A* and *Server B* denote the two servers. The IBM Spectrum Control database repository is installed on *Server A* and the IBM Spectrum Control servers are installed on *Server B*.

To uninstall the software in a multiple-server environment, complete the following steps:

1. Complete these steps on *Server B*:

- a) Log on to *Server B* with the appropriate user privileges to uninstall the IBM Spectrum Control components.
- b) Start the IBM Spectrum Control uninstallation program.

For the Windows operating system, click **Start** > **Control Panel** > **Programs** > **Programs and Features**. Highlight **IBM Spectrum Control** and click **Uninstall/Change**.

For the AIX or Linux operating system, run the following command from the root directory:

installation_dir/_uninst/uninstall

where *installation_dir* is the location where IBM Spectrum Control is installed.

A window is displayed that indicates that all IBM Spectrum Control components installed on the system will be uninstalled.

- c) Click Uninstall. A confirmation is displayed.
- d) Click **Next** to start the uninstallation process.

Tip:

Remember the following for your operating system:

- For the Windows operating system, when the uninstallation process is finished, a window is displayed so you can choose to start your system now or later. You must restart the system before you can reinstall IBM Spectrum Control.
- For the AIX or Linux operating system, you do not have to restart your system.
- 2. Complete these steps for Server A:
 - a) Log on to *Server A* with the appropriate user privileges to uninstall the IBM Spectrum Control database repository.
 - b) Start the IBM Spectrum Control uninstallation program.
 - c) Follow the instructions to uninstall the database repository.
- 3. If an error occurred during the installation process, review the installation log files.

Related reference

"Planning for IBM Spectrum Control authentication and authorization" on page 17

An operating system user name is required to install and log on to IBM Spectrum Control for the first time. After you install IBM Spectrum Control, you can assign roles to users. Roles determine the product functions that are available to users.

"Reviewing the log files to resolve installation issues" on page 77

If an error occurs during IBM Spectrum Control installation, you can review the error log files to resolve issues and continue the installation.

Uninstalling IBM Spectrum Control by using silent mode

You can uninstall IBM Spectrum Control by using silent mode. This mode is useful if your system is running from a terminal that cannot display graphics.

In silent mode, the following server configurations are possible:

Tip: The terms Server A and Server B denote the two servers in a multiserver environment.

Option 1

All IBM Spectrum Control components are installed on one server (single-server environment).

Option 2

The IBM Spectrum Control database repository is installed on Server A and all other IBM Spectrum Control components are installed on Server B.

To uninstall IBM Spectrum Control by using silent mode, complete the following steps:

- 1. Complete the following steps for option 1:
 - a) Log on to the IBM Spectrum Control system with the appropriate user privileges.
 - b) Start the uninstallation program.
 - For the Windows operating system, run the following in the C:\ directory:

installation_dir_uninst\uninstall.bat -i silent

• For the AIX or Linux operating systems, run the following command from the root directory:

installation_dir/_uninst/uninstall -i silent

where *installation_dir* is where IBM Spectrum Control is installed.

- c) Restart the system, if needed.
 - For the Windows operating systems, restart the system after the uninstallation process is complete.
 - For the AIX or Linux operating systems, you do not have to restart your system.
- 2. Complete the following steps for option 2:
 - a) Log on to Server B with the appropriate user privileges to uninstall IBM Spectrum Control.
 - b) Start the uninstallation program.
 - For the Windows operating system, run the following from the C:\ directory:

installation_dir_uninst\uninstall.bat -i silent

• For the AIX or Linux operating system, run the following command from the root directory:

```
installation_dir/_uninst/uninstall -i silent
```

- c) Restart the system, if needed.
 - For the Windows operating systems, restart the system after the uninstallation process is complete.
 - For the AIX or Linux operating systems, you do not have to restart your system.
- d) Log on to Server A with the appropriate user privileges to uninstall the IBM Spectrum Control database repository.
- e) Start the uninstallation program.

• For the Windows operating system, run the following command from the C:\ directory:

```
installation_dir\_uninst\uninstall.bat -i silent
```

- f) Restart the system, if needed.
 - For the Windows operating systems, restart the system after the uninstallation process is complete.
 - For the AIX or Linux operating systems, you do not have to restart your system.

Related tasks

"Manually uninstalling IBM Spectrum Control components on Windows" on page 209 If the IBM Spectrum Control uninstallation process fails, you must manually uninstall the components.

<u>"Manually uninstalling IBM Spectrum Control components on AIX or Linux" on page 208</u> If the IBM Spectrum Control uninstallation process fails, you must manually uninstall the components.

Related reference

"Planning for IBM Spectrum Control authentication and authorization" on page 17 An operating system user name is required to install and log on to IBM Spectrum Control for the first time. After you install IBM Spectrum Control, you can assign roles to users. Roles determine the product functions that are available to users.

"Reviewing the log files to resolve installation issues" on page 77 If an error occurs during IBM Spectrum Control installation, you can review the error log files to resolve issues and continue the installation.

Manually uninstalling IBM Spectrum Control components on AIX or Linux

If the IBM Spectrum Control uninstallation process fails, you must manually uninstall the components.

This procedure assumes the following conditions:

- You installed IBM Spectrum Control in the default directory.
- You used default ports.
- You used the default IBM Spectrum Control database repository named TPCDB.

To manually uninstall IBM Spectrum Control components, complete the following steps:

1. Run the following command to stop the Storage Resource agent:

```
kill -9 `ps -aef | grep /opt/IBM/TPC/agent| grep -v grep | awk '{ print $2 }'` 2> /dev/null
```

2. Run the following command to stop the Data server:

kill -9 `ps -aef | grep data | grep -v grep | awk '{ print \$2 }'` 2> /dev/null

3. Run the following command to stop the Device server:

```
kill -9 `ps -aef | grep deviceServer | grep -v grep | awk '{ print $2 }'` 2> /dev/null
```

4. Run the following command to stop the Alert server:

kill -9 `ps -aef | grep alertServer | grep -v grep | awk '{ print \$2 }'` 2> /dev/null

5. Run the following command to stop the Export server:

```
kill -9 `ps -aef | grep export | grep -v grep | awk '{ print $2 }'` 2> /dev/null
```

6. Run the following command to stop the GUI:

```
kill -9 `ps -aef | grep webServer | grep -v grep | awk '{ print $2 }'` 2> /dev/null
```

7. Run the following command to stop the data collector:

```
kill -9 `ps -aef | grep collector | grep -v grep | awk '{ print $2 }'` 2> /dev/null
```

- 8. Drop the database by completing the following steps:
 - a. Source the db2profile.
 - b. Enter db2 drop db TPCDB.
- 9. Go to the /db2_admin_home/db2_*instance_name*/ directory and ensure that the database directory is deleted.
- 10. Delete the following files and folders:
 - rm -r `find /etc -name *tpcdsrv* -print`
 - rm -r `find / -name *itsanm* -print`
 - rm -r /etc/Tivoli/TSRM/registry
 - rm -r /etc/Tivoli/TSRM/registryNA
 - rm -r /etc/Tivoli/TSRM/lock
 - rm -fr /opt/IBM/TPC

Manually uninstalling IBM Spectrum Control components on Windows

If the IBM Spectrum Control uninstallation process fails, you must manually uninstall the components.

This procedure assumes that the following conditions are met:

- You installed IBM Spectrum Control in the default directory.
- You used default ports.
- The Storage Resource agent service name is Agent1.
- You used the default IBM Spectrum Control database repository name TPCDB.

To manually uninstall IBM Spectrum Control components, complete the following steps in a Windows command window:

1. To uninstall the Storage Resource agent, run the following command:

```
sc stop Agent1
sc delete Agent1
```

2. To remove the Storage Resource agent registry entries, run the following command:

reg delete HKLM\SOFTWARE\IBM\TPCAGENT\1

where 1 is the instance of the Agent.

If you do not have multiple agents, you can also run the following command:

reg delete HKEY_LOCAL_MACHINE\SOFTWARE\IBM\TPCAGENT

Important: If you have multiple agents and you run this command, all of the agents are deleted.

3. To uninstall the Data server, run the following commands:

```
sc stop TSRMsrv1
sc delete TSRMsrv1
```

4. To stop the Device server and data collector, run the following command:

```
cd C:\Program Files\IBM\TPC\scripts stopTPCdevice.bat
```

Tip: If the script does not exist, run the following command to stop the Device server:

```
sc stop deviceServer
```

If the script does not exist, run the following command to stop the data collector:

sc stop datacollector1

5. To delete the Device server, run the following command:

sc delete deviceServer

6. To delete the data collector, run the following command:

```
sc delete datacollector1
```

7. Run the following commands to uninstall the Alert server:

```
sc stop alertServer
sc delete alertServer
```

8. Run the following commands to uninstall the Export server:

```
sc stop exportServer
sc delete exportServer
```

9. Run the following commands to uninstall the Web server:

```
sc stop webServer
sc delete webServer
```

10. Run the following commands to delete the wlp directories:

```
cd C:\Program Files\IBM\TPC del wlp
```

11. Run the following command to remove the IBM Spectrum Control directories:

```
rmdir /s/q "C:\Program Files\IBM\TPC"
```

12. Restart your computer.

Uninstalling Storage Resource agents

You can uninstall locally or remotely installed Storage Resource agents.

To uninstall a Storage Resource agent, use the GUI to remove the server that the agent is deployed on.

Uninstalling Storage Resource agents manually

You can manually uninstall Storage Resource agents.

To uninstall a Storage Resource agent, complete the following steps:

- 1. If the Storage Resource agent is on the Virtual I/O system, complete the following steps:
 - a. Log in with the **padmin** user ID.
 - b. Run the following command to set up the AIX environment:

oem_setup_env

2. Go to the directory where the agent is installed:

agent_install_location

where *agent_install_location* is where the Storage Resource agent is installed.

3. Run the uninstallation command:

Restriction: Do not delete the Storage Resource agent component from the IBM Spectrum Control server by using the GUI or the command-line interface. This component must exist on the server to complete the uninstall process.

```
bin/Agent — -uninstall ______ -serverName — TPC_server_name ___
```

🦾 -debug MAX 🛛 –

Where:

-uninstall

Uninstalls the agent.

-force

This optional parameter forces an uninstallation. If you use this parameter, do not provide the serverName parameter.

-serverName TPC_server_name

TPC_server_name is the Data server name as defined in IBM Spectrum Control. You can check the configuration file for the server name:

agent_install_location/config/Agent.config

where *agent_install_location* is where is the agent is installed.

-debug MAX

This optional parameter is for debugging purposes. If you set the **-debug** parameter, then some files are not deleted.

Tip: If you run the uninstallation program from the bin directory, the bin directory is not deleted.

If you run the uninstallation program outside of the agent installation directory, then you must specify the full path.

If the uninstallation fails, you must look at the return codes. For more information about return codes,

see http://www.ibm.com/support/knowledgecenter/SS5R93_5.3.7/com.ibm.spectrum.sc.doc/ fqz0_r_return_codes_used_by_strg_resource_agent.html.

Deleting Storage Resource agent registry entries after a failed installation or uninstallation

If your IBM Spectrum Control installation or uninstallation fails, you must find and manually delete the Storage Resource agent registry entries that remain.

Deleting registry files in the Windows operating system

To delete registry entries after a failed installation or uninstallation in the Windows operating system:

- 1. In Windows Registry Editor, navigate to HKEY_LOCAL_MACHINE > SOFTWARE > IBM > TPCAGENT> NUMBER or HKEY_LOCAL_MACHINE > SOFTWARE > IBM > TPCAGENT.
- 2. Delete this entry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\IBM\TPCAGENT\1]
"Home"="C:\\Program Files\\IBM\\TPC"
"Port"="9567"
```

3. If the Storage Resource agent is running as a daemon service, delete the service.

For example, sc delete AgentX, where AgentX is the name of the Storage Resource agent.

4. Delete the folder in which the agent was installed.

Display the agent name and folder by running services.msc and right-click the service to see the properties.

5. For daemon agents, verify that the associated CAP file was deleted.

The CAP file is located in the %ALLUSERSPROFILE%\Application Data\IBM\CAP folder. The naming convention for this file is srainstance_default.xml.

Remember: After uninstalling a daemon agent, you must restart your system.

Deleting registry files on the UNIX or Linux operating systems

To delete registry entries after a failed installation or uninstallation on the UNIX or Linux operating systems:

1. Delete the Storage Resource agent entry that is associated with the IBM Spectrum Control installation on the local server.

The terms Server A and Server B are used in this procedure to denote the different servers.

When you install IBM Spectrum Control on Server A, a Storage Resource agent is also installed on Server A. When you deploy another Storage Resource agent from IBM Spectrum Control Server B to Server A, an entry is added to the file /etc/Tivoli/TSRM/registryNA on Server A. This entry is associated with the Storage Resource agent deployed from Server B.

If a failure occurs when you install or uninstall the Storage Resource agent from Server A, you must delete the entry from the /etc/Tivoli/TSRM/registryNA file that is associated with the agent on Server A. For example, you would delete these lines from the file:

```
Instance=1
Home=/opt/IBM/TPC
Port=9567
```

- 2. If the agent was a daemon, verify that the process is running and stop it.
 - To list all the running processes, run the following command:

ps -ef

• To stop a process, run the following command:

kill -9 process_number

3. For daemon agents, verify that the associated CAP File was deleted.

The CAP file is located in the /opt/IBM/CAP directory. The naming convention for this file is srainstance_default.xml.

Removing servers

You can remove servers that you no longer want to monitor with IBM Spectrum Control.

You can use the GUI to remove servers. If a Storage Resource agent is deployed to the server, the agent is uninstalled.

When the server is removed, it is no longer monitored by IBM Spectrum Control. All the data that was collected about the server is removed from the database repository.

Tip: When you remove a server, it is only removed from IBM Spectrum Control. The server is not physically deleted from the storage environment.

To remove a server, complete the following steps:

- 1. In the menu bar, go to **Servers** > **Servers**.
- 2. On the Servers page, right-click the server where the agent is deployed and select Remove.
- 3. Click **Remove** to confirm that you want to remove the server.

Uninstalling Db2

Uninstall IBM[®] Db2[®] after you uninstall IBM Spectrum Control. You must use the Db2[®] uninstallation program to uninstall Db2.

For information about uninstalling DB2[®] Version 10.5 on the Windows operating system, go to <u>Uninstalling</u> your DB2 database product (Windows).

For information about uninstalling Db2[®] Version 11.1 on the Windows operating system, go to <u>Uninstalling</u> your DB2 database product (Windows)

For information about uninstalling Db2 Version 11.5 on the Windows operating system, go to Uninstalling your DB2 database product (Windows)

Uninstalling Db2 on AIX or Linux

You can uninstall IBM[®] Db2[®] on UNIX or Linux systems.

To uninstall Db2[®] on AIX and Linux, complete the following steps:

- 1. As the Db2 instance user (typically db2inst1), drop the databases, and stop Db2.
 - a) If you are the user with root authority, run the **su db2inst1** command to switch the user to the Db2 instance user. Otherwise, log in as the Db2 instance user.
 - b) Run the **db2 list db directory** command to list the databases that might not have been removed by the IBM Spectrum Control uninstallation program.
 - c) For each database name listed by the command in the previous step, run the *database_name* command. For example:

```
Command:

$ db2 drop db tcpdb

Response:

DB20000I The DROP DATABASE command completed successfully.

$ db2 drop db ibmcdb

Response:

DB20000I The DROP DATABASE command completed successfully.
```

d) Run the **db2stop force** command. The following messages are displayed:

```
08/10/2015 21:46:13 0 0 SQL1064N DB2STOP processing was successful. SQL1064N DB2STOP processing was successful.
```

e) Run db2 terminate. The following message is displayed:

DB20000I The TERMINATE command completed successfully.

f) Run the **exit** command to close the su shell or log out.

2. Drop the Db2 instance.

Note: This step must be performed as a user with root authority and run in a shell that has not had the db2profile sourced.

- a) Log in as a user with root authority.
- b) Change to the Db2 instance directory. The default path depends on your operating system.

On AIX, run the cd /opt/IBM/db2/V11.5/instance command.

On Linux, run the cd /opt/ibm/db2/V11.5/instance command.

- c) Run the **./db2ilist** command to list the db2instance name (typically db2inst1).
- d) Run the **./db2idrop db2inst1** command where *db2inst1* is the instance name reported by the **db2ilist** command in the previous step.
- 3. As the Db2 administration server (DAS) user (typically dasusr1), stop DAS.
 - a) If you are the user with root authority, run **su dasusr1** to switch user to the DAS user. Otherwise, log in as the DAS user.

b) Run the **db2admin stop** command. The following message is displayed:

SQL4407W The DB2 Administration Server was stopped successfully.

- c) Run the **exit** command to close the su shell or log out.
- 4. Remove the Db2 administration server. You must remove the Db2 administration server before you remove the Db2 product.
 - a) Log in as a user with **root** authority.
 - b) Change to the Db2 instance directory. The default path depends on your operating system.

On AIX, run the cd /opt/IBM/db2/V11.5/instance.

On Linux, run the cd /opt/ibm/db2/V11.5/instance.

c) Run the **./dasdrop** command. The following messages are displayed:

SQL4410W The DB2 Administration Server is not active. DBI1070I Program dasdrop completed successfully.

- 5. 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) Change to the Db2 installation directory. The default path depends on your operating system.

On AIX, run cd /opt/IBM/db2/V11.5/install.

On Linux, run cd /opt/IBM/db2/V11.5/install.

b) Run the **./db2_deinstall** -a command. The following messages are displayed:

```
DBI1016I Program db2_deinstall is performing uninstallation.
Please wait.
The execution completed successfully.
For more information see the DB2 uninstallation log at
"/tmp/db2_deinstall.log.pid".
```

- 6. Delete Db2 users and groups. The default user and group names are shown in the following commands.
 - a) Run the following commands to remove the users:

```
userdel -r dasusr1
userdel -r db2inst1
userdel -r db2fenc1
```

b) Run the appropriate commands for your operating system to remove the groups.

On AIX run the following commands:

rmgroup dasadm1 rmgroup db2iadm1 rmgroup db2fadm1

On Linux run the following commands:

```
groupdel dasadm1
groupdel db2iadm1
groupdel db2fadm1
```

- 7. Remove the Db2 directory.
 - a) Run the **cd** command.
 - b) Run the command to remove the Db2 directory on your operating system:

On AIX, run the **rm -r /opt/IBM/db2** command.

On Linux, run **rm** -**r** /opt/ibm/db2 command.

8. Remove any Db2 definitions from /etc/services.

Uninstalling Tivoli Common Reporting and Jazz for Service Management

To uninstall Jazz for Service Management and Tivoli Common Reporting, follow the procedures in the Jazz for Service Management documentation.

Use the steps to uninstall Jazz for Service Management and related software that are provided in http://www-01.ibm.com/support/knowledgecenter/SSEKCU_1.1.0.3/com.ibm.psc.doc_1.1.0.3/install/ psc_c_install_uninstall_oview.html.

If your Deployment Engine, which is a component of Tivoli Common Reporting, is corrupt or partially

installed, use the steps to uninstall the Deployment Engine, that are provided in https://www.ibm.com/support/knowledgecenter/SSEKCU_1.1.0.3/com.ibm.psc.doc_1.1.0.3/tcr_original/ttcr_uninstal_manually.html

Chapter 5. Reference

agent.sh command

The **agent.sh** command lets you start, stop, and restart the Storage Resource agent. You can also display the status and version of the Storage Resource agent.

Note:

- You must have root authority to run this command.
- For Windows, the status, stop, and start functions are handled through the Windows Services panel.



Parameters:

status

Displays the current status of the Storage Resource agent. The status is returned is running or not running.

start

Starts the Storage Resource agent.

stop

Stops the Storage Resource agent.

restart

Stop and then start the Storage Resource agent.

version

Displays the current version of the Storage Resource agent.

versionall

Displays the version of the Storage Resource agent and its related components.

Appendix A. Accessibility features for IBM Spectrum Control

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

The following list includes the major accessibility features in IBM Spectrum Control:

- Keyboard-only operation in the GUI.
- A Knowledge Center that includes the following accessibility features:
 - The Knowledge Center is provided in XHTML 1.0 format, which is viewable in most web browsers.
 With XHTML, you can view documentation according to the display preferences that are set in your browser. XHTML supports screen readers and other assistive technologies.
 - All documentation for IBM Spectrum Control is available in Adobe Portable Document Format (PDF)
 - by using the Adobe Acrobat Reader. To access PDFs, go to 🖻 Printable documentation.
 - All images in the Knowledge Center are provided with alternative text, so that visually impaired users can understand the contents of the images.
- Interfaces that are commonly used by screen readers.

The setting for the automatic-refresh button in the screen reader is toggled to the ON position by default. If you want the screen reader to read the previous text, complete the following steps:

- 1. Navigate to the Accessibility Settings Navigation region by using the arrow keys. The region is located after the IBM Spectrum Control application title.
- 2. Click **Enter** to toggle the automatic-refresh button to the OFF position. (An alert sounds to make you aware that the turn-off automatic-refresh toggle button was pressed.)
- 3. To move backward to the previously read text so that the screen reader can read it again, use the arrow keys. You can move backwards and forwards through the page.
- 4. When you are ready to move on, click **Enter** to toggle the automatic-refresh button to the ON position and to refresh the page. (An alert sounds to make you aware that the turn-on, automatic-refresh toggle button was pressed.)

Tip: Alternatively, let the toggle setting persist, and refresh as needed by pressing the F5 key.

Keyboard navigation

Most of the features of the IBM Spectrum Control GUI are accessible by using the keyboard. For those features that are not accessible, equivalent function is available by using the command-line interface (CLI), except as noted in the product release notes.

You can use keys or key combinations to perform operations and initiate many menu actions that can also be done through mouse actions. The following sections describe the keys or key combinations for different parts of the GUI:

For navigating in the GUI and the context-sensitive help system:

- To navigate to the next link, button, or topic within a panel, press Tab.
- To move to the previous link, button, or topic within a panel, press Shift+Tab.
- To select an object, when the object is in focus, press Enter.

For actions menus:

• To navigate to the grid header, press Tab.

- To reach the drop-down field, press the Left Arrow or Right Arrow key.
- To open the drop-down menu, press Enter.
- To select the menu items, press the Up Arrow or Down Arrow key.
- To start the action, press Enter.

For filters:

To specify a filter option and text:

- 1. Press Tab to navigate to the magnifying glass icon.
- 2. Press the Up Arrow or Down Arrow key to navigate the filtering list.
- 3. Press Enter to select a filtering option.
- 4. When a filtering option is selected, the cursor moves to the filter text box. Type the filter text and press Enter. To reset a filter, press Enter.

For text fields:

- To navigate to text fields, press Tab.
- To navigate to the fields that are available for editing, press Tab.
- To navigate to the next field or to the **Submit** button, press Tab.

For tables or lists:

- To navigate between column headers, focus on a column header and use the Left Arrow and Right Arrow keys to move to other column headers.
- To navigate between data cells, focus on a data cell and use the Left, Right, Up, Down, Pageup, and Pagedown Arrow keys.
- To sort a column, focus on a column header and press Enter. The focus remains on the column header after the sort occurs.
- To change the size of a column, focus on the column header, hold Shift+Control, and press the Left or Right Arrow keys.
- To follow a link in a data cell, focus on a data cell and press Shift+F9.
- To open a menu for a table row, focus on the row and press Shift+F10.
- To select consecutive rows, select the first row and hold Shift, press the Up or Down Arrow keys to go to the last row in the range, and press the Space bar to add the new rows to the selection.
- To select non-consecutive rows, select a row and hold Control, press the Up or Down Arrow keys, and press the Space bar to add the new row to the selection.

Restriction: For Chinese languages, the keyboard combination Control+Space bar is not enabled for selecting multiple rows at the same time.

Keyboard navigation with Firefox for Mac users: If you're using Firefox on a Mac with IBM Spectrum Control and want to use keyboard navigation, complete the following steps:

- 1. In Firefox, go to **Preferences** > **Advanced** > **General** and clear the check mark for **Always use the cursor keys to navigate within pages**. This step enables the use of Tab key to navigate between GUI elements.
- 2. In the URL address bar of Firefox, type about:config and press Enter.

Tip: If a warning prompt is displayed, click the button to accept the risk of changing browser settings. Existing settings won't be changed; instead, you'll be adding a preference setting for accessibility.

- 3. To add an accessibility preference for tab focus, right-click on the configuration page and select **New** > **Integer**.
- 4. In the New integer value window, type accessibility.tabfocus and click OK.
- 5. Type **7** to set the integer value and click **OK**.
- 6. Open your Mac's System Preferences app, go to **Keyboard** > **Shortcuts**, and select **All Controls**.

IBM and accessibility

For more information about IBM's commitment to accessibility, see the IBM Human Ability and Accessibility Center website at th <u>http://www.ibm.com/able</u>.

Legal notices

This information was developed for products and services offered in the U.S.A. This material may be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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:

Intellectual Property Licensing Legal and Intellectual Property Law IBM Japan, Ltd. 19-21, Nihonbashi-Hakozakicho, Chuo-ku Tokyo 103-8510, 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 2Z4A/101 11400 Burnet Road Austin, TX 78758 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.

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.

COPYRIGHT LICENSE: This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/privacy/details in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software-as-a-Service Privacy Statement" at http://www.ibm.com/software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Trademarks

IBM, the IBM logo, and ibm.com[®] are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at https://www.ibm.com/legal/us/en/copytrade.shtml.

Intel, Intel logo, Intel Xeon, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Red Hat[®] is a registered trademark of Red Hat, Inc. or its subsidiaries 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 provides terms and definitions for IBM Spectrum Control.

The following cross-references are used in this glossary:

- See refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelledout form.
- See also refers you to a related or contrasting term.

"A" on page 227 "B" on page 228 "C" on page 228 "D" on page 230 "E" on page 231 "F" on page 232 "G" on page 234 "H" on page 234 "I" on page 235 "J" on page 236 "K" on page 236 "L" on page 236 "M" on page 236 "N" on page 237 "O" on page 237 "P" on page 238 "R" on page 239 "S" on page 240 "T" on page 245 "U" on page 245 "V" on page 244 "W" on page 245 "Z" on page 245

Α

activation key

See license key.

active management server

A management server from which the storage environment can be monitored and managed. The active management server replicates its database to the standby server.

advisory lock

A type of lock that a process holds on a region of a file that signals any other process to not use or lock the region or an overlapping region. Other processes are not forced to comply.

allocatable extent limit

A maximum total capacity for the system. The allocatable extent limit is calculated from pool extent sizes.

application key

See license key.

array

An ordered collection, or group, of physical devices (disk drive modules) that are used to define logical volumes or devices. An array is a group of drives designated to be managed with a Redundant Array of Independent Disks (RAID).

asynchronous replication

A type of replication in which control is given back to the application as soon as the write operation is made to the source volume. Some time later, the write operation is made to the target volume. See also synchronous replication.

audit log

An unalterable record of all commands or user interactions that are issued to the system.

authenticated user

A user who has logged in to the system with a valid account (user ID and password).

authentication

The mechanism by which a system determines what permissions a particular authenticated user has to access specific resources or actions. See also authorization.

authorization

The mechanism by which a system determines what permissions a particular authenticated user has to access specific resources or actions. See also authentication.

authorization code

An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

available capacity

The amount of usable capacity that is not yet used in a system, pool, array, or MDisk.

block storage

A unit of data storage on a device.

business continuity

The capability of a business to withstand outages and to operate mission-critical services normally and without interruption in accordance with predefined service-level agreements.

cache

Storage or memory that is used to improve access times to instructions, data, or both. For example, data that resides in cache memory is normally a copy of data that resides elsewhere in slower, less expensive storage, such as on a disk or on another network node.

cache eviction

A process by which data associated with a file is removed from the cache system. The data is removed either by using a Least Recently Used (LRU) algorithm when configured General Parallel File System (GPFS) hard or soft quota limits are exceeded or by issuing a command. When referenced again in the cache system, the data that is associated with the file is retrieved from the home system.

caching I/O group

The I/O group in the system that performs the cache function for a volume.

call home

A communication link established between a product and a service provider. The product can use this link to place a call to a service provider when it requires service. With access to the machine, service personnel can perform service tasks, such as viewing error and problem logs or initiating trace and dump retrievals.

capacity

The amount of data that can be contained on a storage medium.

capacity recycling

The amount of provisioned capacity that can be recovered without causing stress or performance degradation. This capacity identifies the amount of resources that can be reclaimed and provisioned to other objects in an environment.

capacity threshold

The percent of total usable physical capacity that used capacity must exceed before a notification is sent. See also total usable physical capacity.

certificate

A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority.

change volume

A volume that is used in Global Mirror that holds earlier consistent revisions of data when changes are made.

child pool

A user-defined capacity that is formed from capacity that is defined either in another pool or a system. See also parent pool.

CIFS

See Common Internet File System.

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 devices that are compliant with the Common Information Model (CIM).

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

See count key data.

CKD record

See count-key-data record.

CLI

See command-line interface.

client

A software program or computer that requests services from a server. See also host, server.

cloud account

An agreement with a cloud service provider to use storage or other services at that service provider. Access to the cloud account is granted by presenting valid credentials.

cluster

- 1. A collection of complete systems that work together to provide a single, unified computing capability.
- 2. A group of computers and other resources that operate together as a single system.
- 3. A loosely coupled collection of independent systems (or nodes) organized into a network for the purpose of sharing resources and communicating with each other.
- 4. 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.
- 5. In Storwize[®] V7000, a pair of nodes that provides a single configuration and service interface.

command-line interface (CLI)

A computer interface in which the input and output are text based.

Common Information Model (CIM)

An implementation-neutral, object-oriented schema for describing network management or systems management information. The Distributed Management Task Force (DMTF) develops and maintains CIM specifications.

Common Internet File System (CIFS)

A protocol that manages shared, remote file access for applications to files, printers, serial ports, and so on over a TCP/IP network.

community name

The part of an SNMP message that represents a password-like name and that is used to authenticate the SNMP message.

compression

A function that removes repetitive characters, spaces, strings of characters, or binary data from the data being processed and replaces characters with control characters. Compression reduces the amount of storage space that is required for data.

compute node

An independent machine that contains one or more microprocessors, memory, storage, and network controllers and runs its own operating system and applications.

concurrent copy

A function of the DFSMSdss component that is used to back up any collection of data at a point in time with minimum down time for the database or application that uses the collection of data.

consistency group

A group of copy relationships between virtual volumes or data sets that are maintained with the same time reference so that all copies are consistent in time.

copyback

A process that moves data back to its expected or preferred location to maintain an array in a more efficient configuration after a failed drive is replaced.

copy set

The set of source volumes or target volumes involved in a FlashCopy operation.

count key data

- 1. An architecture for a direct access storage device (DASD) device or logical device that specifies the access mechanisms for the logical data units on the device through a specific set of supported channel commands. Extensions to the CKD command set form the basis of Extended CKD.
- 2. A data recording format that uses self-defining record formats in which each record on a volume is represented by up to three fields: a count field identifying the record and specifying its format, an optional key field that can be used to identify the data area contents, and an optional data field that typically contains the user data. See also data record, storage architecture type.

count-key-data record (CKD record)

See data record.

CRU

See customer-replaceable unit.

customer-replaceable unit (CRU)

An assembly or part that can be replaced in its entirety by a user when any one of its components fails.

cylinder

A unit of storage on a count-key-data (CKD) device with a fixed number of tracks.

D

data collection

The process of obtaining performance and availability monitoring data and providing that data to a metric evaluator. Examples of data collectors include Domain Name System (DNS) probes, web page analyzers, or database analyzers. See also discovery.

data consistency

A characteristic of the data at the target site where dependent write order is maintained to guarantee the recoverability of applications.

data record

A basic unit of data recording format. See also count key data, fixed-block architecture.

data reduction

A set of techniques that can be used to reduce the amount of usable capacity that is required to store data. Examples of data reduction include data deduplication and compression. See also <u>data</u> reduction savings, stored capacity.

data reduction savings

The total amount of usable capacity that is saved in a system, pool, or volume through the application of an algorithm such as compression or deduplication on the written data. This saved capacity is the difference between the written capacity and the used capacity. See also data reduction.

data source

A storage resource or agent that provides data about a storage environment.

destage

To move data from cache to a nonvolatile storage medium.

discovery

The process of finding resources within an enterprise, including finding the new location of monitored resources that were moved. See also data collection.

distributed RAID

An alternative RAID scheme where the number of drives that are used to store the array can be greater than the equivalent, typical RAID scheme. The same data stripes are distributed across a greater number of drives, which increases the opportunity for parallel I/O and hence improves overall array performance. See also rebuild area.

DNS

See Domain Name System.

Domain Name System (DNS)

The distributed database system that maps domain names to IP addresses.

drive

A data storage device. A drive can be either a magnetic disk drive or a solid-state drive (SSD).

drive class

A combination of drive technology and speed, which uniquely defines a class of drives that have approximately the same performance characteristics.

drive technology

A category of a drive that pertains to the method and reliability of the data storage techniques being used on the drive. Possible values include enterprise (ENT) drive, nearline (NL) drive, or solid-state drive (SSD).

Ε

ECKD

See extended count key data.

effective capacity

The amount of provisioned capacity that can be created in a system or pool without running out of usable capacity given the current data reduction savings being achieved. This capacity equals the usable capacity divided by the data reduction savings percentage.

enclosure

The metal structure in which various electronic components are mounted.

encryption deadlock

The inability to access encryption keys to decrypt data. See also encryption recovery key.

encryption key label

The list of encryption key labels used by the storage system to identify keys that will be used on the key server.

encryption key manager

See encryption key server.

encryption key server

An internal or external system that runs a key manager that receives and then serves existing encryption keys or certificates to a storage system.

encryption recovery key

An encryption key that allows a method to recover from an encryption deadlock situation where the normal encryption key servers are not available. See also encryption deadlock.

enterprise

Pertaining to a type of data storage device that has higher error recovery limits, vibration tolerance, and end-to-end error detection than standard desktop hard drives.

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 the data server using Java Database Connectivity (JDBC).

event

An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

extended count key data (ECKD)

An extension of the count-key-data (CKD) architecture. It includes additional commands that can be used to improve performance.

extent type

See storage architecture type.

failback

The restoration of an appliance to its initial configuration after detection and repair of a failed network or component.

failover

An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

FB

See fixed block.

FBA

See fixed-block architecture.

FC

See Fibre Channel.

FC-AL

See Fibre Channel Arbitrated Loop.

FCIP

See Fibre Channel over IP.

FCP

See Fibre Channel Protocol.

feature activation code

See license key.

Fibre Channel (FC)

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. See also zoning.

Fibre Channel Arbitrated Loop (FC-AL)

An implementation of the Fibre Channel standards that uses a ring topology for the communication fabric; refer to American National Standards Institute (ANSI) INCITS 272-1996, (R2001). In this topology, two or more Fibre Channel end points are interconnected through a looped interface.

Fibre Channel connection (FICON)

A Fibre Channel communication protocol designed for IBM mainframe computers and peripherals.

Fibre Channel extender

A device used to extend a Fibre Channel link over a greater distance than is supported by the standard, usually a number of miles or kilometers. Devices must be deployed in pairs at each end of a link.

Fibre Channel over IP (FCIP)

A network storage technology that combines the features of the Fibre Channel Protocol and the Internet Protocol (IP) to connect distributed SANs over large distances.

Fibre Channel Protocol (FCP)

The serial SCSI command protocol used on Fibre Channel networks. See also open system.

FICON

See Fibre Channel connection.

field-replaceable unit (FRU)

An assembly that is replaced in its entirety when any one of its components fails.

file module

A component that provides file systems to network users. A file module must be provided with storage for the file systems.

fileset

See file set.

file set

- 1. A subset of a file system that provides granularity of functions such as snapshots or quotas within the file system.
- 2. A hierarchical grouping of files managed as a unit for balancing workload across a cluster.

file system (FS)

A collection of files and certain attributes associated with those files.

file system storage

Data storage that is organized into files and directories.

fixed block (FB)

See fixed-block architecture.

fixed-block architecture (FBA)

An architecture for a virtual device that specifies the format of and access mechanisms for the virtual data units on the device. The virtual data unit is a block. All blocks on the device are the same size (fixed size). The system can access them independently. See also <u>data record</u>, <u>storage architecture</u> type.

FlashCopy

- 1. Pertaining to a point-in-time copy where a virtual copy of a volume is created. The target volume maintains the contents of the volume at the point in time when the copy was established. Any subsequent write operations to the source volume are not reflected on the target volume.
- 2. An optional feature of the Storage System DS family that can make an instant copy of data, that is, a point-in-time copy of a volume.

flash drive

A data storage device, which is typically removable and rewritable, that uses solid-state memory to store persistent data. See also flash module.

flash module

A modular hardware unit containing flash memory, one or more flash controllers, and associated electronics. See also flash drive.

flush-through mode

See write-through mode.

form factor

The industry-standard physical dimensions of a storage system drive enclosure. Possible values include "3.5 inch", "2.5 inch", and "1.8 inch."

frame

The hardware support structure, covers, and all electrical parts mounted therein that are packaged as one entity for shipping.

freeze

An operation in which a storage system blocks I/O from the host system to the affected volumes on the primary site. A freeze operation stops mirroring between the primary and secondary volumes to ensure data consistency at the secondary site. See also thaw.

FRU

See field-replaceable unit.

FS

See <u>file system</u>.

full restore operation

A copy operation where a local volume is created by reading an entire a volume snapshot from cloud storage.

full snapshot

A type of volume snapshot that contains all the volume data. When a full snapshot is created, an entire copy of the volume data is transmitted to the cloud.

G

General Parallel File System (GPFS)

A high-performance shared-disk file system that can provide data access from nodes in a clustered system environment.

Global Copy

A non-synchronous long-distance copy option for data migration and backup. See also remote mirror and copy.

globally unique identifier (GUID)

An algorithmically determined number that uniquely identifies an entity within a system.

Global Mirror

A method of an asynchronous replication that maintains data consistency across multiple volumes within or across multiple systems. Global Mirror is generally used where distances between the source site and target site cause increased latency beyond what the application can accept.

GPFS

See General Parallel File System.

grain size

The unit size for allocating space on thin-provisioned volumes, such as 32, 64, 128, and 256 kibibyte. The grain size is defined when a volume is created.

GUID

See globally unique identifier.

Н

Hardware Management Console (HMC)

- 1. In a system storage environment, a system that acts as the focal point for configuration, management of Copy Services functions, and maintenance.
- 2. A system that controls managed systems, including the management of logical partitions and use of Capacity Upgrade on Demand. Using service applications, the HMC communicates with managed systems to detect and consolidate information, which can then be sent for analysis.

heat map

An overlay that shows where the user performed actions on a web page. The data is summarized and shown as a colored marker at the location of the user action over a snapshot of the web page. The overlay lets the user see where and how the web page user interacted with the web page.

нмс

See Hardware Management Console.

host

A physical or virtual computer system that hosts computer applications, with the host and the applications using storage. See also client, host, server.

host cluster

A configured set of physical or virtual hosts that share one or more storage volumes in order to increase scalability or availability of computer applications.

host interface card

See interface card.

host object

A logical representation of a host within a storage system that is used to represent the host for configuration tasks.

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. It receives read, write, and update application I/O, depending on the site to which the application is writing.

hot-spare

Pertaining to redundant hardware (such as an adapter, a disk, a drive, or a server) that is installed and available in the event of a hardware failure.

HyperSwap

Pertaining to a function that provides continuous, transparent availability against storage errors and site failures, and is based on synchronous replication.

hypervisor

Software or a physical device that enables multiple instances of operating systems to run simultaneously on the same hardware.

Ι

incremental restore operation

A copy operation where a local volume is modified to match a volume snapshot by reading from cloud storage only the parts of the volume snapshot that differ from the local volume.

incremental snapshot

A type of volume snapshot where the changes to a local volume relative to the volume's previous snapshot are stored on cloud storage.

input/output (I/O)

Pertaining to a device, process, channel, or communication path involved in data input, data output, or both.

interface card

An optional part of a node canister that provides the system with additional host and storage connectivity options.

interface node

A node that connects a system to an Internet Protocol (IP) network for file-serving capabilities by using service protocols.

Internet Small Computer System Interface (iSCSI)

An IP-based standard for linking data storage devices over a network and transferring data by carrying SCSI commands over IP networks. See also Small Computer System Interface.

I/0

See input/output.

I/O enclosure

A hardware unit in a storage system where data is transferred into and out of the system.

iSCSI

See Internet Small Computer System Interface.

journal volume

A volume that holds a consistent copy of data until a new consistent copy is formed. The journal volume restores the last consistent point during a recovery.

Κ

key server

- 1. A server that negotiates the values that determine the characteristics of a dynamic virtual private network (VPN) connection that is established between two endpoints.
- 2. See encryption key server.

L

launch-in-context

An operation in which a user starts a secondary application from a primary application to perform a specific task. Using the parameters, navigation instructions, and user credentials that are supplied by the primary application, the secondary application opens to the specific place in which to complete the task.

licensed capacity

The amount of capacity on a storage system that a user is entitled to configure.

license key

An alphanumeric code that activates a licensed function on a product.

license key file

A file that contains one or more licensed keys.

logical unit number (LUN)

In the Small Computer System Interface (SCSI) standard, a unique identifier used to differentiate devices, each of which is a logical unit (LU).

LUN

See logical unit number.

Μ

machine signature

A string of characters that identifies a system. A machine signature might be required to obtain a license key.

Management Information Base (MIB)

In the Simple Network Management Protocol (SNMP), a database of objects that can be queried or set by a network management system.

management node

A node that is used for configuring, administering, and monitoring a system.

management server

A system that provides a central point of control for managing data replication.

management server relationship

A connection between two replication servers, where one server acts as the active server and replicates the data that is necessary for the standby server to take control of the replication environment.

maximum replication delay

The number of seconds that Metro Mirror or Global Mirror replication can delay a write operation to a volume.

Metro Global Mirror

- A cascaded solution where Metro Mirror synchronously copies data to the target site. This Metro Mirror target is the source volume for Global Mirror that asynchronously copies data to a third site. This solution has the potential to provide a disaster recovery with no data loss at Global Mirror distances when the intermediate site does not participate in the disaster that occurs at the production site.
- 2. A three-site, high availability, disaster recovery solution. Metro Global Mirror uses synchronous replication to mirror data between a local site and an intermediate site, and asynchronous replication to mirror data from an intermediate site to a remote site.

Metro Mirror

A method of synchronous replication that maintains data consistency across multiple volumes within the system. Metro Mirror is generally used when the write latency caused by the distance between the source site and target site is acceptable to application performance.

MIB

See Management Information Base.

Ν

namespace

The scope within which a Common Information Model (CIM) schema applies.

native interface

An interface that is specific to a system or subsystem.

nearline

Pertaining to a type of storage in which data is available in a short amount of time, but not instantly.

nearline SAS drive

A drive that combines the high capacity data storage technology of a Serial Advanced Technology Attachment (SATA) drive with the benefits of a serial-attached SCSI (SAS) interface for improved connectivity.

node

A single processing unit within a system. For redundancy, multiple nodes are typically deployed to make up a system.

0

open system

A system that complies with industry-defined interoperability standards. An open system can be connected to other systems complying with the same standards. See also <u>Fibre Channel Protocol</u>, Small Computer System Interface.

order confirmation code

See authorization code.

overhead capacity

An amount of usable capacity that is occupied by metadata in a system or pool and other data that is used for system operations.

overprovisioned ratio

The ratio of provisioned capacity to usable capacity in a system or pool.

overprovisioning

The result of creating more provisioned capacity in a storage system or pool than there is usable capacity. Overprovisioning occurs when thin provisioning or data reduction techniques ensure that the used capacity of the provisioned volumes is less than their provisioned capacity.

Ρ

parent pool

A storage pool that receives its capacity from MDisks and has, or will have, some of its capacity allocated to child pools. See also child pool.

performance group

A collection of volumes that is assigned the same performance characteristics. See also <u>performance</u> policy.

performance policy

A policy that specifies performance characteristics, for example quality of service (QoS). See also performance group.

PFC

See priority flow control.

ping

- 1. The command that sends an Internet Control Message Protocol (ICMP) echo-request packet to a gateway, router, or host with the expectation of receiving a reply.
- 2. 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

- 1. See storage pool.
- 2. A grouping of storage space that consists of volumes, logical unit numbers (LUNs), or addresses that share a common set of administrative characteristics.

pool pair

Two storage pools that are required to balance workload. Each storage pool is controlled by a separate node.

port

The physical entity within a host, system, or storage system that performs the data communication (transmitting and receiving) over the Fibre Channel.

practice volume

A volume that can be used to test disaster-recovery actions while maintaining disaster-recovery capability.

primary site

A physical or virtual site that is made up of hardware, network, and storage resources. Typically, production operations run at the primary site. Data can be replicated to a secondary site for disaster recovery and failover operations. See also <u>secondary site</u>.

primordial pool

Storage capacity that is unallocated on a storage device. Storage pools are created by allocating storage capacity from primordial pools.

priority flow control (PFC)

A link-level flow control mechanism, IEEE standard 802.1Qbb. PFC operates on individual priorities. Instead of pausing all traffic on a link, PFC is used to selectively pause traffic according to its class.

probe

A data collection job that itemizes and creates an inventory of assets, such as computers, controllers, disk drives, file systems, and logical units.

projected capacity

The estimated volume capacity that is available for volume creation, given the current average performance of any data compression, excluding thin-provisioning savings. See also thin-provisioning savings.

protocol

A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

provisioned capacity

The total capacity of all volumes and volume copies in a system or pool.

R

rack

A free-standing structure that can hold multiple servers, storage systems, chassis, switches, and other devices.

RAID

See Redundant Array of Independent Disks.

RAID 0

A data striping technique, which is commonly called RAID Level 0 or RAID 0 because of its similarity to common, RAID, data-mapping techniques. It includes no data protection, however, so, strictly speaking, the appellation RAID is a misnomer. RAID 0 is also known as data striping.

RAID 1

A form of storage array in which two or more identical copies of data are maintained on separate media.

RAID 10

A collection of two or more physical drives that present to the host an image of one or more drives. In the event of a physical device failure, the data can be read or regenerated from the other drives in the RAID due to data redundancy.

RAID 5

A form of parity RAID in which the disks operate independently, the data stripe size is no smaller than the exported block size, and parity check data is distributed across the array's disks.

RAID 6

A form of RAID that can continue to process read and write requests to all of an array's virtual disks in the presence of two concurrent disk failures.

RAID level

The level of protection provided by the specific techniques of striping, mirroring, or parity used by a Redundant Array of Independent Disks (RAID).

RAID type

See RAID level.

raw capacity

The reported capacity of the drives in the system before formatting or RAID (Redundant Array of Independent Disks) is applied.

rebuild area

Reserved capacity that is distributed across all drives in a redundant array of drives. If a drive in the array fails, the lost array data is systematically restored into the reserved capacity, returning redundancy to the array. The duration of the restoration process is minimized because all drive members simultaneously participate in restoring the data. See also distributed RAID.

reclaimable capacity

The amount of provisioned capacity that can be recovered without causing stress or performance degradation. This capacity identifies the amount of resources that can be reclaimed and provisioned to other objects in an environment.

reclaimed capacity

See reclaimable capacity.

recovery key

See encryption recovery key.

recovery point objective

The maximum amount of data loss that can be tolerated during a service interruption.

Redundant Array of Independent Disks (RAID)

A collection of two or more physical disk drives that present to the host an image of one or more logical disk drives. In the event of a physical device failure, the data can be read or regenerated from the other disk drives in the array due to data redundancy.

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. See also Global Copy.

repo

See repository.

repository (repo)

A persistent storage area for data and other application resources.

reserved capacity

The amount of used capacity that is made up of capacity reserved for system use. See also total usable physical capacity.

resource

In a storage environment, an entity that is monitored. Resources can include fabrics, switches, computers, and storage systems.

role

A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.

role pair

The association of two volume roles in a session that take part in a copy relationship. For example, in a Metro Mirror session, the role pair can be the association between host volumes at the primary site and host volumes at the secondary site (H1-H2).

S

scan

A data collection job that monitors storage usage and file statistics on the resources in an environment.

SCSI

See Small Computer System Interface.

SCSI device

A product, such as a drive or adapter, connected to a host through an I/O interface using the Small Computer System Interface (SCSI) protocol. A SCSI device is either an initiator, target, or both. See also Small Computer System Interface.

SCSI-FCP

See SCSI Fibre Channel Protocol.

SCSI Fibre Channel Protocol (SCSI-FCP)

A standard that defines the protocol used to transfer Small Computer System Interface (SCSI) commands over the transport physical layer of the Fibre-Channel interface. This standard is published by ANSI as X3.269-1996.

SCSI initiator

The system component that initiates communications with attached targets.
SCSI target

A device that acts as a subordinate to a SCSI initiator and consists of a set of one or more logical units (LUs), each with an assigned logical unit number (LUN). The LUs on the SCSI target are typically I/O devices.

secondary site

A physical or virtual site that is made up of the hardware, network, and storage resources that support the recovery needs of the primary site. When a failure occurs at the primary site, operations can continue at the secondary site. See also primary site.

server

A computer program or a device that provides functions for other programs or devices, called clients. See also client, host.

Server Message Block (SMB)

A protocol that manages requests and responses in a client/server environment so that clients on a network can share files, directories, and devices. See also Server Message Block 2.0.

Server Message Block 2.0

A higher performing, more scalable version of Server Message Block (SMB). This protocol can send multiple commands in the same packet and uses larger buffer sizes. See also Server Message Block.

session

A collection of source and target volumes that are managed to create consistent copies of data. The type of data replication that is associated with the session determines the actions that can be conducted for the volumes.

site awareness

The association of a location with each storage system in a session. Site awareness ensures that a volume can only be selected for a session if it matches the location of the site. Site awareness helps to prevent both reversing a hardware relationship and selecting volumes at the wrong location.

Small Computer System Interface (SCSI)

An ANSI-standard electronic interface that allows personal computers to communicate with peripheral hardware, such as disk drives, tape drives, CD-ROM drives, printers, and scanners faster and more flexibly than previous interfaces. See also <u>Internet Small Computer System Interface</u>, <u>open</u> system, SCSI device.

SMB

See Server Message Block.

SMI-S

See Storage Management Initiative Specification.

solid-state drive (SSD)

- 1. A storage device that contains nonvolatile flash memory. A solid-state drive (SSD) has no moving mechanical components.
- 2. See flash drive.

space

See capacity.

space efficient

See thin provisioning.

spare drive

A drive reserved in an array for rebuilding a failed drive in a RAID. Should a drive fail in a RAID, a spare drive from within that device adapter (DA) pair will be selected to rebuild it.

SSD

See <u>solid-state drive</u>.

standard-provisioned volume

A volume that completely uses storage at creation.

standard provisioning

The ability to completely use a volume's capacity for that specific volume.

standby management server

A management server that is a backup for the active server. The replication environment cannot be monitored or managed from the standby server.

storage architecture type (storage type)

The type of storage architecture, either count key data (CKD) or fixed block (FB), for which an array, pool, or volume is provisioned. See also count key data, fixed-block architecture.

storage enclosure

A specialized chassis that is designed to hold and power drives while providing a mechanism to allow them to communicate to one or more separate computers.

Storage Management Initiative Specification (SMI-S)

A design specification developed by the Storage Networking Industry Association (SNIA) that specifies a secure and reliable interface with which storage management systems (SMSs) can identify, classify, monitor, and control physical and logical resources in a storage area network (SAN). The interface integrates the various devices to be managed in a SAN and the tools used to manage them.

storage node

A component of a storage system that provides internal storage or a connection to one or more external storage systems.

storage pod

- 1. A subcomponent of a network-attached storage (NAS) system that consists of two or more storage nodes and one or more supported storage systems.
- 2. A logical entity of components of a system consisting of two storage nodes, and one or two storage subsystems directly connected with these storage nodes.

storage pool (pool)

A collection of storage that identifies an underlying set of resources. These resources provide the capacity and management requirements for a volume or set of volumes.

storage resource group

A named collection of logically related resources that are monitored by Tivoli Storage Productivity Center. Monitored resources can include fabrics, switches, computers, storage systems, and other storage resource groups.

storage system

A system that provides persistent storage within a network. A storage system can include facilities for host attachment, user role authentication, a command-line interface (CLI), a graphical user interface (GUI), and storage devices that most often include Redundant Array of Independent Disks (RAID) controllers. It might also include agents for enabling third-party management software to monitor or manage the storage devices.

storage type

See storage architecture type.

stored capacity

The amount of capacity that is used to store data that is written by a host after data reduction See also data reduction, total usable physical capacity.

support assistance

A function that is used to provide support personnel access to the system to complete troubleshooting and maintenance tasks.

synchronous replication

A type of replication in which the application write operation is made to both the source volume and target volume before control is given back to the application. See also asynchronous replication.

syslog

A standard for transmitting and storing log messages from many sources to a centralized location to enhance system management.

target volume

A volume that receives data from a host volume or another intermediate volume.

thaw

Т

An operation in which a storage system releases the block of the I/O from the host system to the affected volumes on the primary site. A thaw operation can occur after a freeze operation ends and consistency is formed on the secondary site. See also freeze.

thin-provisioned volume

A volume that allocates storage when data is written to it.

thin provisioning

- 1. The ability to defer capacity allocation on a storage resource until data is actually written to it.
- 2. A mechanism that provides the ability to define logical volume sizes that are larger than the physical capacity installed on the system.

thin-provisioning savings

The total amount of usable capacity that is saved in a system, pool, or volume by consuming usable capacity only when needed as a result of write operations. The capacity that is saved is the difference between the provisioned capacity minus the written capacity. See also projected capacity, volume capacity, written capacity.

total capacity savings

The total amount of usable capacity that is saved in a system, pool, or volume through thin provisioning and data reduction techniques. This saved capacity is the difference between the used usable capacity and the provisioned capacity.

total usable physical capacity

The amount of physical configured storage space that is available for stored capacity or reserved capacity. This capacity can consist of both internal storage through arrays and external storage through MDisks. See also capacity threshold, reserved capacity, stored capacity.

track space-efficient volume (TSE volume)

A volume in which storage space is allocated on an as-needed basis by using space on the target volume only when tracks are copied from the source volume to the target volume.

transparent cloud tiering

The functions that use cloud storage as an extension of on-premises storage.

trial license

A temporary entitlement to use a licensed function.

TSE for FlashCopy

A thin-provisioning method in which storage space is allocated from a TSE repository on an as needed basis. See also TSE repository.

TSE repository

The amount of capacity in a storage pool reserved for volumes that use a thin-provisioning method of TSE for FlashCopy. See also <u>TSE for FlashCopy</u>.

TSE volume

See track space-efficient volume.

U

unmapped volume capacity

The amount of volume capacity that is not mapped to a host. See also volume capacity.

update

1. To apply fixes to a system.

- 2. Software maintenance such as a manufacturing refresh, refresh pack, or fix pack that changes the modification level of a product.
- 3. To modify a file or data set with current information.

upgrade

- 1. Any hardware or software change to a later release, or any hardware addition or software addition.
- 2. To install a new version or release of a product to replace an earlier version or release of the same product.

usable capacity

The amount of capacity that is provided for storing data on a system, pool, array, or MDisk after formatting and RAID techniques are applied.

used capacity

The amount of usable capacity that is taken up by data or overhead capacity in a system, pool, array, or MDisk after data reduction techniques have been applied.

user role

An identifier that is assigned to a user that defines the set of permissions that are granted to that user.

V

virtual capacity

See provisioned capacity.

virtualization

The substitution of virtual resources for actual resources, where the virtual resources have the same functions and external interfaces as their counterparts, but differ in attributes, such as size, performance, and cost. Virtualization is commonly applied to physical hardware resources by combining multiple physical resources into shared pools from which users receive virtual resources.

virtualized capacity

The amount of capacity that is contributed to a storage pool by a given provisioning group.

virtual machine (VM)

An emulation of a particular computer system. Virtual machines operate based on the computer architecture and functions of a real or hypothetical computer. Their implementations might involve specialized hardware, software, or a combination of both.

virtual storage area network (VSAN)

A fabric within the storage area network (SAN).

VM

See virtual machine.

volume

A fixed amount of physical or virtual storage on a data storage medium.

volume access set

The set of I/O groups that allows host access to a volume. This set can optionally include the caching I/O group.

volume capacity

The total capacity for all volumes in a system or storage pool. Volume capacity is defined by the client when a volume is created and surfaced to the host. See also <u>thin-provisioning savings</u>, <u>unmapped</u> volume capacity.

volume snapshot

A collection of objects on a cloud storage account that represents the data of a volume at a particular time.

VSAN

See virtual storage area network.

worldwide ID (WWID)

A name identifier that is unique worldwide and that is represented by a 64-bit value that includes the IEEE-assigned organizationally unique identifier (OUI).

worldwide name (WWN)

A 64-bit, unsigned name identifier that is unique.

worldwide node name (WWNN)

A unique 64-bit identifier for a host containing a Fibre Channel port. See also worldwide port name.

worldwide port name (WWPN)

A unique 64-bit identifier associated with a Fibre Channel adapter port. The WWPN is assigned in an implementation-independent and protocol-independent manner. See also worldwide node name.

write-through mode

A process in which data is written to a storage device at the same time as the data is cached.

written capacity

The amount of usable capacity that would have been used to store written data in a system or pool if data reduction was not applied. See also thin-provisioning savings.

written capacity limit

The largest amount of capacity that can be written to a drive, array, or MDisk. The limit can be reached even when usable capacity is still available.

WWID

See worldwide ID.

WWN

See worldwide name.

WWNN

See worldwide node name.

WWPN

See worldwide port name.

Ζ

z Global Mirror

A method of an asynchronous replication function that maintains data consistency across multiple volumes that are attached to a z/OS system. Time-based data consistency is maintained through the Data Facility Storage Management Subsystem (DFSMS) system data mover (SDM) component.

zone

A logical grouping of switches, switch ports, and their attached devices in a fabric.

zone alias

A name that is given to a collection of one or more zone members to be managed together.

zone set

A group of zones that function together on a fabric.

zoning

The grouping of multiple ports to form a virtual, private, storage network. Ports that are members of a zone can communicate with each other, but are isolated from ports in other zones. See also Fibre Channel.

Index

A

about this document ix access Cognos Analytics, configuring 97 accessibility features for IBM Spectrum Control 219 adding installation license 79, 80 adding a computer to a Windows domain 9 agent.sh command syntax 217 agents planning for Storage Resource agents 32 scheduling a Storage Resource agent upgrade 196 starting a Storage Resource agent upgrade 195 uninstalling a Storage Resource agent 212 upgrading Storage Resource agents 195 AIX 208 AIX, Linux 55 alerts migrating 198, 201 Application administrator 12 authentication configuring 202

В

back up migrating <u>105</u> backing up <u>106</u> browsers supported 38

С

changing from LDAP and Local OS authentication 202 to LDAP or Local OS authentication 202 changing the browser language 77 changing the language of Spectrum Control 78 changing the operating system language 77 changing the operating system language for AIX 79 changing the operating system language for Windows 78 CIM agents software requirements 39 commands agent.sh 217 comments, sending ix Common User Db2 user 12 common user, about 17 components 208, 209 configuration guidelines 17 configuring **IBM Cognos Analytics 88** copyingDb2 on Windows

copyingDb2 on Windows (continued) JDBC files 88, 89 copyinglinking Db2 library on Linux and AIX JDBC files 88, 89 creatingIBM Spectrum Control IBM Cognos Analytics data source 91 creatingstarting IBM Cognos Analytics on Linux or AIX content store database 89, 90 creatingstarting IBM Cognos Analytics on Windows content store database 89, 90

D

database repository software requirements 38 Db2 installing on AIX 46 installing on AIX with command line 47 installing on Linux 46 licensing 50 uninstalling 213 upgrading 106 verifying installation 49 verifying installation using CLP 50 verifying installation using First Steps 50 DB2 10.5 to DB2 11.5 106 Db2® installing on Windows 44 preparing to install on UNIX 44 preparing to install on Windows 43 Dell EMC PowerPath Multipathing planning for 31

F

fully qualified host names host names fully qualified host names required <u>1</u> required <u>1</u>

G

glossary <u>227</u> groups migrating 201

Н

hardware requirements <u>37</u> hypervisors user roles 22

I

IBM Cognos Analytics installing in AIX 87

IBM Cognos Analytics (continued) installing in Linux 85 installing in Windows 85 migrating reports 125, 150, 175 upgrading 110, 118, 141, 167 upgrading IBM Spectrum Control 133, 158 IBM Cognos BI reports migrating in Windows 110 migrating, multiple server AIX environment 167 migrating, multiple server AIX environment with remote Jazz for Service Management 175 migrating, multiple server Linux environment 141 migrating, multiple server Linux environment with remote Jazz for Service Management 150 migrating, multiple server Windows environment 118 migrating, multiple server Windows environment with remote Jazz for Service Management 125 migrating, single AIX environment 158 migrating, single Linux environment 133 IBM Spectrum Control hardware requirements 37 installing 12, 39 software requirements 38 uninstalling 205-207 uninstalling the agents 210 IBM Spectrum Control server on a separate computer 69 importingIBM Cognos analytics IBM Spectrum Control pre-defined report package 96 installation program, single-server environment 54, 55 reinstalling 98 silent mode, multiple-server environment 65 silent mode, single-server environment 56 upgrading on a single server AIX or Linux using installation program 185 upgrading on a single server Windows using installation program 184 installation failure deleting registry files 211 installing agents 81 components 37 Db2 44 Db2 on AIX 46 Db2 on Linux 46 Db2[®] on Windows 44 Db2[®], preparing for installation on UNIX 44 Db2[®], preparing for installation on Windows 43 deploying Storage Resource agents remotely 84 GUI 1 **IBM Cognos Analytics 84** IBM Spectrum Control in a Windows domain 8 multiple-server environment 62 new installation 1 on a Windows domain 71 single-server environment 54 starting installation program 51 Storage Resource agents locally 81 Storage Resource agents on the Virtual I/O Server 84 when no X Window System is installed 2 Windows domain Dcdiag tool 73 Windows domain or local 8 with no X Window System 1

installing in a Windows domain creating a Windows domain common user account <u>11</u> Db2 by using a Windows domain user account <u>10</u> granting Db2 SYSADM authority <u>12</u> installing on a Windows domain verify that the Netlogon service is running <u>10</u> installing remote database <u>63</u> installing with command line Db2 on AIX <u>47</u> IPv6 planning for 34

L

```
language
changing for AIX <u>79</u>
changing for the Spectrum Control GUI <u>78</u>
changing for Windows <u>78</u>
LDAP
planning for <u>35</u>
LDAP servers
software requirements <u>39</u>
license
adding <u>79, 80</u>
Linux <u>208</u>
Local OS <u>202</u>
log files
installation error <u>77</u>
```

Μ

migrating alerts <u>198</u>, <u>201</u> groups <u>201</u> multipath subsystem device drivers planning for <u>31</u> upgrading <u>31</u>

0

operating systems supported 38

Ρ

passwords valid characters <u>18</u> planning authorization for users <u>17</u> for Solaris Storage Resource agents <u>33</u> IPv6 support <u>34</u> managing storage <u>36</u> overview <u>1</u> problems report <u>x</u> program installation root, non-root user <u>55</u> single-server environment 54, 55

R

reader feedback, sending \underline{ix} replication $\underline{106}$ reporting

reporting (continued) access configuring for Cognos Analytics software 97 Cognos Analytics configuring access 97 configuring security 97 security configuring for Cognos Analytics software 97 reporting problems <u>x</u> rollup servers user roles 22 root, non-root user 55

S

SAN Volume Controller publications vii security Cognos Analytics, configuring 97 sending comments ix servers removing 212 service ix service management connect ix silent mode installation multiple-server environment 65 single-server environment 56 silent-mode upgrade 187 SMC ix software requirements Data Studio 49 database repository 38 for CIM agents 39 for LDAP servers 39 IBM Data Studio 49 operating systems 38 Storage Resource agent support 38 storage management planning 36 Storage Resource agents deploying remotely 84 installing locally 81 installing on the Virtual I/O Server 84 planning for 32 planning for Solaris 33 protocol support 32 scheduling an upgrade 196 starting an upgrade 195 uninstalling manually 210 uninstalling using GUI 212 upgrading 195 upgrading manually 196 storage systems user roles 22 subsystem device drivers planning for 31 upgrading 31 Sudo command privileges using 36 support ix Support contact x

T

TCP/IP ports planning for 25, 27 Tivoli Storage Productivity Center for Replication uninstalling 205–207 trademarks 225 translations browser locale requirement ix

U

uninstall 208, 209 uninstalling Db2 213 IBM Spectrum Control 205–207 IBM Spectrum Control agents 210 Jazz for Service Management and Tivoli Common Reporting 215 Storage Resource agent manually 210 **Tivoli Storage Productivity Center for Replication** 205-207 upgrading in silent mode 187 multiple-server environment 189 remote DB2 and remote Cognos BI reports 190 scheduling a Storage Resource agent upgrade 196 silent mode 192 single-server environment 184 SMI-S providers for storage systems 197 starting a Storage Resource agent upgrade 195 Storage Resource agents 195 Storage Resource agents manually 196 upgrading from version upgrading by using the installation program 189 user authentication Db2 user names and passwords 21 work sheets 24 user names valid characters 18 user roles hypervisors 22 rollup servers 22 storage systems 22 VMware vSphere data sources 22 using Sudo command privileges 36 usingmultiple remote IBM Spectrum Control databases **IBM Cognos Analytics 95**

W

windows 209 Windows 54



Product Number: 5725-F93, 5725-G33, 5725-Y23, 5725-Y24

SC27-8767-07

