

IBM Tivoli Provisioning Manager V7.1.1: Deployment and IBM Service Management Integration Guide

Learn how to implement Tivoli Provisioning Manager V7.1.1 in your environment

Experiment with IBM Service Management integration scenarios

Learn TPM troubleshooting and how to migrate from V5.1.2 troubleshooting

> Alfredo Olivieri Anna Pintus Annarosa Mallozzi Claudio Santucci Danilo Allocca Fabrizio Salustri Gabriella Santoro GianFilippo Maniscalco

Ghufran Shah Jenna Lau Luca Balestrazzi Michael Edler von der Planitz Raffaela Bove Valentina Mariottini Vasfi Gucer Vittorio Calafiore Wing L Leung

Redbooks

ibm.com/redbooks



International Technical Support Organization

IBM Tivoli Provisioning Manager V7.1.1: Deployment and IBM Service Management Integration Guide

December 2009

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

First Edition (December 2009)

This edition applies to IBM Tivoli Provisioning Manager Version 7, Release 1, Modification 1.

© Copyright International Business Machines Corporation 2009. All rights reserved. Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

	Notices	ii v
	Preface xx The team who wrote this book xx Become a published author xxi Comments welcome xxi	v v ii
Part 1. Concep	ots and architecture	1
	Chapter 1. Tivoli Provisioning Manager V7.1.1 overview 1 1.1 Introduction to Tivoli Provisioning Manager 1 1.1.1 Tivoli Provisioning Manager concepts 1 1.1.2 The data center model (DCM) 1 1.3 Security 10 1.2 What is new in this release 1 1.2.1 Custom attributes 1 1.2.2 Compliance 1 1.2.3 Compliance with Federal Information Processing Standard 140-2 1 1.2.4 Discovery 1 1.2.5 Discovery Library Adapter (DLA) 1 1.2.6 High availability 1 1.2.7 Installation 1 1.2.8 IPv6 addressing 1 1.2.10 Operating systems management 1 1.2.11 Patch Management 1 1.2.12 Reporting 1 1.2.13 Scalable distribution infrastructure (SDI) 1 1.2.14 Security 10 1.2.15 Start Centers 10 1.2.16 Target computers 10 1.2.17 Task management 10 1.2.18 Virtualization 11 1.3 Tivoli Provisioning Manager Version 7.X client value 11	34470122223334445556666677
	Chapter 2. Architecture. 19 2.1 Tivoli process automation engine 20 2.1.1 Common User Interface 21	9 0 2

 2.1.2 Common Configuration Services	23 23 23 23 23 25 25 25 25 25 25 25
 2.2.2 Tivoli Provisioning Manager V7.1.1 component 2.2.3 Tivoli Provisioning Manager V7.1.1 configuration data integrity	architecture 27 for high availability and
Part 2. Planning for deployment and implementation	
3.1 Installation considerations 3.2 Installation requirements 3.3 Installation topologies 3.4 Single node installation 3.5 Multi-node installation 3.6 Reusing existing components 3.7 Considerations for the firewall environment 3.8 Gateway manager and gateway service	
 Chapter 4. Installation steps for integration 4.1 Integration assumptions and rules 4.2 Steps to install and set up the environment to run integration 4.3 Tivoli Provisioning Manager V7.1.1 installation 4.3.1 Pre-install Cygwin on the local system 4.3.2 Base Services install 4.3.3 Tivoli Provisioning Manager core components 4.3.4 Tivoli Provisioning Manager Web components 4.4.1 Installing CCMDB on top of Tivoli Provisioning 4.4.2 Installing Tivoli Service Request Manager on to Manager 7.1.1 	57 58 9 (egration scenarios 59 68 68 70 75 89 92 Manager V7.1.1 92 97
Chapter 5. Customizing Tivoli Provisioning Manager installation 5.1 Customization after Tivoli Provisioning Manager V7. 5.1.1 Security overview 5.1.2 Creating a new user or security group and import Provisioning Manager	V7.1.1 after 101 1.1 installation 102 102 102 103

	5.2 Implementing the scalable distribution infrastructure	107 109
	5.2.2 Device management service	120
	5.3 Tivoli Provisioning Manager: Software deployment and management	121
	5.4 Launching and configuring the Software Package Editor	122
	5.4.1 Requirements	122
	5.4.2 Software Catalog. Software Products and Software Definitions	126
	5.5 Creating and saving a software package block by using SPE	127
	5.5.1 Software product capabilities	130
	5.5.2 Software product requirements	130
	5.6 Distributing software	131
Part 3 The ne	w GIII and IBM Service Management integration scenarios	125
rait 5. mene		100
	Chapter 6. Tivoli process automation engine based user interface	137
	6.1 Start Center configuration for LDAP users	138
	6.2 Start Center templates and instances	138
	6.3 Overview of main functionality in the Start Center	139
	6.4 Configuring the Tivoli process automation engine Web-based interface for	or
	users	143
	6.4.1 Creating new users in LDAP and assign them to groups	144
	6.4.2 Synchronizing Tivoli process automation engine users configuration	with
	LDAP settings	145
	6.4.3 Creating a new Start Center template	147
	6.4.4 Assigning permissions to a security group	149
	6.4.5 Creating a Key Performance Indicator	153
	6.4.6 Modifying a Key Performance Indicator cron task	154
	6.4.7 Choosing which portlets to display in your Start Center instance	155
	6.4.8 Modifying the content of a portlet within your Start Center instance	155
	6.4.9 Modifying an existing Start Center template	156
	6.4.10 Updating your Start Center instance according to the template	157
	6.4.11 Choosing how to display a multi-tabbed Start Center	158
	6.5 Tivoli Provisioning Manager Start Center templates	159
	6.5.1 Provisioning Administrator	159
	6.5.2 Deployment Specialist.	161
	6.5.3 Compliance Analyst	162
	6.5.4 Provisioning Configuration Librarian	164
	6.5.5 Automation Package Developer	165
	6.6 Benefits of the new GUI	166
	6.7 Overview of the GUI differences	167
	6./.1 Welcome to Tivoli Provisioning Manager versus Start Center	168
	6.7.2 Tracking Tasks	170
	6.7.3 Managing Computers	172

	6.7.4 N	Managing Depots	174
	6.7.5 C	Computer Details: Software	176
	6.7.6 V	Workflow Status	178
	6.7.6 V Chapter 7. 7.1 IBM S 7.2 Tivoli I 7.3 Custor 7.3.1 S 7.3.2 C 7.3.2 C 7.3.3 T 7.3.3 T 7.3.4 S	 Workflow Status Integrated Service Management with IBM Service Manage Software. Service Management solutions Provisioning Manager in the context of Service Management. Service provisioning scenario using TADDM, CCMDB, Tivoli Service provisioning scenario using TADDM, CCMDB, Tivoli Service provisioning scenario using Tivoli Provisioning Manager Outage remediation scenario using Tivoli Provisioning Manager Tivoli Service Request Manager. Tivoli Provisioning Manager TADDM Discovery and synchroniza process. Software installation, compliance, and remediation scenario 	178 ement 181 182 183 185 vice 186 and 187 tion 188 188 192
	7.3.5 C	Change scenario using Tivoli Provisioning Manager and Change)
	Ν	Management	193
• • •	Chapter 8. 8.1 Introdu 8.1.1 L 8.1.2 In 8.1.3 T 8.1.4 S 8.2 Discov 8.2.1 C 8.2.2 C 8.3.1 V 8.3.1 V 8.3.2 C 8.3.3 C	B. BM Service Management integration scenarios: TADDM Discovery	195 196 os 196 198 199 201 203 203 204 209 210 213 er 215
9	9.1 Overvi 9.2 Compl 9.2.1 C 9.2.2 E 9.3 The co 9.4 Scena	and remediation with TADDM	nce 217 218 218 219 220 223 225

9.4.1 Scenario introduction	226
9.4.2 Setting up users and permissions	227
9.4.3 Scenario implementation.	231
9.4.4 Scenario conclusion	266
	_
Chapter 10. IBM Service Management integration scenarios: Incide	nt
and ITI	nager 271
10.1 Information Technology Infrastructure Library (ITIL) and Incident	
Management	272
10.1.1 Service considerations	
10.1.2 Incident Management process	
10.2 Tivoli Service Request Manager	274
10.2.1 Overview of Tivoli Service Request Manager	274
10.2.2 Service Desk functionality	274
10.3 Lab environment	276
10.4 Prerequisites steps for integration	277
10.4.1 Posts-installation tasks for Tivoli Change and Configuration	
Management Database	278
10.4.2 Import of Configuration Items from Tivoli Application Depende	ency
Discovery Manager to CMDB	285
10.4.3 Import of Computers from Tivoli Application Dependency Disc	covery
Manager to Tivoli Provisioning Manager Data Center Model	297
10.5 Incident Management integration scenario	300
	300
10.5.2 Creation and configuration of users needed to run the incider	1 001
Management integration scenario	301 opt
Management integration seenario	202
10.5.4. Implementation stops	200
	309
Chapter 11. IBM Service Management integration scenarios: Proble	em and
Change Management integration with Tivoli Service Rec	luest
Manager and CCMDB	325
11.1 Problem and Change Management according to ITIL.	326
11.1.1 IBM Tivoli Change and Configuration Management Database	
(CCMDB)	326
11.1.2 Change Management	326
	328
11.2 Scenario process now	
11.2.1 Users of the scenario	330
11.2.2 Users and groups as delined in webophere	33U
11.3.1 From Service Request to Incident	 222
	000

	11.3.2 From Incident record to Problem and Change record 11.3.3 From Change to software patch deployment	336 341
	Chapter 12. Tivoli Provisioning Manager integration methods with non-	IBM
	Solutions	347
	12.2 Functional integration	349
	12.2 1 Advantages and disadvantages of functional integration	251
	12.2.1 Auvantages and disadvantages of functional integration	252
	12.2.2 Tiveli Provisioning Manager Web Services SOAP Services and	352
	12.2.3 Tivoli Provisioning Manager web Services, SOAP Services, and	250
	10.0.4 Eunstianal integration summary	309
	12.2.4 Functional integration summary	201
	12.3 Data Integration	302
	12.3.1 Auvantages and disadvantages of data integration	262
	12.3.2 The Free Provisioning Manager data importing/exporting capabilities	303
	12.3.3 IDM Tivoli Integration Composer (ITIC)	303
	12.3.4 Data integration	202
	12.4 Data reversion	267
	12.4.2 IBM InfoSphere Enderation Sonver	267
		307
Part 4. Patch M	anagement, Operating System Deployment, and IBM Tivoli Monitoring	
agenti	or Tivoli Provisioning Manager	369
agent	or Tivoli Provisioning Manager	369 371
agent	or Tivoli Provisioning Manager	369 371 nt
agent i	or Tivoli Provisioning Manager Chapter 13. Patch Management scenarios 13.1 Changes and improvements to Windows and UNIX Patch Managemen capabilities	369 371 nt 372
agent i	Or Tivoli Provisioning Manager Chapter 13. Patch Management scenarios 13.1 Changes and improvements to Windows and UNIX Patch Management capabilities 13.2 Patch Management in small Windows environments	369 371 nt 372 372
agent f	 or Tivoli Provisioning Manager Chapter 13. Patch Management scenarios 13.1 Changes and improvements to Windows and UNIX Patch Managemen capabilities 13.2 Patch Management in small Windows environments	369 371 nt 372 372 374
agent	 Chapter 13. Patch Management scenarios 13.1 Changes and improvements to Windows and UNIX Patch Management capabilities 13.2 Patch Management in small Windows environments 13.2.1 Predefined roles for Patch Management 13.2.2 Requirements for Patch Management 	369 371 nt 372 372 374 374
agent	 Chapter 13. Patch Management scenarios 13.1 Changes and improvements to Windows and UNIX Patch Management capabilities 13.2 Patch Management in small Windows environments 13.2.1 Predefined roles for Patch Management 13.2.2 Requirements for Patch Management 13.2.3 Web Replay scenarios 	369 371 nt 372 372 374 374 375
agent	 Chapter 13. Patch Management scenarios 13.1 Changes and improvements to Windows and UNIX Patch Managemer capabilities 13.2 Patch Management in small Windows environments 13.2.1 Predefined roles for Patch Management 13.2.2 Requirements for Patch Management 13.2.3 Web Replay scenarios 13.2.4 Patch Management in small Windows environments 	369 371 nt 372 372 374 374 374 375 376
agent	 Chapter 13. Patch Management scenarios 13.1 Changes and improvements to Windows and UNIX Patch Management capabilities 13.2 Patch Management in small Windows environments 13.2.1 Predefined roles for Patch Management 13.2.2 Requirements for Patch Management 13.2.3 Web Replay scenarios 13.2.4 Patch Management in small Windows environments 13.2.5 Patch Management in large Windows environments 	369 371 nt 372 372 374 374 374 375 376 380
agent	 Chapter 13. Patch Management scenarios 13.1 Changes and improvements to Windows and UNIX Patch Management capabilities 13.2 Patch Management in small Windows environments 13.2.1 Predefined roles for Patch Management 13.2.2 Requirements for Patch Management 13.2.3 Web Replay scenarios 13.2.4 Patch Management in small Windows environments 13.2.5 Patch Management in large Windows environments 	369 371 1t 372 372 374 374 375 376 380 396
agent	 Chapter 13. Patch Management scenarios 13.1 Changes and improvements to Windows and UNIX Patch Management capabilities 13.2 Patch Management in small Windows environments 13.2.1 Predefined roles for Patch Management 13.2.2 Requirements for Patch Management 13.2.3 Web Replay scenarios 13.2.4 Patch Management in small Windows environments 13.2.5 Patch Management in large Windows environments 13.3 Patch Management in AIX environments 13.3.1 Acquiring patches 	369 371 1t 372 372 374 374 375 376 380 396 399
agent	 Chapter 13. Patch Management scenarios 13.1 Changes and improvements to Windows and UNIX Patch Management capabilities 13.2 Patch Management in small Windows environments 13.2.1 Predefined roles for Patch Management 13.2.2 Requirements for Patch Management 13.2.3 Web Replay scenarios 13.2.4 Patch Management in small Windows environments 13.2.5 Patch Management in large Windows environments 13.3 Patch Management in AIX environments 13.3.1 Acquiring patches 13.3.2 Setting up compliance 	369 371 372 372 374 374 375 376 380 396 399 400
agent	 Chapter 13. Patch Management scenarios 13.1 Changes and improvements to Windows and UNIX Patch Management capabilities 13.2 Patch Management in small Windows environments 13.2.1 Predefined roles for Patch Management 13.2.2 Requirements for Patch Management 13.2.3 Web Replay scenarios 13.2.4 Patch Management in small Windows environments 13.2.5 Patch Management in large Windows environments 13.3 Patch Management in AIX environments 13.3.1 Acquiring patches 13.3.3 Scanning for missing patches 	369 371 1 372 372 374 374 374 375 376 380 396 399 400 401
agent	 Chapter 13. Patch Management scenarios 13.1 Changes and improvements to Windows and UNIX Patch Management capabilities 13.2 Patch Management in small Windows environments 13.2.1 Predefined roles for Patch Management 13.2.2 Requirements for Patch Management 13.2.3 Web Replay scenarios 13.2.4 Patch Management in small Windows environments 13.2.5 Patch Management in large Windows environments 13.3 Patch Management in AIX environments 13.3.1 Acquiring patches 13.3.2 Setting up compliance 13.3.4 Approving compliance recommendations 	369 371 372 372 374 374 375 376 380 396 399 400 401 401
agent	 Chapter 13. Patch Management scenarios 13.1 Changes and improvements to Windows and UNIX Patch Management capabilities 13.2 Patch Management in small Windows environments 13.2.1 Predefined roles for Patch Management 13.2.2 Requirements for Patch Management 13.2.3 Web Replay scenarios 13.2.4 Patch Management in small Windows environments 13.2.5 Patch Management in large Windows environments 13.3 Patch Management in AIX environments 13.3.1 Acquiring patches 13.3.3 Scanning for missing patches 13.3.4 Approving compliance recommendations 13.3.5 Distributing patches 	369 371 1 372 372 374 374 374 375 376 380 396 399 400 401 401 402
agent	 Chapter 13. Patch Management scenarios 13.1 Changes and improvements to Windows and UNIX Patch Management capabilities 13.2 Patch Management in small Windows environments 13.2.1 Predefined roles for Patch Management 13.2.2 Requirements for Patch Management 13.2.3 Web Replay scenarios 13.2.4 Patch Management in small Windows environments 13.2.5 Patch Management in large Windows environments 13.3 Patch Management in AIX environments 13.3.1 Acquiring patches 13.3.3 Scanning for missing patches 13.3.4 Approving compliance recommendations 13.3.5 Distributing patches 13.3.6 Installing patches 	369 371 1 372 372 374 374 374 375 376 380 396 399 400 401 401 402 402
agent i	 Chapter 13. Patch Management scenarios 13.1 Changes and improvements to Windows and UNIX Patch Management capabilities 13.2 Patch Management in small Windows environments 13.2.1 Predefined roles for Patch Management 13.2.2 Requirements for Patch Management 13.2.3 Web Replay scenarios 13.2.4 Patch Management in small Windows environments 13.2.5 Patch Management in large Windows environments 13.3.1 Acquiring patches 13.3.2 Setting up compliance 13.3.4 Approving compliance recommendations 13.3.5 Distributing patches 13.3.6 Installing patches 13.3.7 Verifying compliance results 	369 371 1 372 372 374 374 374 375 376 380 396 399 400 401 401 402 402 403
agent i	 Chapter 13. Patch Management scenarios 13.1 Changes and improvements to Windows and UNIX Patch Management capabilities 13.2 Patch Management in small Windows environments 13.2.1 Predefined roles for Patch Management 13.2.2 Requirements for Patch Management 13.2.3 Web Replay scenarios 13.2.4 Patch Management in small Windows environments 13.2.5 Patch Management in large Windows environments 13.3 Patch Management in AIX environments 13.3.1 Acquiring patches 13.3.2 Setting up compliance 13.3.4 Approving compliance recommendations 13.3.5 Distributing patches 13.3.6 Installing patches 13.3.7 Verifying compliance results 13.3.8 Uninstalling patches 	369 371 1 372 372 374 374 375 376 380 399 400 401 401 402 402 403 403
agent i	Chapter 13. Patch Management scenarios 13.1 Changes and improvements to Windows and UNIX Patch Management capabilities 13.2 Patch Management in small Windows environments 13.2.1 Predefined roles for Patch Management 13.2.2 Requirements for Patch Management 13.2.3 Web Replay scenarios 13.2.4 Patch Management in small Windows environments 13.2.5 Patch Management in small Windows environments 13.2.6 Patch Management in small Windows environments 13.3.1 Acquiring patches 13.3.2 Setting up compliance 13.3.3 Scanning for missing patches 13.3.4 Approving compliance recommendations 13.3.5 Distributing patches 13.3.7 Verifying compliance results 13.3.8 Uninstalling patches 13.3.4 Patch Management in SUSE Linux Enterprise environments	369 371 1 372 372 374 374 375 376 380 396 399 400 401 401 402 402 403 403 404

	13.4.2 SUSE Linux update site model	406
	Chapter 14. Operating system provisioning. 14.1 Tivoli Provisioning Manager for OS Deployment architecture. 14.1.1 Product components. 14.1.2 DHCP configuration 14.1.3 Deployment basics 14.2 Parent-child boot servers 14.3 Software modules 14.3.1 Windows platforms 14.3.2 Linux 14.3.3 AIX 14.3.4 Solaris 14.3.5 Tivoli common agent software modules 14.3.6 Bindings 14.4 Hardware configuration 14.5.1 Windows 14.5.2 Linux 14.5.3 AIX, solaris, and Linux on PPC 14.5.4 Golden master image 14.5.2 Diving computers	409 411 413 415 423 426 451 451 451 452 454 469 469 483 487 489 490
	Chapter 15. The IBM Tivoli Monitoring Agent for Tivoli Provisioning Manager 15.1 IBM Tivoli monitoring agent software 15.1.1 Features and functions of the monitoring agent 15.1.2 Configuring the agent 15.3 Predefined workspaces 15.4 Sample workspaces data	497 498 498 498 502 503 503
Trouble	eshooting and migration from Tivoli Provisioning Manager V5.1.2	509
	Chapter 16. Troubleshooting 16.1 Troubleshooting basics 16.1.1 What are the symptoms of the problem? 16.1.2 Where does the problem occur? 16.1.3 When does the problem occur? 16.1.4 Under which conditions does the problem occur? 16.1.5 Can the problem be reproduced? 16.2 Installation troubleshooting 16.2.1 Troubleshooting the provisioning server	511 513 513 513 514 514 515 515 515

Part 5.

16.2.2 Tivoli Provisioning Manager core components	517
16.2.3 Tivoli Provisioning Manager Web components	517
16.2.4 Tivoli Provisioning Manager installation logs	. 518
16.2.5 Troubleshooting the infrastructure components installation	. 519
16.3 Runtime troubleshooting	520
16.3.1 Configuring logging levels	520
16.3.2 Setting logging levels	521
16.4 Collecting logs from Tivoli Provisioning Manager server	523
16.5 Displaying and exporting provisioning workflow logs	524
16.6 Verifying if the Tivoli Common Agent is working	526
16.7 Setting up the Tivoli common agent log levels	527
16.8 Collecting a log file from the Tivoli common agent	528
16.9 Verifying if the depot has been successfully installed	529
16.10 Collecting a log file from the depot server	531
16.11 Troubleshooting the software distribution	531
16.11.1 Debugging the software distribution in a scalable distribution	
infrastructure (SDI)	531
16.11.2 Debugging the software distribution in a deployment engine	
infrastructure	536
16.12 Troubleshooting operating system provisioning	540
·····	
Chapter 17. Migrating from Tivoli Provisioning Manager Version 5.1.1.	2 to
Tivoli Provisioning Manager Version 7.1.1	541
17.1 Migration objectives	. 543
17.1.1 Gradual phased migration process approach	543
17.1.2 Artifacts migration	544
17.2 Environment used for the migration	. 545
17.2.1 Tivoli Provisioning Manager Version 5.1.1.2 system	. 546
17.2.2 Tivoli Provisioning Manager Version 7.1.1 system	547
17.3 Migration overview	. 548
17.4 Tivoli Provisioning Manager Version 5.1.1.2 pre-migration tasks	. 550
17.4.1 Upgrading the provisioning server to version 5.1.1.2	551
17.4.1 Upgrading the provisioning server to version 5.1.1.2	. 551 . 552
 17.4.1 Upgrading the provisioning server to version 5.1.1.2 17.4.2 Upgrading the common agent to version 1.3.2.29 17.4.3 Copying the files for the scalable distribution infrastructure (SDI) 	. 551 . 552
 17.4.1 Upgrading the provisioning server to version 5.1.1.2 17.4.2 Upgrading the common agent to version 1.3.2.29 17.4.3 Copying the files for the scalable distribution infrastructure (SDI) installation 	551 552 552
 17.4.1 Upgrading the provisioning server to version 5.1.1.2 17.4.2 Upgrading the common agent to version 1.3.2.29 17.4.3 Copying the files for the scalable distribution infrastructure (SDI) installation 17.4.4 Copying the backup tools to the 5.1.1.2 provisioning server 	. 551 . 552 . 552 . 553
 17.4.1 Upgrading the provisioning server to version 5.1.1.2 17.4.2 Upgrading the common agent to version 1.3.2.29 17.4.3 Copying the files for the scalable distribution infrastructure (SDI) installation 17.4.4 Copying the backup tools to the 5.1.1.2 provisioning server 17.4.5 Backing up the LDAP server 	. 551 . 552 . 552 . 553 . 554
 17.4.1 Upgrading the provisioning server to version 5.1.1.2 17.4.2 Upgrading the common agent to version 1.3.2.29 17.4.3 Copying the files for the scalable distribution infrastructure (SDI) installation 17.4.4 Copying the backup tools to the 5.1.1.2 provisioning server 17.4.5 Backing up the LDAP server 17.4.6 Pre-migration tasks for Tivoli Directory Server 	551 552 552 553 553 554 554
 17.4.1 Upgrading the provisioning server to version 5.1.1.2 17.4.2 Upgrading the common agent to version 1.3.2.29 17.4.3 Copying the files for the scalable distribution infrastructure (SDI) installation 17.4.4 Copying the backup tools to the 5.1.1.2 provisioning server 17.4.5 Backing up the LDAP server 17.4.6 Pre-migration tasks for Tivoli Directory Server 17.4.7 Prerequisites for migrating automation packages 	. 551 . 552 . 552 . 553 . 554 . 554 . 555
 17.4.1 Upgrading the provisioning server to version 5.1.1.2 17.4.2 Upgrading the common agent to version 1.3.2.29 17.4.3 Copying the files for the scalable distribution infrastructure (SDI) installation 17.4.4 Copying the backup tools to the 5.1.1.2 provisioning server 17.4.5 Backing up the LDAP server 17.4.6 Pre-migration tasks for Tivoli Directory Server 17.4.7 Prerequisites for migrating automation packages 17.4.8 Exporting the 5.1.1.2 report query 	. 551 . 552 . 552 . 553 . 554 . 554 . 555 . 556
 17.4.1 Upgrading the provisioning server to version 5.1.1.2 17.4.2 Upgrading the common agent to version 1.3.2.29 17.4.3 Copying the files for the scalable distribution infrastructure (SDI) installation 17.4.4 Copying the backup tools to the 5.1.1.2 provisioning server 17.4.5 Backing up the LDAP server 17.4.6 Pre-migration tasks for Tivoli Directory Server 17.4.7 Prerequisites for migrating automation packages 17.4.8 Exporting the 5.1.1.2 report query 17.4.9 Migrating file repositories 	. 551 . 552 . 552 . 553 . 554 . 554 . 555 . 556 . 556
 17.4.1 Upgrading the provisioning server to version 5.1.1.2 17.4.2 Upgrading the common agent to version 1.3.2.29 17.4.3 Copying the files for the scalable distribution infrastructure (SDI) installation 17.4.4 Copying the backup tools to the 5.1.1.2 provisioning server 17.4.5 Backing up the LDAP server 17.4.6 Pre-migration tasks for Tivoli Directory Server 17.4.7 Prerequisites for migrating automation packages 17.4.8 Exporting the 5.1.1.2 report query 17.4.9 Migrating file repositories 17.4.10 Migrating images created using Tivoli Provisioning for OS 	. 551 . 552 . 552 . 553 . 554 . 554 . 555 . 556 . 556
 17.4.1 Upgrading the provisioning server to version 5.1.1.2 17.4.2 Upgrading the common agent to version 1.3.2.29 17.4.3 Copying the files for the scalable distribution infrastructure (SDI) installation 17.4.4 Copying the backup tools to the 5.1.1.2 provisioning server 17.4.5 Backing up the LDAP server 17.4.6 Pre-migration tasks for Tivoli Directory Server 17.4.7 Prerequisites for migrating automation packages 17.4.8 Exporting the 5.1.1.2 report query 17.4.9 Migrating file repositories 17.4.10 Migrating images created using Tivoli Provisioning for OS Deployment. 	. 551 . 552 . 552 . 553 . 554 . 554 . 555 . 556 . 556 . 556

17.4.11 Removing nicknames and views	557
17.5 Tivoli Provisioning Manager Version 7.1.1 pre-installation tasks	558
17.6 Tivoli Provisioning Manager Version 7.1.1 installation	559
17.6.1 Starting the launchpad	559
17.6.2 Installing the middleware	560
17.6.3 Creating the database and database server user	565
17.6.4 Core components installation	567
17.7 Completing the property file	5//
17.8 Migrating Livoli Provisioning Manager	591
17.8.1 Migration tasks for the Tivoli Provisioning Manager Version 5.1.1.	2
17.9.0 Migration tasks for the Tiveli Drevisioning Manager Version 7.1.1	591
17.6.2 Migration tasks for the Tivon Provisioning Manager Version 7.1.1	506
17.9.2 Changing the WebSphere Application Server assprofile profile	590
naceword	616
17.8.4 Installing the base services and the Web components	616
17.8.5 Assigning the bostnames	625
17.8.6 Continuing the migration on the 7.1.1 provisioning server	638
17.9 Post-migration tasks	655
17.9.1 Backing up the administrative workstation	656
17.9.2 Configuring SSL with IBM HTTP Server	657
······	
Appendix A. Miscellaneous upgrade scenarios	671
Upgrade to Tivoli Provisioning Manager V7.1.1 and Tivoli CCMDB V7.1.1.5	672
Upgrade to Tivoli Provisioning Manager V7.1.1 and Tivoli Service Request	
Manager V7.1.0.4	674
Integration between Tivoli Provisioning Manager V7.1.1 and IBM Tivoli Asset	t
Management for IT V7.1.0.5.	678
Installing Tivoli Asset Management for TL on top of Tivoli Provisioning Mana	ager
V/.1.1	6/8
Installing Tivoli Provisioning Manager on top of Tivoli Asset Management	tor
11 V/.1.0.5	080
Appendix B. Tivoli Provisioning Manager Version 7.1.1 pre-installation	
checks	685
File systems creation	686
Required packages	688
openssl and openssh	690
Operating System checks	692
Environment checks	695
Prepare the installation media	697
Appendix C. tpm5112backup.sh script	699
трть і і и раскир.sn script	700

Appendix D. Additional material Locating the Web material Using the Web material System requirements for downloading the Web material How to use the Web material	711 711 712 712 712 712
Abbreviations and acronyms	713
Related publications IBM Redbooks Online resources How to get Redbooks Help from IBM	717 717 717 719 719
Index	721

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give 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.

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.

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.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX 5L™	Maximo®
AIX®	MVS™
AS/400®	Netcool®
DB2 Universal Database™	Netfinity®
DB2®	NetView®
Enterprise Asset Management®	OS/2®
IBM®	PowerPC®
InfoSphere™	Redbooks®
iSeries®	Redbooks (logo) 🧬 🛽
Library Reader™	Roma®

ServerGuide™ System p™ System z™ SystemView® Tivoli Enterprise Console® Tivoli® TotalStorage® WebSphere®

The following terms are trademarks of other companies:

AMD, the AMD Arrow logo, and combinations thereof, are trademarks of Advanced Micro Devices, Inc.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

Snapshot, and the NetApp logo are trademarks or registered trademarks of NetApp, Inc. in the U.S. and other countries.

Novell, SUSE, the Novell logo, and the N logo are registered trademarks of Novell, Inc. in the United States and other countries.

Oracle, JD Edwards, PeopleSoft, Siebel, and TopLink are registered trademarks of Oracle Corporation and/or its affiliates.

SAP, and SAP logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries.

Java, Java runtime environment, JDBC, JRE, JumpStart, SmartStart, Solaris, Sun, Sun Java, Ultra, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Active Directory, BitLocker, Internet Explorer, Microsoft, Visual Basic, Windows Server, Windows Vista, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Itanium, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Preface

This IBM® Redbooks® publication is a complete reference for the recently available Tivoli® Provisioning Manager V7.1.1 product. This document provides information valuable to those who want to plan for, customize, and use the IBM Tivoli Provisioning Manager V7.1.1 product to automate and manage IT provisioning and integrated IT service management processes in their environments. It includes five parts:

- Concepts and architecture: Provides an overview of provisioning concepts and introduces Tivoli Provisioning Manager V7.1.1 concepts and architecture, in perspective with the overall Tivoli process automation engine platform.
- Planning for deployment and implementation: Discusses planning considerations for deploying Tivoli Provisioning Manager V7.1.1 in a production environment, installation and initial customization of product components, and a sample software deployment scenario to verify the successful deployment of the product.
- The new GUI and IBM Service Management integration scenarios: Covers value added integration scenarios with several IBM Service Management products such as IBM Tivoli Application Dependency Discovery Manager, IBM Tivoli Service Request Manager, and IBM Tivoli Change and Configuration Management Database. Also included is a section explaining the Start Center based new GUI, and a section on implementing Tivoli Provisioning Manager V7.1.1 with a non-IBM configuration management database.
- Patch Management, Operating System Deployment, and IBM Tivoli Monitoring Agent for Tivoli Provisioning Manager: Introduces several scenarios on Patch Management and Operating System Deployment, focusing on the new features. Also provided is an overview of the IBM Tivoli Monitoring Agent for Tivoli Provisioning Manager.
- Troubleshooting and migration from Tivoli Provisioning Manager V 5.1.2: Provides some tips for troubleshooting Tivoli Provisioning Manager V 7.1.1 installation and operation and discusses a migration scenario from Tivoli Provisioning Manager V 5.1.2.

The team who wrote this book

This book was produced by a team of specialists from around the world working at the Tivoli Rome Lab in Italy.



Alfredo Olivieri is an IT Architect working in Software Group Services in Italy. He holds a degree in Electronic Engineering and is ITIL® v3 certified. He has ten years experience in IT, nine of which have been spent in IBM. Throughout his career, he has been involved in the design and the implementation of several projects in the availability and automation areas of the Tivoli portfolio for clients all over Europe. His experience includes Netcool® and IBM Service Management family products. At present he is working as an IT Architect on CCMDB and TBSM projects in Italy.



Anna Pintus is a Tivoli Technical Consultant working for IBM Software Group Tivoli Lab Services, in Italy. She is an Open Group Master Certified IT Specialist. Anna accumulated more than 15 years of experience in Information Technology working across Network and Systems Management areas. Throughout her career she has been involved in several large-scale Tivoli projects for important customers located in Italy and EMEA and she gained extensive experience with many Tivoli products and solutions.

Her current interests are in the Provisioning and Service Management areas. Before joining the Tivoli Lab Services she worked for five years in the L2 Customer Support team as technical leader for the PAN-EMEA Tivoli Framework escalation team. In the past she spent some years in the Rome Tivoli Lab Verification team working on different technologies and applications (NetView DM, SystemView, TME10 NetFinity, Tivoli Configuration Manager). She holds a degree in Engineering and she is SOA and ITIL v3 certified. She has also received some Deployment Professional Certifications in the Tivoli Provisioning Manager area.



Annarosa Mallozzi is a Certified IT Specialist (Systems Management) working in the IBM L2 Customer Support organization. She has 11 years experience in IT, eight of which were in IBM. She is a DB2 Associate Certified, ITIL Service Management Foundation Certified and Deployment Professional Tivoli Data Warehouse Certified.

Throughout her career, she gained a wide experience with different platforms, RDBMSs and IBM products. She worked as a Services Consultant in the mainframe area (CICS, IMS, DB2), developed application monitoring solutions on UNIX based on shell scripting, built data analysis procedures in PL*SQL (Oracle). acquired a significant experience with MQSeries installation and configuration on Windows, DB2 Data Warehouse solutions, DB2 installation and configuration. She has been involved in several projects for important world wide customers with different Tivoli products in the provisioning area (Tivoli Configuration Manager, Tivoli Provisioning Manager for OS Deployment, Tivoli Data Warehouse and Tivoli License Manager). She teaches IBM methods applied to projects and for method tailoring tools such as Rational Method Composer.



Claudio Santucci is a Software Support Specialist working for Italy in Tivoli Customer Support within IBM Global Services. He has worked for IBM since 1996, and has extensive experience with the AS/400® SW Platform. Before joining the Tivoli Support team, he worked as a certified iSeries® IT Specialist and has joined multiple projects to implement AS/400 solutions for clients of IBM Italy. He also worked for several years in iSeries Customer support. In March 2007, he joined the Tivoli Customer Support within IBM Global Service.



Danilo Allocca has been working for IBM since 2004. He worked on development and testing for the IBM Tivoli License Manager product. In the past year, he has been working in the Support Area (G.R.T. Global Response Team) for S.P.A. products.



Fabrizio Salustri is a Software Support Specialist working for Italy IMT in Tivoli Customer Support within IBM Global Services. He worked for IBM since 1996, and has extensive experience with Tivoli products suite. Throughout his career, Fabrizio has been involved in several projects implementing Tivoli solutions for important clients of IBM Italy. Before joining the Tivoli Support team, he worked as a Certified AIX® System Administrator in AIX Technical Support. In March 2005 he got an IBM Tivoli Monitoring 5.1.1 Deployment Professional Certification and in April 2006, an IBM Tivoli Monitoring 6.1 Deployment Professional Certification.



Gabriella Santoro started working for IBM in 1990 at the IBM Software Laboratory in Rome. During these years she built a broad and valuable knowledge with experience on both IBM (Tivoli) Systems Management products, and the software development life cycle, starting from requirements collection and prioritization, as EMEA Product Manager, until post sale implementation at the Customer site, as Tivoli Services Project Manager. Her main involvement has been in the Quality Assurance area, testing systems management products across different life cycle phases. In 2008 she received the IBM Tivoli Workload Scheduler V8.3 Deployment Professional Certification.

These are the products she has worked on: Tivoli Provisioning Manager, Tivoli Workload Scheduler, IBM Tivoli Monitoring, Tivoli Enterprise Console®, Tivoli Business Systems Manager, Tivoli Inventory, Tivoli Software Distribution, Tivoli Framework, Tivoli Remote Control, Tivoli NetView, Telecommunications Manager Network for AIX, OSI/X.400, OSI/6000 X.400 and NetView Distribution Manager for OS/2®.



GianFilippo Maniscalco is a Software Support Specialist working in Rome in Tivoli Customer Support within Tivoli Lab. He holds a degree in Electronic Engineering in 1996. He has worked for IBM since 2000 and has extensive experience in IT (Build/Packaging Specialist and UNIX System Administrator) and customer support, mainly on Tivoli products such as Tivoli onfiguration Manager, Tivoli Provisioning Manager Express, and Tivoli Provisioning Manager. In December 2007 he received the ITIL v.3 certification and in January 2008 he received the Certified Tivoli Provisioning Manager V5.1 and Tivoli Provisioning Manager Express V4.1 for Software Distribution Deployment Professional certification.



Ghufran Shah is an IBM Certified Advanced Deployment Professional in Enterprise, Provisioning, and Business Application Management Solutions. He has 15 years of experience in Systems Development and Enterprise Systems Management and holds a degree in Computer Science. His areas of expertise include Tivoli Systems Management Architecture, Implementation, and Tivoli Training, together with Business Process Improvement. He has written extensively about Event Management, Monitoring, and Business Systems Management integration and has taught IBM Tivoli. courses worldwide. He is currently at TeamSwift Solutions, a trusted advisor for IT Service Management Solutions with a focus on Automation, Service Provisioning, Monitoring, and Virtualization.



Jenna Lau is an IBM Software Developer at the IBM Toronto Lab. She has been with IBM Canada since 2006, and has worked in automation package development, test automation, and various other test phases for Tivoli Provisioning Manager V5.1 through V7.1.1. Prior to IBM, she attended York University where she completed a double major in Computer Science and Creative Writing.



Luca Balestrazzi is a Certified IBM IT Architect in Global Technology Services in Italy. He has five years of experience in the RNSL Rome Laboratory in service support, two years of experience in service support for SystemView and Netfinity® products, and 10 years of experience with Tivoli Area of Network and Systems Management products. He also has experience with IBM Service Management family products. He has a degree in Economics and is ITIL v3 certified. Luca is working as a Delivery IT Architect on Change and Configuration Management Database (CCMDB) Projects in Italy.



Michael Edler von der Planitz is an IBM IT Specialist working for IBM Tivoli Support in Germany. He worked in IBM and the formerly subsidiary company IT Services and Solutions GmbH since 1995. Michael has extensive experiences with the System Management portfolio of Tivoli products such as Tivoli Framework and Tivoli Configuration Manager. For this he was involved in several projects implementing Tivoli System Management solutions for clients in Germany beside his work in Tivoli Support team Germany. He is also a member of the Virtual Front-End for Tivoli Provisioning Manager, a European team providing extended skills for Tivoli Provisioning Manager support. Before joining IBM Tivoli support, he worked in the banking area and telecommunication sector and was involved in national and international projects implementing and developing IBM products. In 2005 he got a Certified Deployment Professional for IBM Tivoli Configuration Manager 4.2.



Raffaela Bove is a Software Support Specialist at the IBM Maintenance & Technology Service in Italy. She joined IBM in 1998 and has extensive experience with the Tivoli products suite. Throughout her career, Raffaela has been involved in several projects implementing Tivoli solutions for Italy important customers. She is a certified Tivoli Storage Manager specialist. Since 2007, she is the Team Leader of the Tivoli Provisioning Manager Virtual Front-end.



Valentina Mariottini joined IBM in 1998 and started to work for as an IT Specialist on AIX, gaining knowledge and experience on various products and IT environments. Since 2004, she has been working for the Italy Tivoli Technical support as Front-End.



Vasfi Gucer is a project leader at the ITSO Austin/TX. He has more than 15 years of experience in Systems Development and Enterprise Systems Management. He writes extensively and teaches IBM classes worldwide on Tivoli software. Vasfi is also an IBM Certified Senior IT Specialist, PMP, and ITIL Expert.



Vittorio Calafiore is a Software Support Specialist working in Rome in Tivoli Customer Support within Tivoli Lab. He holds a degree in Electronic Engineering in 1997. He has worked for IBM since 2000 and has extensive experience in test, development, and customer support, mainly on Tivoli products such as License Management and Provisioning. In November 2007 he received the ITIL v.3 certification. In June 2008 he received the Certified Tivoli Provisioning Manager V5.1 Deployment Professional certification.



Wing L Leung is a Senior Process Automation Specialist working in the ISST ATG SWAT team. He has over 10 years of experience with IBM working on various teams ranging from OS2 development, IBM Global Services (IGS) consulting, Tivoli development, ATG Security and Provisioning SWAT teams. He is ITIL certified and currently enjoys his role where he supports potential customers world wide in better understanding, evaluating, and utilizing IBM Service Management solutions.

Thanks to the following people for their contributions to this project:

Wade Wallace International Technical Support Organization, Austin Center

Yvonne Lyon International Technical Support Organization, San Jose Center Sarvi Aryanpour, Linda Burn, Pablo Caceres, Paul Chen, Andrew Kaye-Cheveldayoff, Dragan Damnjanovic, Andrew Edgar, Tesshu Flower, Daniela Grigoriu, Yang Han, Juliana Hsu, Andreea Jurj, Partha Kaushik, Cindy Lee, Kimberly Mungal, Wing Lee, Mark Leitch, Michael Li, Lewis Lo, Jeffrey Luo, Jeff McRae, Mike Ng, Vincenzo Pasquantonio, Eugen Postea, Delia Rusu, Duke Shih, Amy Song, Di Qiu, Ian Watts, Ting Xue, Nicola Yap, Alice Yeung, Ken S Zhang

IBM Canada

Scott Berens, Mark Fantacone, Willie Harris, Emma Jacobs, Hari Madduri, Sanjay D. Pillay, Rajeeta Shah, Lily Orozco, Adriana Lopez Russell, Patrick Woods IBM USA

Silvia Bellucci, Gianluca Bolognesi, Luigi Buoscio, Anna Ciotti, Donatello Le Donne, Giuseppe Grammatico, Giulia Farinelli, Claudio De Ingeniis, Fabrizio Loppini, Salvatore Matrone, Giuseppe Parisi, Federica Scarfone, Edoardo Turano IBM Italy

Marcio Rogerio Luccas IBM Brazil

Pawel Niezgoda IBM Poland

Lucian Ticov IBM Romania

Gary Hamilton, Phil Billin IBM UK

The team would like to express special thanks to people managers Calogero Bufalino Marinella and Pietro Scarscioni from *IBM Italy* and Steve Roberts from *IBM Canada* for providing the logistics and resources for the project.

Also we would like to acknowledge the efforts of Stefano Sidoti and Davide Cosentino from *IBM Rome Lab*, who provided the technical support and coordinated access to the resources during the residency.

Finally, a well deserved thank you to Barbara Fierro from *IBM USA* and Iris Leung from *IBM Canada*, for their support in IBM Service Management scenarios.

Become a published author

Join us for a two- to six-week residency program! Help write a book dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You will have the opportunity to team with IBM technical professionals, Business Partners, and Clients.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you will develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

Use the online Contact us review Redbooks form found at:

ibm.com/redbooks

Send your comments in an e-mail to:

redbooks@us.ibm.com

Mail your comments to:

IBM Corporation, International Technical Support Organization Dept. HYTD Mail Station P099 2455 South Road Poughkeepsie, NY 12601-5400

xxiv IBM Tivoli Provisioning Manager V7.1.1: Deployment and IBM Service Management Integration Guide

Part 1

Concepts and architecture

In this part of the book, we first provide a brief overview of provisioning concepts. We then introduce Tivoli Provisioning Manager V7.1.1 and explain how this product can be used to implement a comprehensive provisioning solution in your environment, focusing on the business value of the solution. We also discuss Tivoli Provisioning Manager architecture, in perspective with the overall Tivoli process automation engine platform.



1

Tivoli Provisioning Manager V7.1.1 overview

In this chapter we provide an overview of Tivoli Provisioning Manager Version 7.1.1, together with the new features in this release, as well as a summary of the changes between this version and Tivoli Provisioning Manager Version 5.1.x.

We cover the following topics:

- "Introduction to Tivoli Provisioning Manager" on page 4
- 1.2, "What is new in this release" on page 11
- "Tivoli Provisioning Manager Version 7.X client value" on page 17

1.1 Introduction to Tivoli Provisioning Manager

Provisioning is an end-to-end capability to *automatically* deploy and dynamically optimize resources in response to business objectives in heterogeneous environments. Provisioning helps you to respond to changing business conditions by enabling a dynamic allocation of the existing available resources to the processes that most need them, as driven by business policies. Provisioning of individual elements, such as identities, storage, servers, applications, operating systems, and middleware is a critical step to orchestrate the entire environment enabling it to respond to business needs on demand.

Provisioning focuses on the self-configuring, dynamic allocation of individual elements of the IT infrastructure so that identities or storage or servers are supplied as business needs dictate. These elements could be:

- A single software package
- A software stack, which consists of a group of software packages
- A server, which conforms to a template that is a defined set of software and hardware resources

1.1.1 Tivoli Provisioning Manager concepts

If you are new to Tivoli Provisioning Manager, the following section will help you understand some of the important concepts related with the product.

	Workflow	A series of steps that are sequentially executed to accomplish a particular task. A step in a workflow is called a <i>transition</i> . Each workflow has a single compensating workflow that is executed if any transition fails.
	Automation package	A collection of commands, shell scripts, workflows, logical device operations, and Java [™] plug-ins that applies to the operation of a specific type of software component or a physical device.
	Device driver	Also referred to as a <i>device model</i> , this is a group of workflows that can be a applied to an IT asset.
	Logical device operation	A task that is abstracted from its implementation. Logical device operations (LDOs) are implemented by Enterprise Java Beans (EJB). They provide a common interface and can perform logic. An example is a data center task of adding an IP address. It is a logical operation in that it makes no assumptions about the implementation. (Note that adding an IP address to Linux is very different from adding an IP address to Windows.)

Transition	A step in a workflow. This could be another workflow, a logical operation, a simple command, or a Java plug-in.
Data center model	A representation of all of the physical and logical assets under Tivoli Provisioning Manager management.
Customer	A customer owns applications. Customers can be unique corporations or departments within a single corporation.
Application	A grouping of one or more clusters. Service level priority (Silver, Gold, Platinum) is assigned at this level.
Application tier	A grouping or container for like resources or servers that support an application. Automated resource allocation and deallocation occurs at the cluster level.
Resource pool	A container of available (deallocated) servers that support one or more application clusters. Also referred to as a spare pool.
Servers	Data center model objects that represent physical servers. They belong to or are assigned to pools and clusters.
Software stack	Either an image stack or product stack that contains an ordered list of software products, software stacks, or both.
Software product	The attributes and the methods for deploying a piece of software on an asset. A software product can be user-written or COTS (commercial off-the-shelf).
Capability	Identifies attributes of a piece of software that can be used for prerequisite and co-requisite validation.
Requirement	Defines dependencies on software or hardware. Requirements can be used to define different types of relationships, such as requirements that identify an installation mechanism, requirements to run the software, hosting requirements.
Service Access Point (SAP)	A definition of the protocol and credentials used by or associated with an asset. The configuration data for a service access point includes the application protocol, network protocol, and the endpoint details (IP address, port). An asset can have more than one SAP.

Software Configuration Template (Software Resource Template (SRT))

A software configuration template identifies software resources and associated configuration details that you want to represent in the data center model after the software is installed on a system. Each software configuration template is used to create a software resource on the target system.

Figure 1-1 shows the relationship between device model, logical device operations, workflows, and data center infrastructure.



Figure 1-1 Data center infrastructure mapped into the device model

1.1.2 The data center model (DCM)

The data center model is a model of physical assets in a data center with a logical organizational structure to give context. The logical organizational structure answers questions such as, "What customer is using this server?" and "Which applications can use this server when their needs increase?

The data center model is an internal representation of the data center including hardware, software, logical entities and customers. In order to make intelligent decisions about reallocating resources, the current state is always modeled.

When changes are made, the ramifications of those changes must be completely understood. A server can belong to one resource pool, be assigned to a given application tier, be a member of a particular VLAN (virtual lan), and so on. All of these relationships need to be understood so that when the server is moved, it is returned to the correct pool, it is changed to the correct VLAN if necessary and so on. The data center model captures all of these relationships and maintains them appropriately when reallocating resources.

The data center model is implemented as a relational database.

When software is installed on a computer using Tivoli Provisioning Manager, the software will be installed on the physical machine, and also the DCM will be updated to update the logical model in the DCM. If management operations such as software installs or computer network re-configuration are performed without using the Tivoli Provisioning Manager environment, then the logical model in the DCM will no longer be a correct representation of the real physical environment.

Data center model objects

Physical elements in the data center are modeled as DCM objects that are generic representations of the physical elements. See Figure 1-2. A Cisco 2600 and a Cisco 3548 would each be modeled as a *Switch* DCM object; an xSeries server and a pSeries server would each be modeled as a *Computer* DCM object; and an installation binary for Apache on Windows or Apache on Linux would each be modeled as a *SoftwareInstallable* DCM object.



Figure 1-2 Data center model objects

Configuration information is also modeled in the DCM. An example of this is information used to connect to remote systems. This connection information is modeled as a *ServiceAccessPoint* DCM object.

Management operations

Typical management operations are generalized and grouped by the sort of device that would be the target of the operation. Operations such as *turn port on* and *turn port off* are most often run against switches, so those operations are grouped and associated with a *logical device* called Switch. Operations such as *execute command* and *copy file* are so generic that they are grouped and associated with a logical device. Because all of the generic operations are associated with logical devices, they are called *logical device operations* (*LDOs*).

DCM objects can behave like one or more logical devices. It is possible to associate any LDO with any DCM object, but not all of these associations would make sense and not all LDOs would function (some validate the DCM object type before running).

Workflows

Workflows are the instructions that the deployment engine executes when it is carrying out a management task. These instructions are expressed in a script-like language and can call logical device operations and other workflows.

Parameters can be passed to workflows at run time, and parameters can be looked up by the workflow when it is running, allowing for modular and reusable workflows.

Using LDOs, a workflow can be written at a high level to carry out a complicated management task, and the LDOs can call other workflows to interact with specific hardware and software.

Important: As shown in Figure 1-2 on page 8, Tivoli Provisioning Manager is an object oriented system where not only data about resources can be stored but also operations on them. Invoking those operations programmatically leads to task automation. It is extensible to accommodate new device types, by adding automation packages. Programmability is a key strength of Tivoli Provisioning Manager.

Customer topology

A typical data center will be used to provide to provide one or more services to one or more customers. When servers are being utilized to provide a management service such as Web Hosting to Application Hosting, the customer topology can be used to model this situation.

As shown in Figure 1-3, A *Customer* can be defined, each with one or more *Applications*. Each Application can have one or more *Application Tiers*. Each Application Tier will have one more servers assigned to it. Application Tiers can have a number of dedicated servers, or a number of servers that have been assigned from a Resource Pool.



Figure 1-3 Customer modelling in the DCM

Resource pools are used to share resources (Servers) between different application tiers, and are defined to increase the utilization rates of servers in a data center. Increased utilization rates are the result of sharing processors among multiple applications. In order to realize these performance improvements, one must share the servers. Resource pools are unallocated resources that can be given to an application cluster in response to increased demand. Likewise, when demand declines, servers are returned to the resource pool by the applications. (Resource pools are also called spare pools.)

An example is shown in Figure 1-4.



Figure 1-4 Customer example in the DCM

1.1.3 Security

In Tivoli Provisioning Manager, the security consists of:

- Authentication
- Authorization
- Workflow security services

Authentication is the process of logging into Tivoli Provisioning Manager.

It uses the framework provided by Tivoli process automation engine platform (see 2.1, "Tivoli process automation engine" on page 20). This is integrated into WebSphere® security service to accomplish the authentication service.

Authorization is the control of which users can use which applications.
The resources that a user has permission to access are defined by security constraints. Security constraints in Tivoli Provisioning Manager 7.1.1 are the combination of conditions and data restrictions in Maximo®.

Workflows can be protected. This means that they can only be run by a user having the correct set of permissions. The underlying security for workflow uses Maximo (its combination of conditions and data restrictions).

All of them are integrated in the Maximo Security Framework, which is now part of the Tivoli process automation engine.

1.2 What is new in this release

This section provides a summary of new product features and enhancements in Tivoli Provisioning Manager version 7.1.1 as compared to Tivoli Provisioning Manager version 7.1. Most of these enhancements are expanded in the subsequent chapters of this book.

Note: You can refer to the following link for an overview of Tivoli Provisioning Manager V7.1.1 features:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp?to
pic=/com.ibm.tivoli.tpm.scenario.doc/overview/covw_overview.html.

We discuss the following enhancements in this section:

- Custom attributes
- Compliance
- Compliance with Federal Information Processing Standard 140-2
- Discovery
- Discovery Library Adapter (DLA)
- Installation
- IPv6 addressing
- Migration
- Operating systems management
- Patch Management
- Reporting
- Scalable distribution iInfrastructure (SDI)
- ► Security
- ► Start Centers
- Target computers
- Task management
- Virtualization

1.2.1 Custom attributes

You can now add custom attributes, both as *data model properties* and *Configuration Item (CI) extended attributes*.

Note: A *Configuration Item* is any component of an IT infrastructure that is under the control of configuration management. A *Configuration Item extended attribute* is an attribute that is not part of the original data model, but is added by the user.

1.2.2 Compliance

You can now create a software configuration template that represents a standard software configuration to be implemented on target computers. After you have created the template, you can create a software configuration check based on it and run the check to compare the configuration of the application on target computers with the standard configuration for that application.

See Chapter 9, "IBM Service Management integration scenarios: Compliance and remediation with TADDM" on page 217 for a compliance scenario.

1.2.3 Compliance with Federal Information Processing Standard 140-2

You can enable FIPS 140-2 compliance for new Tivoli Provisioning Manager installations.

Note: FIPS 140-2 compliance is not supported for upgrade from version 7.1 to version 7.1.1.

1.2.4 Discovery

Here are some improved discovery capabilities:

- By using custom inventory extensions, you can extend the data model inventory schema with additional attributes, and you can perform custom inventory scans.
- You can generate reports for inventory extensions.
- Improved automation packages for HMC (Hardware Management Console) discovery are available in this release.
- Discovery of IPv6 addresses is now supported

1.2.5 Discovery Library Adapter (DLA)

The Tivoli Provisioning Manager Discovery Library Adapter (DLA) has been enhanced. You can now export a specific subset of data types, such as software products or a set of computers, computer related objects (software installations and operating systems), and attributes to the discovery library book. In addition, the DLA now writes physical CPU information into the discovery library book, which can be consumed by other products through the DLA itself.

1.2.6 High availability

The managed agents can now be automatically configured to work with a back-up manager. When the secondary manager is established, the managed agents are reconfigured to be associated with the new manager.

See 2.2.3, "Tivoli Provisioning Manager V7.1.1 configuration for high availability and data integrity" on page 34 for details of configuring Tivoli Provisioning Manager for high availability.

1.2.7 Installation

The following enhancements have been made:

- ► Administrative workstation on UNIX® operating systems is supported.
- New platforms and versions are supported for installation: Windows® Server 2008, Windows Server 2003 R2, AIX® 6.1, Red Hat Enterprise Linux® 5, SUSE Linux® Enterprise Server 10, and Solaris 10.
- A new database version is supported for installation: Oracle 11g.
- A new directory server version is supported for installation: IBM® Tivoli Directory Server 6.2.
- Enhanced installation process and user interface are available: The installation process is more streamlined by installing the base services before Tivoli Provisioning Manager components. The launchpad options are better designed and the fields provide more details and explanatory information.
- This release offers enhanced verification of prerequisites during the installation process:
 - Created additional checks for the required packages.
 - Included checks for AIX disk space requirements.
 - Added requirements checklists to be reviewed and validated by the user during the installation process.
 - Consolidated the prerequisite check results.

The recovery procedure was enhanced by automating the WebSphere® Application Server, database, and base services deployment folder backup procedures.

Refer to 4.3, "Tivoli Provisioning Manager V7.1.1 installation" on page 68 for Tivoli Provisioning Manager installation.

1.2.8 IPv6 addressing

A dual stack environment supports communication using either IPv4 and IPv6 addressing. The dual stack environment helps organizations to transition their network from IPv4 to IPv6 addressing. By default, IPv6 support is disabled. If you want to use IPv6 support, you must enable it after installation.

Note: For Tivoli Provisioning Manager on Windows, IPv6 enablement is not supported.

1.2.9 Migration

You can migrate data and artifacts from version 5.1.1.2 to the version 7.1.1 level. See Chapter 17, "Migrating from Tivoli Provisioning Manager Version 5.1.1.2 to Tivoli Provisioning Manager Version 7.1.1" on page 541 for a detailed coverage of the migration.

Note: To migrate your data from version 5.1.1.2, you must install version 7.1.1 on another computer on the same VLAN as the 5.1.1.2. That is because at a certain point in the migration process, you have to configure the new system to use the 5.1.1.2 system host name and IP address.

1.2.10 Operating systems management

The following enhancements have been made:

- You can view the replication status of your OS deployment servers.
- You can copy log files from a remote OS deployment server to the local repository on the provisioning server using a provisioning workflow.
- You can create an image properties file that defines parameters for to all future deployments of an image. An image properties file includes settings that are not available in the Web interface.

Refer to Chapter 14, "Operating system provisioning" on page 409 for a detailed coverage and scenarios.

1.2.11 Patch Management

The following enhancements have been added:

- Scalable Patch Management on Linux RHEL 5 target computers using the scalable distribution infrastructure.
- Patch Management for HP-UX environments using Software Assistant (SWA).
- Patch Management solution for SUSE Linux environments using the rug command-line tool, provided with SLES 10 operating systems.
- Enhanced Patch Management solution for Solaris environments using Sun Update Connection Enterprise.

For more information, see Chapter 13, "Patch Management scenarios" on page 371.

1.2.12 Reporting

New notification reports are available using the Business Intelligence and Reporting Tool (BIRT) framework.

1.2.13 Scalable distribution infrastructure (SDI)

The following SDI enhancements have been added:

- ► IPv6 addressing can be used in the scalable distribution infrastructure.
- An enhanced agent upgrade mechanism using the scalable distribution infrastructure is available. This solution provides highly scalable update distribution capabilities to previously installed agents.
- The maximum size of a software package block for software distribution has been doubled and can reach now up to 4 GB.

For more information, see 5.2, "Implementing the scalable distribution infrastructure" on page 107.

1.2.14 Security

The following security enhancements have been added:

- Multiple LDAP repositories are now used for storing user and group information with the help of the Virtual Member Manager (VMM) framework.
- Authorization on workflow executions is enabled by instance level security.
- Authorization for Web interface elements based on role permissions and new security groups is now available. These are provisioning permission groups that identify the specific user, the permission, and the resources to be protected.

For more information about implementing Tivoli Provisioning Manager V7.1.1 security, refer to 5.1.1, "Security overview" on page 102.

1.2.15 Start Centers

New Start Centers exist for focused role-based access to functions and data. For more information, see Chapter 6, "Tivoli process automation engine based user interface" on page 137.

1.2.16 Target computers

The following new operating systems and functions are supported on provisioning server target computers:

- Linux RHEL 5 is now supported on endpoints.
- The ability to pause and resume a deployment operation offers the ability to define the maintenance window for each target computer under management.

1.2.17 Task management

The following enhancements have been made in the task management area:

- You can create a group from the target computers, on which you have run a provisioning task. In this way, you can schedule new tasks to run on the same set of targets.
- You have now the ability to rerun a failed task on specific target computers where the initial task failed.

You can define a concurrency level within a provisioning task before the provisioning task is run. The concurrency level determines the maximum number of concurrent jobs that are permitted within a task.

1.2.18 Virtualization

The following virtualization enhancements have been added:

- The virtual server status can be verified from the provisioning server before requesting a virtual machine.
- Because of the multipath I/O function, you now have continuous access when a virtual I/O server has to be taken offline for planned outages.
- Streamlined creation of VMware virtual machines by supporting the discovery and deployment of VMware templates.
- When creating a virtual server template, you can now specify a target folder for the virtual server container.
- ► Advanced search capabilities are available for virtualization management.

1.3 Tivoli Provisioning Manager Version 7.X client value

For existing Tivoli Provisioning Manager V5.X customers, the following list summarizes the business benefits that will be realized after moving to a Tivoli Provisioning Manager V7.1 or Tivoli Provisioning Manager V7.1.1 environment:

- Inclusion of Tivoli Provisioning Manager tasks in Change, Release, and Tivoli Service Request Manager flow definitions.
- Ability to easily take Tivoli Provisioning Manager actions on CCMDB CIs:
 - The use of CMDB CIs as database for process flow construction and information is automatically translated to Tivoli Provisioning Manager DCM for operational purposes.
- Ability to use Tivoli process automation engine workflow editor to design and formalize Tivoli Provisioning Manager activities:
 - You can define Tivoli process automation engine workflows to formalize and automate multi-person Tivoli Provisioning Manager activity flows.
 - Tivoli Provisioning Manager activity flows can include non-Tivoli
 Provisioning Manager related tasks (for example, sign-offs, escalations).
- Extensive Web Replay scenario library provides guidelines and education on product use (quick method for product education and skills transfer).

- ► New, highly customizable Tivoli Provisioning Manager GUI technology:
 - Easy modification of existing applications.
 - Ability to create your own applications.
 - Easily customizable to display only required data and tasks for a specific role or user.
 - Consistent look and feel across IBM Service Management products provides seamless interactions and minimizes user education requirements.
 - Ability to incorporate functions from multiple IBM Service Management products on single screen.
- Orchestrated automation capabilities:
 - Advanced automation technology can be used to support infrastructure service level agreements (SLAs) through dynamic resource allocation based on monitoring inputs.
- Enhanced integration with Tivoli Application Dependency Discovery Manager (TADDM), Tivoli Storage Productivity Center (TPC), and IBM Rational Test Lab Manager (RTLM):
 - TADDM: Closed loop desired state management for software configurations.
 - TPC: Launch in context from Tivoli Provisioning Manager to TPC.
 - RTLM: Test lab server provisioning with transitions to production.
- Integration with Tivoli Provisioning Manager for Operating System Deployment:
 - Seamless transition from using Tivoli Provisioning Manager to using Tivoli Provisioning Manager for Operating System Deployment; no product switching is required to utilize baremetal or initial image install functions.
 - Automated database exchange between the two products.
- Enhanced SDI management capabilities:
 - Better status information and enhanced control of deployment infrastructure.
- Additional virtualization technology support.
- Additional OS support.

2

Architecture

In this chapter we address the challenge of integrating many solutions to multiple problems in a service management environment, especially when the solutions were supplied by different vendors.

We cover the following topics:

- "Tivoli process automation engine" on page 20
- "How Tivoli Provisioning Manager extends the Tivoli process automation engine" on page 25
- "Tivoli Provisioning Manager V7.1.1 component architecture" on page 27
- "Tivoli Provisioning Manager V7.1.1 configuration for high availability and data integrity" on page 34
- "Tivoli Provisioning Manager V7.1.1 scalability" on page 34

2.1 Tivoli process automation engine

Because there are multiple problems to tackle in a service management environment, you need to implement multiple solutions, such as Asset Management, and Configuration Management, as shown in Figure 2-1. The challenge is how to integrate all these different solutions to provide an end-to-end service management environment, especially when these solutions were supplied by different vendors.

Tivoli's strategy is to build the complete IBM Service Management portfolio of products on top of a common platform, called the *Tivoli process automation engine*. This platform provides the common user interface, configuration services, process workflow runtime and services, and common data system. *It is more than what Maximo was in previous Maximo products. It includes installation solutions, common services needed for IBM Service Management, and other services.*

This approach has two important benefits:

- You can introduce these solutions incrementally.
- All of these solutions are integrated on top of the Tivoli process automation engine platform to provide an overall, end-to-end service management solution. You do not need to implement this integration yourself.

The Tivoli process automation engine is unique in its ability to:

- Combine asset and service management in one environment
- Deliver a federated configuration management system
- Provide advanced business process management and integration with other Web-based tools
- Preserve upgradeability and ease of configuration, and offer full end-to-end management views of business applications



Figure 2-1 Tivoli process automation engine

As you can see from Figure 2-2, the Tivoli process automation engine is composed of four blocks, which are sets of core capabilities:

- Common User Interface
- Common Configuration Services
- Process Workflow Runtime and Services
- Common Data Subsystem



Figure 2-2 Tivoli process automation engine core capabilities

2.1.1 Common User Interface

The Common User Interface is a Web interface that can be accessed by using the most common browsers such as Firefox 2 or 3 and Internet Explorer® 7 from almost every machine in the network. A certificate ensures the security of an access.

The views can be customized to make a corporate identity and moreover to configure windows that fit for the specific roles of the users. For example, you can change these windows so that a user responsible for the Software Packaging will not see another window pertaining to the user responsible for the Inventory.

As you build solutions on this Common User Interface, you can navigate from one to another easily.

2.1.2 Common Configuration Services

The Common Configuration Services provides a set of tools to change the user interface or data configuration easily using drag and drop icons on a canvas. Using the tools, you can link the UI widgets to the underlying data model, and the underlying data model to the actual database tables. This allows clients to configure IBM Service Management applications for different environments and requirements.

Common Configuration Services provides interfaces to several common functions used in IBM Service Management applications, such workflows, data extensions, and report definitions. The data visualization is also done here.

2.1.3 Common Data Subsystem

The Common Data Subsystem holds all the data to describe the objects in the environment. It stores the data as Configuration Item (CI) in the database. The CI represents a single object (for instance, a server or printer together with their specific attributes) and used in ITIL based Configuration Management solutions, such as CCMDB.

There is also metadata to describe an object and process artifacts, which are objects you need in CCMDB with any of the service management processes, for example, a Request For Change (RFC) for Change Management or Problems for Incident Management. This information is read for configuration operations and processes.

2.1.4 Process Workflow Runtime and Services

The Process Workflow Runtime and Services provide a set of tools and an engine to define your process flows. You can use these facilities, for example, to inform users about the current process status or to notify and escalate events in your process flows. Common Process Workflow Runtime and Services also provides collaboration and security methods to ensure integrity on the process level.

2.1.5 An integrated Service Management portfolio on top of the Tivoli process automation engine

Figure 2-3 shows that all IBM Service Management products are built on top of this common platform, the Tivoli process automation engine, and they use all of these services provided by the platform.



Figure 2-3 Tivoli process automation engine enables an integrated portfolio

The Tivoli process automation engine integrates a portfolio of applications such as Service Request Management, Release Management, Storage Management and Asset Management. This allows other applications to use the existing Tivoli process automation engine and to extend it with additional features and capabilities. The user interface can be employed to give a familiar picture to the user.

For this integration, the Process Workflow and Runtime Services can be extended by integration modules from other IBM and non-IBM software, such as IBM Tivoli Monitoring, Discovery Tools, customer developed software.

Important: When an IBM Service Management product needs to make a change in the IT infrastructure, it does not talk to Operational Management products directly, but does this through an integration module. For example, in a Change Management process, if a change needs to be done in the IT environment (for example, as a result of an approved RFC), CCMDB does not directly talk to the Operational Management product, but communicates through an integration module. Operational Management product performs the change.

The integration modules can connect to other Operational Management Products such as Storage Management, Application Management, Network Management, and Security Management.

The Operational Management Products and also other software running on the IT Infrastructure (servers, storage, networks, software, applications, and transaction services) can start workflows controlled by the integration modules, but they can also store and retrieve data to and from a Discovery and Application Discovery Mapping. This data can be read from and written to the Common Data Subsystem. This allows a flexible and, at the same time, a single way of the processes.

Any product that has the Tivoli process automation engine as its foundation can get installed with any other product that has the Tivoli process automation engine. The Installer will detect that the Tivoli process automation engine is already installed and will just enable the additional applications and features of the product being installed.

Note: Every product ships with a specific version of the Tivoli process automation engine. The versions must match up if you are installing more than one product.

2.2 Tivoli Provisioning Manager capabilities

In this section we describe many new capabilities of Tivoli Provisioning Manager.

2.2.1 How Tivoli Provisioning Manager extends the Tivoli process automation engine

Since Version 7.1, Tivoli Provisioning Manager is built on top of the Tivoli process automation engine. This has made possible many new capabilities, such as integrated process automation and improved user interaction experience, by using the powerful Start Center functionality.

Another advantage of this integration is the capability to use the powerful Tivoli process automation engine functions, such as uniform security, common BIRT reporting, common installation, automation tasks, escalations, and actions, which are available to all applications that utilize the Tivoli process automation engine platform.

The Tivoli Provisioning Manager extends the Tivoli process automation engine for the *Tasks Automation Processes*, task management, and data retrieve, as shown in Figure 2-4.

When we discuss the *Tasks Automation Processes*, we mean using *Tivoli Provisioning Manager deployment engine* and *scalable distribution infrastructure* to execute tasks on a large distributed endpoints.

Important: Tivoli Provisioning Manager is the *Do'er* of the process tasks from other ISM products.



Figure 2-4 How Tivoli Provisioning Manager extends Tivoli process automation engine

As you can see from Figure 2-4, Tivoli Provisioning Manager adds Patch Deployment, Software Deployment, Operating System Deployment, and Virtualization capabilities, and provides interfaces to the Change and Configuration Management Database (CCMDB) and Tivoli Service Request Manager and other IBM Service Management Products. The discovery of existing applications and relationships done by Tivoli Application Dependency Discovery Manager (TADDM) feeds the Common Data Subsystem, storing data in Configuration Items and assets and so on in the database. Tivoli Provisioning Manager adds his own Tivoli Provisioning Manager discovery to extend TADDM functionality and stores data in an additional segment of the Common Data Subsystem. The Tivoli Provisioning Manager data contains the DCM objects and other Tivoli Provisioning Manager specific data.

All retrieved data is merged in the Common Data Subsystem so that Tivoli Provisioning Manager can use it for provisioning. This combination provides the opportunity to combine the Process Level Information with Provisioning Level Information and provides better integration between IBM Service Management processes and Tivoli Provisioning Manager processes.

The main advantage is that with the Tivoli Provisioning Manager strictly integrated with Change and Configuration Management Database and Tivoli Service Request Manager, we give to IBM Service Management structure the provisioning functionality.

The Tivoli process automation engine is able to control applications such as TADDM and CCMDB. Tivoli Provisioning Manager makes use of additional functionalities from the other applications to provide provisioning for networks, storage, and virtual server environments. The Workflows describe tasks in the customer environment and can be adjusted for specific needs to automate provisioning tasks in the most effective way.

2.2.2 Tivoli Provisioning Manager V7.1.1 component architecture

Tivoli Provisioning Manager consists of a provisioning server, a Web-based operator and administrator console, and an Automation Package Developer Environment.

Figure 2-5 illustrates the architecture of the components, and highlights how such components interact with your managed IT infrastructure and other applications in your environment.



Figure 2-5 Tivoli Provisioning Manager main components and interaction

Next we describe each of these components:

Provisioning server:

The provisioning server is the server on which Tivoli Provisioning Manager is installed. The provisioning server contains the following components.

Provisioning database:

The provisioning database is the physical database for Tivoli Provisioning Manager. The provisioning database holds the data model.

► Data model:

The data model is a representation of all of the physical and logical assets that are managed by the provisioning applications, such as computers, switches, load balancers, application software, virtual LANs, and security policies. It keeps track of hardware and associated allocations to applications, as well as changes to configuration. When a provisioning workflow successfully completes a requested change, the data model is updated to reflect the current infrastructure.

The data model also stores information about allocated and unallocated computers in resource pools for tier management. This information can include computer identifiers, resource pool size, the number of active and idle computers, computer priority, and similar information.

Discovery and configuration management also use the data model to identify configuration changes that are made outside of the provisioning applications. You can review changes and use the change information to restore an asset to a previously known state.

Automation package:

An automation package is a collection of provisioning workflows, scripts, and other commands and tools that apply to the operation of a specific type of software component or a physical device. The deployment engine manages the deployment of provisioning workflows and associated components in an automation package.

You can use automation packages to automate the provisioning of software, patches, images and operating systems, as well as devices, including computers, network devices, and storage.

Compliance and remediation:

Compliance management enables you to examine the software and security setup that you have on a target computer (or a group of computers) in your managed infrastructure and then compare that setup with the setup that you want in order to determine if they match. If they do not match, noncompliance occurs, and recommendations (remediation) on how to fix the noncompliance issues are generated.

► Reporting:

Reports enable you to retrieve current information about enterprise inventory, activity, and system compliance. The reporting functionality includes:

- Predefined reports:
 - A Web-based query builder, which you can use to customize existing reports or create new reports
 - · Access to information in the data model using views
 - Sharing of report definitions using import and export capabilities in the Web interface
- Charts and graphs
- The ability to schedule reports to run at a later time or at repeating intervals
- E-mail report distribution and notification
- Integration with vendor reporting software
- ► Discovery:

Discovery provides automated processes that enable you to find resources, as well as changes to existing resources, within your enterprise or managed IT infrastructure. You can use the following discovery technologies:

- Microsoft Active Directory discovery: Discovers computers by organizational unit, Microsoft Active Directory groups, and computer attributes defined in Microsoft Active Directory.
- Tivoli Provisioning Manager network discovery: Discovers computers, their host name and networking information, new resources and changes to existing managed resources.
- Tivoli Provisioning Manager Inventory discovery: Discovers configuration changes and hardware and software on devices.

Deployment infrastructures:

You can reconfigure and reallocate resources in your managed environment using two different deployment infrastructures as shown in Figure 2-5 on page 28. These are a scalable distribution infrastructure (SDI) and a deployment engine infrastructure (DE), which are further described next.

- Scalable distribution infrastructure:

The scalable distribution infrastructure provides a scalable infrastructure for implementing software distribution activities inside Tivoli Provisioning Manager. It includes the following main components:

• Agent Manager: This component provides an infrastructure for managing the computer systems in your environment, enabling secure

connections between managed systems, and storing information about the managed systems and the software running on them.

- Content Delivery Service: This component enables the efficient distribution of files and content to large numbers of targets through intermediate depot components or peer-to-peer distributions between agents.
- Device Management Service: This component provides a solution for managing various devices by performing jobs, which can be targeted to individual Tivoli common agent devices or to groups of devices.

- Deployment engine:

The deployment engine is a virtual server that is designed to run provisioning workflows.

Provisioning workflows are used for specific automation tasks which cannot be done through the scalable distribution infrastructure. Provisioning workflows can also operate on target computers that do not have Tivoli common agent installed on them. An instance of a provisioning workflow being run against a target computer is called a deployment request.

- Deployment engine infrastructure:

The deployment engine infrastructure is generally used for automating operations on smaller sets of managed target computers and runs the automation packages that are available.

The deployment engine creates, stores, and runs provisioning workflows and communicates their success or failure in performing an operation. The deployment engine runs the provisioning workflows against the managed target computers, using whatever native communication protocol is available. The provisioning workflows can be triggered by commands from an administrator, by external tools that send SOAP commands, or by recommendations from the policy engine.

Web Services interface:

Web Services, including Web Services Resource Framework (WSRF) services, allow you to access the data model directly without launching the Web interface. You can use Web Services to access, manipulate, or change objects directly in the data model.

Operator and administrator console:

The Web-based operator and administrator console allows you to interact with the provisioning server. The operator and administrator console provides a graphical representation of the IT assets, includes wizards to simplify configuration, and other features such as reporting and task status tracking that are not available from the command-line interface.

► Automation Package Developer Environment:

Automation Package Developer Environment (APDE) is an Eclipse-based plug-in environment that automation package developers can use to create or customize automation packages.

► IBM Open Process Automation Library:

The IBM Open Process Automation Library (OPAL) is an IBM managed, shared library of process automation. It is a comprehensive online catalog, which contains over 500 IBM Tivoli and Business Partners Product Extensions including automation packages, integration adapters, agents, and documentation.

User directory:

Tivoli Provisioning Manager integrates with several directory servers, allowing you to manage your user accounts and user authentication with a directory server of your choice.

External management applications:

Tivoli Provisioning Manager includes the capability to integrate with external system management applications, including IBM IT Service Management and other vendor software.

Tivoli common agent:

The Tivoli common agent (common agent) consists of common agent services code and product-specific subagent code. For example, Tivoli Provisioning Manager includes subagents for deploying software and obtaining software inventory from managed endpoints. The product-specific subagents consist of one or more OSGi bundles. A bundle is an application that is packaged in a format defined by the Open Services Gateway Initiative (OSGi) Service Platform specification, which is implemented in a lightweight runtime based on WebSphere Everywhere Deployment technology.

Note: The common agent services code is installed once on a managed endpoint. For example, if you have two management applications on the same endpoint (application A and application B), the common agent code is installed only once on the endpoint. However, there will be two product-specific subagents: one for application A and one for application B.

This documentation uses the term *agent* to refer to both the common agent services code and to the agent code when it runs the product-specific subagent, unless specifically stated otherwise.

The common agent provides:

- Continuous operation. Self-healing features ensure that the common agent and subagents are always available. If the common agent stops, a "watchdog" process called the nonstop service automatically restarts it.
- A single set of security credentials and a common security infrastructure for all management applications.
- Automated management of security credentials. When common agent certificates near their expiration date, they are automatically renewed.
- Deployment and life cycle management of subagents. Resource managers can remotely install, upgrade, patch, or uninstall bundles on any common agent. This helps keep the common agent deployment current without having to take explicit action on each common agent system.
- Common agent health monitoring and configuration monitoring. The common agent has a *heartbeat function* that sends periodic status and configuration reports to the agent manager.

The common agent allows any subagent to participate and to provide status information. Management applications can register to receive these updates. Updates are initiated by certain bundle events and periodically by the common agent. You can turn off periodic updates or control the frequency of updates. The default frequency is 24 hours.

The common agent contacts the agent manager and reports its status and any configuration changes at these times:

- When a common agent starts or stops.
- After a configurable period of time. The default is 24 hours.
- Any time a bundle is installed, upgraded, or removed.

The main common subagents are:

- The Device Management Service (DMS) subagent, which periodically polls Device Management Service on Tivoli Provisioning Manager server for new jobs
- The Dynamic Content Delivery (DCD) subagent, which interacts with Dynamic Content Delivery service on depots and Tivoli Provisioning Manager server for downloading software packages
- The Common Inventory Technology (CIT) subagent, which manages collection of inventory data
- The Security Compliance Manager (SCM) subagent, which collects security data
- The Software Installation Engine (SIE) subagent, which is the engine managing software installation on the target system

2.2.3 Tivoli Provisioning Manager V7.1.1 configuration for high availability and data integrity

Tivoli Provisioning Manager 7.1.1 supports an automatic failover technology (often called a high availability cluster) based upon the *Tivoli System Automation for Multiplatforms* product. In particular, the required version of Tivoli System Automation for Multiplatforms is 2.3 (PTF 2 or later is recommended).

The white paper *Tivoli Provisioning Manager 5.1.1: An Automated HADR Customer Solution using Tivoli Systems Automation for Multi Platforms*, written by a team (Mark Leitch, Andrew Kaye-Cheveldayoff, Eugen Postea and Sarvi Aryanpour) from IBM Toronto Lab describes this scenario in detail. Although this white paper was written for Tivoli Provisioning Manager 5.1.1, it is still applicable to Tivoli Provisioning Manager 7.1.1. You can download this document at:

http://www.ibm.com/software/tivoli/opal/?NavCode=1TW10106X

2.2.4 Tivoli Provisioning Manager V7.1.1 scalability

Given the large scale enterprise management goal of Tivoli Provisioning Manager, performance is critical. The most basic performance and scalability statement for Tivoli Provisioning Manager V7.1 was:

- Management of up to 30,000 targets (also knows as endpoints)
- Support for up to 200 concurrent administrators

The results are published in the following white paper: *Tivoli Provisioning Manager 7.1: Capacity Planning Cookbook* (written by Mark Leitch and Andrew Kaye-Cheveldayoff). It is available at:

http://www-01.ibm.com/software/brandcatalog/portal/opal/details?catalog
.label=1TW101070

Tivoli Provisioning Manager V7.1.1 is expected to have *comparable or better* results, but at the time of writing the book, the tests and performance analysis were not finished and the results were not yet published for Tivoli Provisioning Manager V7.1.1.

Note that these numbers represent the maximum tested configuration for Tivoli Provisioning Manager and should not be considered as hard limits. Depending on your environment and workload, the limits can be lower or higher.

Part 2

Planning for deployment and implementation

In this part of the book, we first discuss some important considerations you should take into account before deploying Tivoli Provisioning Manager V7.1.1 in a production environment. Then we discuss installation of Tivoli Provisioning Manager V7.1.1 components followed by the initial customization. We have included a simple software deployment scenario in order to test our deployment and verify that the environment we have installed is up and running.

Note: If you are not familiar with Tivoli Provisioning Manager, take a look at Chapter 5, "Customizing Tivoli Provisioning Manager V7.1.1 after installation" on page 101 and go over this scenario before moving on to the more complex scenarios covered in Part 3, "The new GUI and IBM Service Management integration scenarios" on page 135.



3

Installation planning and deployment scenarios

In this chapter we provide an overview to deployment scenarios, such as an installation of Tivoli Provisioning Manager on a single node or on multiple nodes. We discuss considerations for smaller and larger environments, as well as some hints about working in a firewall environment.

We cover the following topics:

- "Installation topologies" on page 43
- "Multi-node installation" on page 45
- "Considerations for the firewall environment" on page 48

3.1 Installation considerations

The simplest form of installation is the single node installation. It is good for demonstration purposes or in a small test or educational environment, but it is less suitable for large production environments.

The other type of installation is the custom installation. Here components can be spread to two or three machines. With the custom installation, you can choose where to install the middleware, such as database and LDAP server.

Important: This is the deployment topology recommended for production purposes.

Tivoli Provisioning Manager includes and requires the following components:

Application gateway service: WebSphere application gateway service:

Tivoli Provisioning Manager is a Web-based application that uses WebSphere Application Server as the application server.

Database Server: DB2 or Oracle RDBMS:

The database server hosts the provisioning database, which includes the data model of managed assets. It also stores the Tivoli process automation engine database which contains text for the user interface and field-level help entries.

Note: If you want to use DB2, you can either install it as part of the Tivoli Provisioning Manager installation, or use an existing version of DB2 from your system.

If you want to use Oracle Database, you must obtain your own Oracle Database installation media and install it before installing Tivoli Provisioning Manager.

HTTP Server: IBM HTTP Server:

A a separate, dedicated HTTP server that can be configured to work with the application server.

Directory Server (LDAP): Tivoli Directory Server or Microsoft Active Directory:

The directory server provides user authentication and access control.

Note: If you want to use Tivoli Directory Server, you can either install it as part of the Tivoli Provisioning Manager installation, or use an existing version of Tivoli Directory Server from your system.

If you want to use Microsoft Active Directory, you must obtain your own Microsoft Active Directory and install it before installing Tivoli Provisioning Manager.

 Tivoli Provisioning Manager for Dynamic Content Delivery Management Center:

A core component for provisioning. It provides centralized control of the uploading, replication, and downloading of files. It also monitors the state of depot servers in distributed locations and stores file data.

► Tivoli Provisioning Manager for Job Management Service Federator (JMS):

A core component for provisioning. Also called the device manager service, this component acts as a federated server that manages job distribution. It pushes incoming jobs to all of the endpoint agents or regional agents.

► Agent manager:

A core component for provisioning. Tivoli Provisioning Manager uses the Tivoli Common Agent Services for software distribution and compliance. The agent manager is the server component of the Tivoli Common Agent Services and provides secure connections with managed computers on which the common agent is installed.

Tivoli Provisioning Manager for Operating System Deployment (OSD):

A core component for operating system provisioning. It provides operating system management capability, including deployment of captured images and unattended setup.

Monitoring agent:

A core component that provides the ability to monitor the provisioning server.

Administrative system:

The administrative workstation is used to deploy Tivoli Provisioning Manager. After the initial deployment, the administrative workstation is used to make updates or changes to the deployment and add additional process manager applications. Changes to the deployment typically require that the product Enterprise Archive (EAR) files be rebuilt, which can only be done from the administrative workstation. Web components:

Tivoli Provisioning Manager includes a set of applications specific to provisioning.

3.2 Installation requirements

The following topics provide a short summary of installation requirements for single and multiserver installations.

Users and passwords

User names have some limitations, as follows:

- The names can only contain the English alphabet and the following special characters: the period (.), at sign (@), number sign (#), underscore (_) and minus(-). The DB2 Database system requires additional restrictions. On Linux and UNIX, the names must be in lowercase.
- Group names and user names can contain up to 8 characters.

Additional recommendations for the Windows operating system

Because of the DB2 database system application, the following additional restrictions for user names and passwords must be considered.

On Windows, the user name can consist of upper and lowercase letters. The group and user names can contain up to 30 characters. If you are not using client authentication, non-Windows 32-bit clients connecting to Windows with user names longer than 8 characters are supported when the user name and password are specified explicitly.

On Windows, the user and group names must not be any reserved word such as USERS, ADMINS, GUESTS, PUBLIC, LOCAL, or SQL reserved word. It is also not allowed for names to start with IBM or SQL or SYS.

To be on the safe side, we recommend to use user and group names equal to 8 characters and in lowercase. Names should begin with a character.

Note: To avoid potential problems, do not use the special characters @, #, and \$ in a database name if you intend to use the database in a communications environment. Also, because these characters are not common to all keyboards, do not use them if you plan to use the database in another language.

For passwords, the same recommendations are valid as for user and group names. Because of different international keyboard layouts, the special characters should be avoided in passwords.

Passwords

The WebSphere Application Server administrator password must be exactly 8 characters. For DB2, this password cannot be longer than 14 characters on Windows and 8 characters on UNIX and Linux.

More requirements

Depending on Operating System and policies there are more rules such as minimum password length and simplicity:

- Some security controls configured in your environment can prevent the Tivoli Provisioning Manager installer from creating the required user accounts on your system for installation. Here are some factors involved:
 - Permissions or access control lists configured for the computer can prevent the installer from creating users, creating user-related files and directories, or assigning permissions.
 - If a password that is specified during installation does not conform to the password policy configured in environment, the user creation process fails for the user associated with the noncompliant password.
- If problems are encountered with user creation during installation, the users should be created manually to ensure compliance with all security policies and compliance with Tivoli Provisioning Manager requirements. The installer can then use the configured user accounts and user settings to perform the installation.
- The installation on Windows must be started with an administrative account. Users are created as system accounts in the operating system. Domain account users defined on a directory server are not supported for the users required during installation.

- On UNIX systems, including Linux, the umask value must be set to 002 for the root user. If a umask setting already exists, change the value to 002. You can return to the original setting after installation. To set the umask value, perform the following actions:
 - AIX

In the file /etc/security/user, change the umask setting for root to umask = 002.

Linux

If using the bash shell, in the home directory for root, add the line umask 002 at the end of the .bashrc file.

Linux

If using the Korn shell, in the home directory for root, add the line umask 002 to the .profile file.

- If you are using DB2 as your database and the database server is on a different computer than the one where you will install Tivoli Provisioning Manager core components, the following requirements must be met for DB2:
 - You must manually create an operating system user called maximo on the database server. The Tivoli Provisioning Manager core component installer will set any required permissions for the user.
 - For DB2 UNIX installations, the database instance user must exist on the DB2 server. For example, if you plan to create a DB2 instance ctginst1, you must create a user (including the home directory for the user) on the UNIX DB2 server. The fenced user must be db2fenc1 and the group db2grp1 must exist.
 - NIS is not supported for managing user accounts or groups. Ensure that NIS user management is disabled.

3.3 Installation topologies

The installer supports the following installation scenarios out of the box, as shown in Table 3-1.

Table 3-1	Installation topologies	
-----------	-------------------------	--

1 NODE: All components in one box (Windows or UNIX)	2 NODE: Using remote DB server (Windows or UNIX)	2 NODE: Using remote LDAP server (Windows or UNIX)	3 NODE: Using remote database and LDAP servers (Windows or UNIX)
 Node1: Tivoli Provisioning Manager LDAP (Lightweight Directory Access Protocol) Server Database Server WebSphere Server CAS (Common Agent Service) DCD (Dynamic Content Delivery Service) DMS (Device Manager Service) Tivoli Provisioning Manager for OS Deployment TPM-ITM agent (Tivoli Provisioning Server Tivoli Monitoring Agent) 	 Node1: Tivoli Provisioning Manager WebSphere Server Database Client LDAP Server CAS DCD DMS Tivoli Provisioning Manager for OS Deployment TPM-ITM agent 	 Node1: Tivoli Provisioning Manager WebSphere Server Database Server CAS DCD DMS Tivoli Provisioning Manager for OS Deployment TPM-ITM agent 	 Node1: Tivoli Provisioning Manager WebSphere Server Database Client Tivoli Provisioning Manager CAS DCD DMS Tivoli Provisioning Manager for OS Deployment TPM-ITM agent
	Node2: ► Database Server	Node2: ► LDAP Server	Node2: ► Database Server
			Node3: ► LDAP Server

3.4 Single node installation

The single node installation is useful as a demonstration or evaluation system. Only one machine is required, where all required components are installed.

All components such as Tivoli Provisioning Manager server, and middleware, including the administrative workstation, are installed on a single computer with default values. For custom installation, a single-server deployment is one of the possible topologies. It can be chosen between a default installation, where most of the configuration values are predefined; and a custom installation, where some configuration settings such as the installation path can be modified.

A default single-node installation is supported on Windows operating systems such as Windows 2003 and Windows 2008. The Tivoli Provisioning Manager will be installed with default settings and does not include language packs.

The custom installation allows you to specify some more settings such as names, installation directories, and port numbers. The installation is slightly different depending on the requirements of an administrative workstation.



Figure 3-1 shows the single node installation.

Figure 3-1 Single node installation

If an installation has to be done on other operating systems such as AIX, then a Windows OS administrative workstation is required to deploy the components to the target system.

The new installer also allows direct installation on AIX 6.1 and SLES 10 SP2 Linux (64 Bit) systems. There is no additional administrative workstation required.

Note: The administrative workstation will have the Maximo deployment folder to deploy the software to target systems.

For the installation, a static IP address is required and a full qualified domain name registered in DNS. During installation the **nslookup** command checks the machine name.

For the ports required by Tivoli Provisioning Manager, refer to "Considerations for the firewall environment" on page 48.

3.5 Multi-node installation

For larger or more complex environments, the components can be installed on different machines to improve performance and scalability. In addition, existing components such as existing database systems can be re-used.

There is no default installation method if the components will be deployed to different servers. If you plan to reuse existing resources, make sure that the existing middleware software versions satisfy version levels supported by Tivoli Provisioning Manager. Refer to "Reusing existing components" on page 47 for more information about this topic.

If the database server resides on a separate machine, we recommend using a dedicated network for traffic between the Tivoli Provisioning Server (provisioning server) and the RDBMS Server. Usually this implies that you need two network cards with at least 1 GBit per machine. This reduces packet loss and network contentions.

Figure 3-2 shows multi-node topology.



Figure 3-2 Multi-node topology

For a supported multi-server topology, the following components can be installed on a separate computer:

- The database server
- The directory server
- The administrative workstation

Note: The administrative workstation must be a separate computer if the Provisioning server is installed on a platform that is not supported by the deployment software for the base services and Web components.

The middleware installer has to be used on each machine to install required middleware components for communication purposes in the environment. There is a topology.properties file that must be modified for each node to inform the installer about already installed and configured components.
3.6 Reusing existing components

If resources already exist in the environment, such as database server, directory server, or CCMDB, they can be reused for Tivoli Provisioning Manager.

Important note for reusing existing components: Keep in mind that the installer does not check the installed version and it does not install the patches on the existing components. You need to ensure that existing middleware versions are compatible with the Tivoli Provisioning Manager V7.1.1 prerequisites.

The middleware installer can automatically configure DB2 9.5 FP3a and Tivoli Directory Server 6.2 FP1 and 6.1.0.10 for Tivoli Provisioning Manager. IBM WebSphere Application Server, Oracle Database, and Microsoft Active Directory must be configured manually and before the installation starts.

Case study: Configuration of an existing database instance for reusing with Tivoli Provisioning Manager

The following example shows configuration of an existing database instance for reusing with Tivoli Provisioning Manager:

- 1. Log in as a user with administrative authority.
- 2. Launch the middleware installer from the launchpad.
- 3. Proceed through the middleware installer panels as instructed in Installing and configuring the middleware with the middleware installer, until you reach the Deployment Choices panel.
- From the Deployment Choices panel, select Database Server, and then click Next. The Tivoli middleware installer will display any instances of DB2 found on the system.
- 5. From the Installation drop-down menu, select the appropriate instance to reuse, and then click **Next**.
- 6. Complete the installation by proceeding through the remainder of the middleware installer panels.
- 7. If you are using a virtual IP on the computer where the DB2 server for Tivoli Provisioning Manager is installed, run the following DB2 command on the computer:

db2set -g DB2SYSTEM=virtual_hostname

8. Replace *virtual_hostname* with the virtual host name.

For example, if DB2 is installed on a computer with the virtual host name database.example.com, run this command on the computer database.example.com:

db2set -g DB2SYSTEM=database.example.com

9. After you have configured DB2, install the DB2 client on the Tivoli Provisioning Manager server machine.

10. When all the middleware installation is complete, install the base services.

It is also possible to install Tivoli Provisioning Manager on a machine with CCMDB using the same WebSphere Application Server. To do this, run the Tivoli Provisioning Manager launchpad and (if required) upgrade the WebSphere Application server to Version 6.1.0.23. Then, install base services, the core components, and the Web components.

For more details, see Chapter 4, "Installation steps for integration" on page 57.

Important: For Tivoli Provisioning Manager capacity planning information, you can refer to the following white paper: *Tivoli Provisioning Manager 7.1: Capacity Planning Cookbook*, which is available at:

http://www-01.ibm.com/software/brandcatalog/portal/opal/details?cata log.label=1TW101070

This document also provides some best practices showing how to configure Tivoli Provisioning Manager components for small and large production environments.

3.7 Considerations for the firewall environment

During the installation, the firewall must be disabled. See Table 3-2, which shows the ports required for communication of the Tivoli Provisioning Manager. In the Direction column, the arrow points from the source port to the destination port.

Usage	Protocol	Provisioning server port	Direction	Managed computer port
DHCP REQUEST	UDP (broadcast)	67	←	any
DCHP REPLY	UDP	67	\rightarrow	68

Table 3-2 Communication ports

PROXY DHCP	UDP	4011	\leftarrow	any
TFTP	UDP	69	←	any
BootDiscovery	UDP (multicast)	4011 IP:233.1.0.1	~	any
MTFTPPort	UDP	4015	←	any
MTFTPClients	UDP (multicast)	any	\rightarrow	8500 IP:233.1.0.1
NBPServer	UDP	4012	←	any
FileServerPort	UDP	4013	\leftarrow	any
FileMCAST-Address	UDP	any	\rightarrow	10000
FASTPort	UDP	4025	←	any
SSH	TCP	any	\rightarrow	22
Telnet	ТСР	23	\leftarrow	any
TS	ТСР	any	\rightarrow	3389
SNMP	UDP	any	\rightarrow	161
SNMP-TRAP	UDP	162	←	any
NetBIOS name service	ТСР	137	\rightarrow \leftarrow	137 Used during installation. In multiserver topologies, enable the port on a remote database server or remote directory server.
SMB / NetBIOS	ТСР	any	\rightarrow	139
agent manager	ТСР	9511, 9512, 9513	\rightarrow	any
Usage	Protocol	Provisioning server port	Direction	Managed computer port
WebSphere Application Server	ТСР	8881, 9080, 9082, 9061, 9045, 9046, 9443	\rightarrow	any
Eclipse embedded database	TCP	1527	~	any

The ports required for common agent installation depend on the configured connectivity to the target computer. To install the common agent, one of the following configurations must be available:

Default service access points (SAPs)

You can predefine default *Service Access Points (SAPs)* for **Device.ExecuteCommand** and **Device.CopyFile** commands. These SAPs can be used to install the common agent. The port numbers for these SAPs depend on the protocol defined for the SAPs.

Secure Shell (SSH) or Server Message Block (SMB)

If no default SAPs are defined, an SAP for the Remote Execution and Access (RXA) protocol is created on the target computer when the common agent is installed using the Install Common Agent page. The RXA SAP is then used to perform common agent installation. RXA uses the default SSH port 22, or ports 135 (remote procedure call) or 139 (NetBIOS over TCP/IP) to connect to the target.

Ports for the agent manager are created during agent manager installation. An SAP for the common agent is created during the common agent installation with the default port number. The default port for the common agent can be changed. This is described in the manual in the chapter "Changing the common agent default port number".

Table 3-3 and Table 3-4 show the default port numbers that are used.

Table 3-3	Default	ports	used	on	the	managen	nent	side

Connection security
Secure SSL
Secure SSL with Client Authentication
Unsecure
Secure SSL
Au Ur Se

Table 3-4	Default ports used	on the	e target	computer	side

Default ports used on the computer side				
Component	Port	Use	Connection Security	
Common Agent	9510	The default common agent listening port. Configurable.	Secure SSL	
	9010 or 9015	Enable communication between the common agent and the dynamic content delivery management center.	Secure SSL	
	9514 or 9515	Nonstop service. The Nonstop agent service monitors processes on the agent, to make sure they are running and available. The service automatically restarts the processes it monitors if they stop.	Unsecure	

Default ports used on the computer side					
Component	Port	Use	Connection Security		
Dynamic content Delivery Depot	2100	 Used for management and downloads. Enables communication between: The common agent and the dynamic content delivery depot servers. The dynamic content delivery depot servers The dynamic content delivery management center and the dynamic content delivery depot servers. 	Secure SSL		

If a firewall exists between the common agents and the agent manager server, inbound traffic on ports 80 and 9513 to the agent recovery service must be allowed. Opening these ports allows agents to report registration problems. If the agent manager is configured to use a port other than 9513 for the public port, the port must be opened as well, so that agents can report communication problems after their initial registration.

When Tivoli Provisioning Manager is used to install the agent manager, port 80 is disabled and port 9513 is used as the backup port for the agent recovery service. Opening the backup port is especially important when the agent manager use of port 80 is disabled.

Endpoints with multiple network interface cards (NICs) can also be managed. The appropriate host name for that NIC must be configured and the route to be used to the provisioning server. When the common agent is installed, it discovers the IP address of the NIC which is used during communication with the Agent Manager. Tivoli Provisioning Manager uses the IP address used by the common agent to register itself as the management IP address, and the defined host name as seen by the target computer on the management IP as the computer name.

Table 3-5 shows the ports used for communication in the scalable distribution infrastructure. The "Source system" and "Target system" columns show the physical systems involved. The "Source component" and "Target component" columns contain the name of the involved scalable distribution infrastructure components. The "Any" value for source port means that connection uses an ephemeral port and therefore the firewall must be configured so that the source port can have any value.

Source system	Source Component	Source port	Destination system	Destination component	Destination port	Connectio n security
Tivoli Provisioning Manager server	CDS Management Center	Any	Depot	Depot CDS depot server		Secure SSL
Depot	CDS depot server	Any	Depot	CDS depot server	2100	Secure SSL
Common agent	CDS subagent	Any	Depot	CDS depot server	2100	Secure SSL
Depot	CDS depot server	Any	Tivoli Provisioning Manager	CDS Management Center	9045 9046	Secure SSL
Common agent	DMS subagent	Any	Tivoli Provisioning Manager	DMS federated agent	9045 9046	Secure SSL
Common agent	CDS subagent	Any	Tivoli Provisioning Manager	CDS Management Center	9010 9015	Secure SSL
Tivoli Provisioning Manager	Agent Manager	Any	Common agent	Common agent	9510	Secure SSL
Common agent	Nonstop process	Any	Common agent	Common agent	9514 9515	Unsecure
Common agent	Common agent	Any	Tivoli Provisioning Manager	Agent Manager	9511	Secure SSL
Common agent	Common agent	Any	Tivoli Provisioning Manager	Agent Manager	9512	Secure SSL with Client Authenticati on
Common agent	Common agent	Any	Tivoli Provisioning Manager	Agent Manager	9513	Unsecure

Table 3-5 Ports used for communication between Tivoli Provisioning Manager components



Figure 3-3 illustrates the components and connections.

Figure 3-3 Used ports by components

In a typical single firewall scenario, the firewall is between the central management environment and a separate network, either a remote office branch or a demilitarized zone (DMZ). In these cases, the firewall is between the provisioning server and the upload server on the secure side; and the depot and common agent are on the unsecure side. The firewall configuration for this case is shown in Table 3-6.

Source system	Source port	Destination system	Destination port
Tivoli Provisioning Manager server	Any	Depot in unsecure zone	2100
Upload Depot	Any	Depot in unsecure zone	2100
Common agent	Any	Tivoli Provisioning Manager server	9045 9046 9010 9511 9512 9513 9015
Tivoli Provisioning Manager	Any	Common agent	9510

Table 3-6 Open ports in a single firewall environment

3.8 Gateway manager and gateway service

In environments where servers are in another network separated by firewalls, Tivoli Provisional Manager provides the mechanism to tunnel communication through the firewall. The gateway manager component is the firewall component next to the provisioning server that is responsible for tunneling traffic through the firewall. It can reside on the server or another machine on the same side of the firewall.

On the agent side resides the gateway service that receives data packets from the gateway manager and forwards them to the common agent. The gateway service can be installed on any computer residing on same side of the firewall as the gateway service. The firewall components are intended to use with the scalable distribution infrastructure (SDI). The gateway manager and agent service use Secure Socket Layer (SSL) for the communication.

A *proxy relay* is used if there are multiple firewalls between the common agent and the provisioning server. It listens on the default port 1960 for data and forwards it to the next firewall component. This can be either another proxy or the gateway manager or the gateway agent service. It is possible to define other ports if the default ports are not allowed to open. The gateway manager and service are transparent for the server and for the agent. The applications will not see additional components in between the direct communication flow. But the limitation is the execution of workflow.

If a workflow requires direct contact between the provisioning server and the common agent, this will fail because the firewall components cannot route this direct communication request.

Note: As mentioned above, the firewall components are for SDI. Therefore an SDI-SAP must exist for the target computer. This will force us to use the scalable distribution infrastructure and not the deployment engine.

The firewall components are located in the directory, \$TIO_HOME/repository/FirewallProxy. These are bundled in the Java file proxy.jar.

For the gateway manager, the configuration file gateway.xml describes the ports on which the gateway service listens. The same ports are used to contact the provisioning server. At the beginning, the gateway manager instructs the gateway server on which ports it has to listen. The file *gateway.private* holds the private key for the SSL encryption and has to be created manually with IBM Key Management application **ikeyman.sh** or **ikeyman.bat** from the directory \$WAS_installdir/bin. It creates the private and the public key files.

The gateway service needs the generated gateway.public key file and the proxy.jar file from the gateway manager machine.

It is started with:

java -jar proxy.jar -gwservice <Port Number>

This allows the gateway service port to be different from default port 1961.

4

Installation steps for integration

In this chapter we provide guidance for installing the Tivoli Provisioning Manager V7.1.1 product in the same environment as other IBM Service Management products. For the exact levels of CCMDB and other IBM Service Management software installed in our lab environment, refer to "Summary of the product components installed" on page 67.

We cover the following topics:

- "Integration assumptions and rules" on page 58
- "Steps to install and set up the environment to run integration scenarios" on page 59
- "Tivoli Provisioning Manager V7.1.1 installation" on page 68
- "Other samples of integrated environments" on page 92

Important: The information listed here does not replace that available in the official documentation. For detailed instructions for installing and using each Tivoli product involved in the integration scenarios, refer to the Tivoli Provisioning Manager V7.1.1 InfoCenter at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp

4.1 Integration assumptions and rules

In this topic we make the following assumptions:

- Tivoli Provisioning Manager and the products with which it integrates are installed on the same server.
- The server used for installation is listed among the supported platforms for all products to install.

Notes:

- In this book we list the steps to install the products and fix packs on a Windows Server 2003 Enterprise x64 Edition SP2 with 16 GB RAM. Refer to the official product documentation if you plan to run the same steps on a different operating system.
- Starting from V7.1.1, Tivoli Provisioning Manager also supports the UNIX administrative workstation when installing on the UNIX operating system. However, because not all ISM products support the UNIX administrative workstation, the integration described in the following topics can be obtained only when using a Windows administrative workstation.
- On that server, all prerequisites for installing the two products have already been applied.
- The product images and fix packs to install are available on the system.

Tivoli Provisioning Manager V7.1.1 integrates with the following products and versions:

- IBM Tivoli Change and Configuration Management Database (from now on, CCMDB) V7.1.1.5
- IBM Tivoli Service Request Manager V7.1.0.4
- IBM Tivoli Application Dependency Discovery Manager V7.1.2
- IBM Tivoli Asset Management for IT V7.1.0.5

You can install Tivoli Provisioning Manager 7.1.1 first and then the other products, or the other way around.

Refer to Appendix A, "Miscellaneous upgrade scenarios" on page 671, for information about the following scenarios:

 Integration between Tivoli Provisioning Manager V7.1.1 and IBM Tivoli Asset Management for IT V7.1.0.5.

- ▶ Upgrade to Tivoli Provisioning Manager 7.1.1 and CCMDB V7.1.1.5
- Upgrade to Tivoli Provisioning Manager 7.1.1 and Tivoli Service Request Manager V7.1.0.4

In this chapter we first explain how we installed the environment to run the integration scenarios described in Part 3, "The new GUI and IBM Service Management integration scenarios" on page 135. This environment includes Tivoli Provisioning Manager V7.1.1 installed, on the same system, on top of CCMDB V7.1.1.5 and Tivoli Service Request Manager V7.1.0.4, and Tivoli Application Dependency Discovery Manager V7.1.2 installed on another system.

We also list, for your convenience, the steps to install the following items:

- CCMDB V7.1.1.5 on top of Tivoli Provisioning Manager V7.1.1
- Tivoli Service Request Manager V7.1.0.4 on top of Tivoli Provisioning Manager V7.1.1

If you have already CCMDB V7.1.1 installed in your environment, make sure that you upgrade to FP5 before integrating with Tivoli Provisioning Manager V7.1.1.

If you have already Tivoli Service Request Manager V7.1 installed in your environment, make sure that you first check the latest Tivoli Service Request Manager level installed and then upgrade to FP4 before integrating with Tivoli Provisioning Manager V7.1.1.

Important: It is very important that you follow exactly the sequence of steps listed in the next sections about installing the integrated environment to avoid mismatches or conflicts among versions.

4.2 Steps to install and set up the environment to run integration scenarios

Here is the main sequence of steps that we followed to set up and install the following products in our environment:

- 1. CCMDB V7.1.1 plus fix pack 5
- 2. Tivoli Application Dependency Discovery Manager V7.1.2 plus fix pack 1
- 3. Tivoli Service Request Manager V7.1 plus fix pack 4
- 4. Tivoli Provisioning Manager V7.1.1
- 5. Tivoli Integration Composer V7.1.1 plus fix pack 4

Refer to the official product documentation for these products to run a backup of your installation steps when advisable.

Step 1: Install CCMDB V7.1.1 middleware

From the Change and Configuration Management Database launchpad, start the Tivoli middleware installer to install and automatically configure new instances of DB2, IBM Tivoli Directory Server, and WebSphere Application Server.

Note: When the middleware installation completes, if you want CCMDB and Tivoli Application Dependency Discovery Manager to use as authenticator the same Tivoli Directory Server just installed, do the following actions:

1. Create a Tivoli Application Dependency Discovery Manager.ldif file like the following example:

```
dn: cn=administrator,ou=users,ou=SWG,o=IBM,c=US
uid: administrator
userPassword: collation
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: top
title: TADDM Administrator
sn: administrator
cn: administrator
```

2. Load the file to the Tivoli Directory Server using the 1dapadd command.

In our environment, we skipped this step because, for Tivoli Application Dependency Discovery Manager, we used the default file-based user registry.

Step 2: Install Tivoli Application Dependency Discovery Manager V7.1.2 on a separate machine

Run a simple Tivoli Application Dependency Discovery Manager installation.

When we installed our environment, we selected the following options:

- Install the DB2 database on the local system.
- Select Tivoli Application Dependency Discovery Manager Domain Server as server type to install.
- Select the default file-based user registry for security.
- Do not select to start the server after installation.

Note: If you plan to use as authenticator the Tivoli Directory Server installed with the CCMDB middleware, you must:

- 1. Run a Tivoli Application Dependency Discovery Manager advanced installation.
- 2. Select LDAP User Registry as user registry.
- 3. Point to the Tivoli Directory Server on the Change and Configuration Management Database server.

After the installation completes, you can double-check that Tivoli Application Dependency Discovery Manager is properly installed, as follows:

- 1. Start Tivoli Application Dependency Discovery Manager.
- 2. Go to the Tivoli Application Dependency Discovery Manager interface at the following URL:

```
http://<Tivoli Application Dependency Discovery Manager_fully
qualified_hostname>:9430
```

3. Log on as administrator user to ensure that you can launch the product console.

Step 3: Complete CCMDB V7.1.1 installation

First of all, ensure that both CCMDB middleware and Tivoli Application Dependency Discovery Manager are up and running.

Then, from the CCMDB launchpad, select **Install Change and Configuration Management Database** to start the Base Services installation.

When we installed our environment, we selected the following options:

- Choose to import configuration settings information from the previously installed middleware.
- Provide the installed Tivoli Application Dependency Discovery Manager configuration information when requested.
- Choose to automate database and WebSphere configurations.

After the installation completes, to double-check that the CCMDB is properly installed, you can log on to the CCMDB interface at the following URL:

```
http://<fully qualified_hostname>/maximo
```

Step 4: Upgrade CCMDB to fix pack 5

Follow the instructions provided in the fix pack readme file and run the installation.

Step 5: Install Tivoli Service Request Manager V7.1

First of all ensure that CCMDB middleware is up and running.

- 1. Stop Maximo applications as follows:
 - a. Log on to the WebSphere Application Server console at the URL:

http://<fully qualified_hostname>:9060/ibm/console

- b. Navigate to Applications \rightarrow Enterprise Applications.
- c. Select MAXIMO and MAXIMOHELP, and click the Stop button.
- d. Log out from the WebSphere Application Server console.
- 2. From the Tivoli Service Request Manager launchpad, select **Install Service Request Manager** to start the installation.

When we installed our environment, we selected to install the following components:

- Service Request Manager Search
- Service Desk
- Service Catalog

Note: Before installing Tivoli Service Request Manager fix pack 4, check the date of the latest level of Tivoli Service Request Manager V7.1 installed on your system. Follow these steps to check it:

1. Log on to the Tivoli process automation engine user interface at the following URL:

http://<fully qualified hostname>/maximo

- 2. Click Help and then select System Information.
- 3. In the **System Information** panel, look for the Service Request Manager Service Request Management entry among the Versions listed.

The time stamp of that entry with format yyyymmddD represents the latest level applied of the Tivoli Service Request Manager product.

Step 6: Install Tivoli Service Request Manager fix pack 4

Follow the instructions provided in the fix pack readme file and run the installation.

Step 7: Upgrade WebSphere Application Server to fix pack 23

You must upgrade the WebSphere Application Server if the version installed is lower than 6.1.0.23.

Follow the instructions provided in the fix pack readme file and run the installation.

Step 8: Run Tivoli Provisioning Manager V7.1.1 pre-installation steps

Make sure that you review and run the following steps before starting to install Tivoli Provisioning Manager V7.1.1:

- 1. Only if you installed a level of Tivoli Service Request Manager V7.1 sooner than March 2009, then run the following steps:
 - a. Open a DB2 command window:

db2cmd

b. Set the DB2 instance:

set db2instance=ctginst1

c. Connect to the maxdb71:

db2 connect to maxdb71 user maximo using password <maximo password>

d. Update the CTRLCONDITION table as follows:

update CTRLCONDITION set CTRLCONDITIONID=99999200 where CTRLCONDITIONID=200;

update CTRLCONDITION set CTRLCONDITIONID=99999201 where CTRLCONDITIONID=201;

2. Run these steps to ensure that configuration changes are applied to the Maximo database and to drop any temporary table.

Note: Run these steps to see if there are temporary tables to drop:

1. Open a DB2 command window:

db2cmd

2. Set the DB2 instance:

set db2instance=ctginst1

3. Connect to maxdb71:

db2 connect to maxdb71 user maximo using password <maximo_password>

4. Run the following command to list existing temporary tables, if any:

```
db2 select count * from sysibm.systables where name like 'XX%' and creator='MAXIMO'
```

a. Stop the MXServer by running this command:

%WAS_HOME%\profiles\ctgAppSrv01\bin\stopServer.bat MXServer -username wasadmin -password <wasadmin password>

b. Open a command prompt on the CCMDB system and issue the following commands:

cd C:\IBM\SMP\maximo\tools\maximo configdb.bat restorefrombackup.bat dropbackup.bat dropbackup.bat

Attention: Run the dropbackup.bat *twice* to ensure that there are no more changes to apply.

c. Restart the MXServer by running:

%WAS_HOME%\profiles\ctgAppSrv01\bin\startServer.bat MXServer

- 5. Stop Maximo applications as follows:
 - a. Log on to the WebSphere Application Server console at the URL:

http://<fully qualified_hostname>:9060/ibm/console

- b. Navigate to Applications \rightarrow Enterprise Applications.
- c. Select MAXIMO and MAXIMOHELP, and click the Stop button.
- d. Log out from the WebSphere Application Server console.

Step 9: Install Tivoli Provisioning Manager V7.1.1

Refer to "Tivoli Provisioning Manager V7.1.1 installation" on page 68 to install the following Tivoli Provisioning Manager parts:

- Only the Web Replay component among the Base Services
- Core Components
- Web Components

After the installation completes, you can do the following steps to double-check that Tivoli Provisioning Manager is properly installed:

1. Log on to the Tivoli Provisioning Manager User Interface at:

https:<fully_qualified_hostname>:9443/maximo

As default administrator userid maxadmin with password maxadmin.

- 2. In the Welcome page, you should see the following Start Centers for the Tivoli Provisioning Manager roles added by the Tivoli Provisioning Manager installation:
 - Automation Package Developer
 - Compliance Analyst
 - Deployment Specialist
 - Provisioning Administrator
 - Provisioning Configuration Librarian

For information about how to use the Tivoli Provisioning Manager V7.1.1 user interface, refer to Chapter 6, "Tivoli process automation engine based user interface" on page 137.

Step 10: Run Tivoli Provisioning Manager V7.1.1 post-installation steps

Run the following steps on the system where you installed CCMDB, Tivoli Service Request Manager, and Tivoli Provisioning Manager:

1. When Tivoli Provisioning Manager installation completes, by default, the SSL port is enabled.

Optionally, you can run the following steps to enable the non-SSL port also:

a. Log on to the WebSphere Application Server console as userid wasadmin at the URL:

https://<fully_qualified_hostname>:9043/ibm/console

- b. Navigate to Environment \rightarrow Virtual Hosts \rightarrow maximo_host \rightarrow Host Aliases.
- c. Click New.

d. Specify the following values:

```
Host Name: *
Port: 80
```

- e. Click OK.
- f. Click Save.
- g. Restart Tivoli Provisioning Manager as follows:

```
%TIO_HOME%\tools\tio.cmd stop <wasadmin> <wasdmin_password>
%TIO_HOME%\tools\tio.cmd start
```

Note: If you notice that Tivoli Provisioning Manager Deployment Engine does not start properly, run the following commands in a command shell:

```
cd "C:\ibm\SMP\maximo\deployment\default"
unzip maximo.ear businessobjects.jar
```

Then copy the businessobjects.jar file into the following directories:

%TIO_HOME%\eclipse\plugins\tpm_pmp\maximoLibs
%TIO_HOME%\lwi\runtime\tpm\eclipse\plugins\tpm_pmp\maximoLibs

As the last step, restart Tivoli Provisioning Manager as follows:

%TIO_HOME%\tools\tio.cmd stop <wasadmin> <wasdmin_password> %TIO_HOME%\tools\tio.cmd start

h. Verify that you can connect to the Tivoli Provisioning Manager user interface using a non-secure connection:

http://<fully_qualified_hostname>/maximo

Step 11: Install Tivoli Integration Composer V7.1.1

IBM Tivoli Integration Composer is the Tivoli application used to transform the data about hardware and software installed on the devices scanned by Tivoli Application Dependency Discovery Manager and import them into a target database. In our scenarios, that target database is the MAXIMO database.

In our environment, we chose to install Tivoli Integration Composer on a different system to save system resources on the main server.

Start the Tivoli Service Request Manager launchpad on the system where you plan to install and select **Install Integration Composer** to start the installation.

During the installation you will be asked to provide the information about the target Tivoli process execution engine database.

Step 12: Upgrade Tivoli Integration Composer to fix pack 4

Follow the instructions provided in the fix pack readme file and run the installation.

Summary of the product components installed

This is a summary of the products installed in our environment after the whole installation has completed:

- On the main server (Windows Server R2 Enterprise x64 Edition SP2):
 - Middleware components, which include:
 - IBM DB2 Enterprise Server Edition v9.5 plus fix pack 3a
 - IBM WebSphere Application Server Network Deployment v6.1 plus fix pack 23
 - IBM HTTP Server v6.1 plus fix pack 23
 - IBM Tivoli Directory Server v6.2 plus interim fix 2
 - Tivoli Change and Configuration Management Database V7.1.1 plus fix pack 5, which includes:
 - Base Services V7.1.1.5
 - Tivoli Service Request Manager V7.1.1 plus fix pack 4, which includes:
 - Service Request Manager Service Desk V7.1.0.4
 - Service Request Manager Service Catalog V7.1.0.4
 - Service Request Manager Search V7.1.0.3
 - Tivoli Provisioning Manager V7.1.1, which includes:
 - Base Services V7.1.1.5
 - Core Components V7.1.1
 - Web Components V7.1.1
- On the Tivoli Application Dependency Discovery Manager server (Windows Server 2003 EE SP2 32-bit):
 - Tivoli Application Dependency Discovery Manager V7.1.2 plus fix pack 1 with its own middleware:
 - IBM DB2 Enterprise Server Edition v9.5 plus fix pack 1
- On the system where Tivoli Integration Composer is installed (Windows Server 2003 EE SP2 32-bit):
 - IBM Tivoli Integration Composer V7.1.1 plus fix pack 4

4.3 Tivoli Provisioning Manager V7.1.1 installation

Now that we have finished our CCMDB, TADDM, and Tivoli Service Request Manager installation, we can proceed with the Tivoli Provisioning Manager V7.1.1 installation. We use the **Custom Installation** type and re-use the middleware and the Base Services that is already installed (except for Web Replay, which was not installed during the CCMDB installation).

Note: For a standalone Tivoli Provisioning Manager V7.1.1 installation (without other IBM Service Management products) on an AIX V6.1 system, you can refer to 17.6, "Tivoli Provisioning Manager Version 7.1.1 installation" on page 559.

Also, if you have problems during installation of Tivoli Provisioning Manager V7.1.1 components described in this chapter, you can refer to 16.2, "Installation troubleshooting" on page 515.

4.3.1 Pre-install Cygwin on the local system

The Tivoli Provisioning Manager core components installer and Web components installer require a fresh installation of Cygwin.

Note: The computer must have only one Cygwin installation. Multiple copies are not supported.

We did not have access to the Internet in our lab environment, so we had to pre-install Cygwin, as follows:

1. Cygwin is pre-installed by downloading and running the setup.exe found on:

http://www.cygwin.com.

Use the **Download Without Installing** option from the setup program, selecting the default packages and the additional packages needed for Tivoli Provisioning Manager, as described in *IBM Tivoli Provisioning Manager 7.1.1, Installation Guide* at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp?to
pic=/com.ibm.tivoli.tpm.ins.doc/install/cins_overview.html

2. Next, select the option **Install from Local Directory**, pointing to the directory where the packages were downloaded. Install all packages found in *setup.ini*, by clicking **Next** for the all categories, as shown in Figure 4-1.

Cygwin Set	up - Select Pa	ackages					
Select Pac Select pa	kages ackages to insta	all			E		
		C Keep C Prev	⊙ Curr (Exp View	Category		
Category	Current	New		B S Size	Pa 📥		
🗆 All 😌 De	efault						
E Acces	sibility 😯 Defa	ult					
🕀 Admin	🚯 Default						
Archiv	re 📀 Default						
🕀 Audio	Default						
⊞ Base	😯 Default						
🕀 Datab	ase 📀 Default						
E Devel	Default						
	E Doc & Default						
•					•		
✓ Hide obso	olete packages						
			< Back	Next >	Cancel		

Figure 4-1 Cygwin installation

The default text will change to **Install**, and all the pre-loaded packages will be installed. In this way you do not need to specify the Tivoli Provisioning Manager packages again.

Note: To install the Tivoli Provisioning Manager V7.1.1, the following new Cygwin package is required (this one is different than the one that was used with the Tivoli Provisioning Manager V5.1.1 installation).

- Category: Python
- Package: All default packages under the category plus the package Urlgrabber.

4.3.2 Base Services install

Base Service installer is used to deploy the Maximo Base Services and the common PMPs (process manager product).

In our IBM Service Management integration scenario, it will install only Toolbox Web Replay V7.1.1, because in our system we have already installed the Base Services from the CCMDB install package. Because CCMDB does not require Toolbox Web Replay V7.1.1, this component was not installed during the CCMDB installation.

Tip: It might be useful, at this stage, to back up your current database and application server configuration. This way, after the Base Services and Web Components installation, if you need to return to the previous state, you can restore this backup. Alternatively, you can use the procedure described in the *IBM Tivoli Provisioning Manager 7.1.1, Installation Guide* to uninstall Base Services and Web Components.

Note: For WebSphere Application Server Network Deployment, ensure that the Cell and all related nodes are actively running.

This means that:

Deployment Manager has to be up and running: Use the following command to start it if necessary:

C:\Program Files\ibm\WebSphere\Appserver\profiles\ctgDmgr01\bin\ StartManager.bat.

The node has to be up and running: Use the following command to start it if necessary:

C:\Program Files\ibm\WebSphere\Appserver\profiles\ctgAppSrv01\bin \startNode.bat.

MXServer has to be down:
 Use the following command to start it if necessary:

C:\Program Files\ibm\WebSphere\Appserver\profiles\ctgAppSrv01\bin \stopServer.bat MXServer -username <user_name> -password <password>. To install the Base Services:

- 1. Logon to an account with system privileges.
- Make sure that the solution installer, if already present on the system, is started. The default installation location is: C:\Program Files\IBM\Common\acsi.

If the solution installer is already installed, start the service *IBM ADE*, if it is not yet up and running.

- 3. Start the launchpad (launchpad.exe in the installation DVD).
- 4. In the Launchpad Navigation panel, click **Custom Installation**. Then, click **Verifying and confirming the prerequisites** and return to the custom installation page.
- 5. Click Install the Base Services.
- 6. Select a language for the installation and click OK (we used English).
- 7. In the Package Summary panel, review the package deployment actions (see Figure 4-2), and then click **Next**.

🗏 IBM Tivoli Base Services					
					Package Summar
:	The The pac	e installer has completed the installer will initiate Change kages to deploy all packages	analysis of the Requests to in s to the target ve	packages associ stall new packag rision.	ated with the offering. es or update currently installed
	Г ^{Рас}	kages Analyzed			
		Package Name	Target Version	Installed Version	Analysis
· · · ·	4	Application Deployment Toolkit	1.0.3	1.0.2	Will update to target version.
		base services Package	7.1.1.5	7.1.1.5	Already deployed at target version.
		IBM Tivoli Maximo Common PMP	7.1.1.5	7.1.1.5	Already deployed at target version.
		WebReplay	7.1.1	Not Installed	Will deploy to target version.
		Maximo Change Process Manager	7.1.1.5	7.1.1.5	Already deployed at target version.
InstallAnywhere					Previous Next

Figure 4-2 Package Summary panel

8. From the Run Configuration Step panel, select an option to perform the configuration to deploy the application files (see Figure 4-3) and then click **Next**.

🖳 IBM Tivoli Base Services	
	Run Configuration Step
	 The following options are independent choices. You can choose to run the configuration step now or to run it manually after the install is complete. The configuration step includes database configuration, application server configuration and the installation of process managers. Perform installation configuration now Copy files now, and perform installation configuration later, manually You can choose to deploy enterprise archive (EAR) files during this installation, or defer it until later. Deferring improves performance when there are other product files that get compiled into the EAR files. Deploy application files automatically Deploy application files manually later
InstallAnywhere	
<u>C</u> ancel	Previous Next

Figure 4-3 Run Configuration panel

9. In the Input Summary panel, review the information (see Figure 4-4), and then click **Next**.



Figure 4-4 Input Summary panel

10. The Pre-Installation Summary panel, review the information (see Figure 4-5), and then click **Install**.

堰 IBM Tivoli Base Services	
	Pre-Installation Summary
	Please review the following before continuing:
:= :	Product Name: IBM Tivoli Base Services
	Install Folder: C:\ibm\SMP
InstallAnwhara	
<u>Cancel</u>	Previous Install

Figure 4-5 Pre-Installation Summary

11. From the Install Complete panel, click **Done**.

The Base services Installation (Web Replay 7.1.1) is now completed.

4.3.3 Tivoli Provisioning Manager core components

Tivoli Provisioning Manager core components are installed by using Tivoli Provisioning Manager Core Components Installer. It is used for installing the following components:

- ► Tivoli Provisioning Manager engines and runtime
- SDI management servers (Common Agent Services, Dynamic Content Delivery, device manager service)
- Tivoli Provisioning Manager for OS Deployment
- Tivoli Provisioning Manager IBM Tivoli Monitoring agent
- IBM DB2 client

Also, it performs the following tasks:

- 1. Performs registration of Tivoli Provisioning Manager with Agent Manager.
- 2. Creates WebSphere Application Server profile for Common Agent Services (CAS).
- 3. Performs Secure Sockets Layer (SSL) configuration.
- 4. Calls silently all component installers and performs the configuration steps required.

The core components must be installed on the provisioning server. To install the core components, follow these steps:

- 1. Start the launchpad.
- 2. In the launchpad navigation pane:
 - a. Click Custom Installation.
 - b. Scroll down to 3. Install Tivoli Provisioning Manager core components and click Verify core components installation prerequisites.
 - c. After verifying and confirming the prerequisites, return to the custom installation page.
- 3. Click Install core components.
- 4. Select the language for the installation and click **OK**.
- 5. In the Welcome panel, click Next.
- 6. Accept the license agreement and click Next.
- In the Topology Configuration panel, specify all required fields and click Next. See Figure 4-6.

TBM	Topology Configuration
121TL.	Database Information
	Select the type of relational database available in your environment. Select remote database check box if you are using remote database
	© IBM DB2
	O Oracle Database
	Use Remote Database
	LDAP Directory Server Information
	Select the type of LDAP directory available in your environment.
	© Tivoli Directory Server
	O Microsoft Active Directory
	The maxadmin user exists in the LDAP repository
	Middleware Installer Workspace Information
	Select the check box if you want to import data from Middleware Installer Workspace and enter the workspace location.
	☑ Import data from Middleware Installer workspace
	Middleware Installer workspace directory
	C:libmttivoliumwitworkspace
	Browse
	Select this option if you are using service IP addresses and host names for the computers in your installation, for example, in an HADR environment. The host names that you specify in this installer must
InstallObjeld	
instalishield	
	< <u>B</u> ack <u>Next></u> <u>C</u> ancel

Figure 4-6 Topology Configuration panel

8. In the Select Components panel, select the components to install and click **Next**.

We did not install the following components:

- Cygwin (because it was previously installed manually)
- Tivoli Provisioning Manager for OS Deployment
- IBM Tivoli Monitoring Agent

See Figure 4-7 and Figure 4-8 for further details.

	Select Components
IBM.	Select the components to install. You should only clear an option if
	 It is identified as an optional component. Optional components can be installed separately after installation
	 You are trying to recover from a failed installation, and components before the failure point were successfully installed and configured. See the Tivoli Provisioning Manager Installation Guide for specific recovery steps.
	Cygwin
	Installs Cygwin, a UNIX-like environment for Windows that is used by the provisioning server.
and the second second	☑ Back Up Database and WebSphere Application Configuration
	Backs up the local database server and WebSphere Application configuration for recovery in case of installation failure. If using a remote database server, you must back it up manually before starting the core components installation.
	☑ Tivoli Provisioning Manager engines
	Installs the Tivoli Provisioning Manager engines.
	☑ Agent Manager
	Installs the agent manager server. This core component handles software distribution and secure connections with managed computers where the common agent is installed.
	Tivoli Provisioning Manager for Dynamic Content Delivery
	Installs the dynamic content delivery management center. This core component provides centralized control
InstallShield	
	< <u>B</u> ack <u>N</u> ext > <u>C</u> ancel

Figure 4-7 Select Components panel - 1/2

TBV	Select Components
1211.	Backs up the local database server and WebSphere Application configuration for recovery in case of installation failure. If using a remote database server, you must back it up manually before starting the core components installation.
	☑ Tivoli Provisioning Manager engines
	Installs the Tivoli Provisioning Manager engines.
	☑ Agent Manager
	Installs the agent manager server. This core component handles software distribution and secure connections with managed computers where the common agent is installed.
and the second	✓ Tivoli Provisioning Manager for Dynamic Content Delivery
	Installs the dynamic content delivery management center. This core component provides centralized control of the upload, replication, and download of files in distributed locations.
and the second	☑ Tivoli Provisioning Manager for Job Management Service
	Installs the job management service federator. This core component acts as a federated server that manages job distribution.
	Tivoli Provisioning Manager for OS Deployment (optional)
	Installs software for deployment of operating systems.
	IBM Tivoli Monitoring Agent (optional)
	Installs an agent for monitoring activity on the provisioning server. IBM Tivoli Monitoring (purchased separately) must be installed to use the agent.
InstallShield	
	< <u>B</u> ack <u>N</u> ext > <u>C</u> ancel

Figure 4-8 Select Components panel - 2/2

9. In the Directories for Core Components panel, specify all required fields (see Figure 4-9) and click **Next**.

TRM	Directories for Core Components	
	Enable support for Federal Information Processing Standard (FIPS) 140-2	
	This option is disabled if you install Tivoli Provisioning Manager for OS Deployment or the Tivoli monitoring agent.	
	Specify the directory where you have placed the downloaded installation images, or where you want the installer to copy the images from the installation DVDs.	
	C:\images\TPM711_U2817\TPM_v711]
	Browse	
	Copy installation images from DVDs	
	Specify the directory for temporary files	
	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp	1
	Browse	
	* Backup Files Location (On UNIX and Linux, it must have 755 permissions)	
	Specify the directory for installation backup data. This data is used to restore the application server and the database in case you need to receiver form failed back controls or Web components installation.	
	Catabase in case you need to recover non-naned base services of web components instantation.	-
		4
InstallShield		
	< <u>B</u> ack <u>N</u> ext > <u>C</u> ancel	

Figure 4-9 Core Components panel

10. In the DB2 Configuration panel, specify all required fields (see Figure 4-10) and click **Next**. The values must match the values that you specified during the CCMDB middleware installation.

	DB2 Configuration
LDM.	IBM DB2 has been selected as the relational database for storing data. Provide the information necessary to access the installed version of IBM DB2. Click Next to continue with the installation.
	* Fully-Qualified Domain Name or IP Address of the IBM DB2 server. An example of a fully-qualified domain name is database.example.com.
	nc117218.romelab.it.ibm.com
	* DB2 Server Instance Port Number
	50005
	* Database Name for the IBM Tivoli Provisioning Manager database
	MAXDB71
and the second second	* DB2 Server Instance Owner
	db2admin
	* DB2 Server Instance Owner Password
and the second	
	* Confirm Password
	Select this option to allow the Tivoli Provisioning Manager installer to configure your DB2 instance.
	☑ Use Tivoli Provisioning Manager recommended instance configuration
	Select this option to allow the Tivoli Provisioning Manager installer to configure your database.
	Se Twoil Provisioning wanager recommended database conliguration
	* DB2 Server User Name
	Imaximo
	* DB2 Server User Password
	* Confirm Password

Figure 4-10 DB2 Configuration panel

11. In the WebSphere Application Server Network Deployment Configuration panel, specify all required fields and click **Next.** See Figure 4-11.

	WebSphere Application Server Network Deployment Configuration
IBM.	Wah Pahara Application Contex Matural Deployment Configuration
	Websphere Application Server Network Deproyment Configuration
	* Installation Directory
	C:\Program Files\IBM\WebSpheretAppServer
	* Fully-Qualified Domain Name of WebSphere Application Server
	nc117218.romelab.it.ibm.com
	* Cell Name
	ctgCell01
	* WebSphere Deployment Manager Profile Name
	ctgDmgr01
	* Application Server Node Name
	ctgNode01
	* Application Server Profile Name
	ctgAppSrv01
	* Server Name
	MXServer
	* Deployment Manager Administrator User
	wasadmin
	* Denloyment Monager Administrator Paceword
	t Canfine Descurred
	* Deployment Manager Port
	1001.3
InstallShield	
	< Back Next > Cancel

Figure 4-11 WebSphere Application Server Network Deployment Configuration panel

In Figure 4-11, the fields that are shown in a box were filled in manually. All other fields are taken from the deployment plan created in the workspace directory at middleware installation time.

12.On the LDAP Server Configuration panel, specify all required fields (see details in Figure 4-12), and click **Next**.

TEM	LDAP Server Configuration
±2/275+	Provide your LDAP information and click Next to continue.
	* Fully-Qualified Domain Name or IP Address. An example of a fully-qualified domain name is Idapserver.example.com.
	nc117218.romelab.it.ibm.com
	Host Public Port
	389
	* User Base DN
	ou=users,ou=SWG,o=IBM,c=US
	* Instance Administrator User ID
	maxadmin
	* Instance Administrator Password

AP 5.	* Confirm Password

	Select this option if you want to use the Distinguished Name of LDAP Binding User
	*LDAP Dinging Llogr Name
	t L DAR Binding Lloor Boogward
	t Canfirm Descurard
	+ Linear Lance (Hither Generation with a set)
	* Oser Logon Name Attribute (for example, uid or cn)
	User search filter (for example, (&(uid=%v)(objectclass=inetOrgPerson)))
	(&(uid=%v)(objectclass=inetOrgPerson))
InstallShield	
	< Back Next > Cancel

Figure 4-12 LDAP Server Configuration panel
13. In the IBM Tivoli Provisioning Manager Configuration panel, specify all required fields and click **Next**. For further details, see Figure 4-13 and Figure 4-14.

	IBM Tivoli Provisioning Manager Configuration	
IBM.	Fill in the following information for IPM Tixeli Provisioning Manager installation	
	Specify the destination directory for IBM Tivoli Provisioning Manager.	
	C:\Program Files\IBM\tivoli\tpm	
		Browse
and the second		
	C:\Program Files\IBM\tivoli\tpm\repository	
		Browse
and the statements	* tioadmin Password. The tioadmin user will be created if it does not exist.	

	* Verify tioadmin Password	
and the	*****	
	* Management IP Address	
	Intel(R) PRO/1000 MT Network Connection: 9.168.117.218	-
	* Software Distribution Infrastructure Server SSI Port	
	9045	
- 14	* Software Distribution Infrastructure Client SSL Port	
	9046	
	* Software Distribution Infrastructure Server Non-SSL Port	
	9080	
	* Tivoli Provisioning Manager SSL Port	
	9443	
	* Tivoli Provisioning Manager SSL Keystore Name	
	tpmKeyStore.jks	
	* Tibeli Duminimin a Managam OOL Manatana Desamand	•
InstallShield		
	< Back Nevt >	Cancel
	- Back Next	

Figure 4-13 Tivoli Provisioning Manager Configuration panel 1/2

7775.2	IBM Tivoli Provisioning Manager Configuration		
LDM.	* Software Distribution Infrastructure Server SSL Port		
	9045		
	* Software Distribution Infrastructure Client SSL Port		
	9046		
	* Software Distribution Infrastructure Server Non-SSL Port		
	9080		
	* Tivoli Provisioning Manager SSL Port		
	9443		
	* Tivoli Provisioning Manager SSL Keystore Name		
and the statements	tpmKeyStore.jks		
	* Tivoli Provisioning Manager SSL Keystore Password		

and the second	* * Confirm Password		
and the second s	*******		
	* * Tivoli Provinianing Managar SSL Trustetara Nama		
	tomTrustStore.iks		
	tripli Dravisioning Manager CCI. Trustatore Descurred		
	* Tivon Provisioning Manager SSL Truststore Password		
	t Our fam. De comment		
	* Confirm Password		
	* Your company name (This name will be used for Tivoli P	rovisioning Manager Certificate)	
	Agents will connect to agent manager using		
	Agent Manager Fully Qualified Domain Name		
	O Agent Manager IP Address		_
la ete ll'Objected			
installShield			
		< <u>B</u> ack <u>N</u> ext >	<u>C</u> ancel

Figure 4-14 Tivoli Provisioning Manager Configuration panel 2/2

14.On the WebSphere Profile Configuration for Agent Manager panel, accept all the defaults values and click **Next**.

15.On the Agent Manager Configuration panel, specify all required fields and click Next. For further details, see Figure 4-15 and Figure 4-16.

TRM	Agent Manager Configuration
	Provide the necessary information for agent manager installation and registration and click Next to continue.
	Agent Manager Install Directory
	C:\Program Files\IBM\AgentManager
	Proven
	Diowse
	* Agent Manager Fully Qualified Domain Name
	* Registration Port
	* Secure Port
	Public Port
	* Registration Password
	* Confirm Registration Password
	* Agent Manager Password
	* Confirm Agent Manager Password
	* Security Domain
	romelab.it.ibm.com
	* Agent Manager IP Address
	9.168.117.218
etallShield	
natalionielu -	

Figure 4-15 Agent Manager Configuration panel - 1/2

	Agent Manager Configuration
IBM.	
	nc117218.romelab.it.ibm.com
	* Registration Port
	9511
	* Secure Port
	9512
	* Public Port
	9513
	* Registration Password

	t Oranfara Deviatorian Decement
	Contirm Registration Password
and the second second	* Agent Manager Password
and the second	******
	* Confirm Agent Manager Password

	* Security Domain
	romelab.it.ibm.com
	* Agent Manager IP Address
	9.168.117.218
	* Resource Manager User Name
	liprimanager
	* Resource Manager Password

Figure 4-16 Agent Manager Configuration panel - 2/2

16.On the Dynamic Content Delivery Configuration panel, leave the default values and click **Next**.

17.. Review the summary of your installation settings and click **Next.** In our installation, the Summary panel looks like Figure 4-17 and Figure 4-18.



Figure 4-17 Installation Preview -1/2

TOM	Installation Preview			
1 <i>01</i> 11.	Server Name = MXServer Deployment Manager Administrator User = wasadmin Deployment Manager Port = 8879			4
	LDAP Server Configuration LDAP Host Name or IP Address = nc117218.romelab.it.ibm. LDAP Host Port = 389 LDAP Binding User Name = cn=root User Logon Name Attribute (for example, uid or cn) = uid User search filter (for example, (&(uid=%v)(objectclass=inet((&(uid=%v)(objectclass=inetOrgPerson)) IBM Tivoli Provisioning Manager Configuration Installation Directory = C:Program Files/IBM/tivolity Management IP Address = 9 168.117.218	.com OrgPerson))) = pm\repository		
	Software Distribution Infrastructure Server SSL Port = 9045 Software Distribution Infrastructure Client SSL Port = 9046 Software Distribution Infrastructure Server Non-SSL Port = 90 Tivoli Provisioning Manager SSL Port = 9443 Tivoli Provisioning Manager SSL Keystore Name = tpmKeyS Tivoli Provisioning Manager SSL Truststore Name = tpmTrus Your company name (This name will be used for Tivoli Provis Agents will connect to agent manager using = Agent Manager	080 tore.jks stStore.jks sioning Manager C er Fully Qualified D	ertificate) = IBM Iomain Name	
	Agent Manager Configuration Agent Manager Fully Qualified Domain Name = nc117218.ro Agent Manager IP Address = 9.168.117.218 Agent Manager Registration Port = 9511 Agent Manager Public Port = 9513 Agent Manager Secure Port = 9512 Resource Manager User Name = tpmManager	omelab.it.ibm.com		
	Dynamic Content Delivery Configuration Dynamic Content Delivery Installation Directory = C:Program Tivoli Provisioning Manager for Job Management Service C Device Manager Installation Directory = C:Program Files/IBM	n Files\IBM\tivoli\CL <u>Configuration</u> A\DeviceManager)S	
InstallShield				
		< <u>B</u> ack	<u>N</u> ext ≻	<u>C</u> ancel

Figure 4-18 Installation Preview - 2/2

18. When the installation is complete, click **Finish**.

As a result, the following software has been installed:

- ► Tivoli Provisioning Manager engines
- The Agent Manager
- Tivoli Provisioning Manager for Dynamic Content Delivery
- Tivoli Provisioning Manager for Job Management Service

4.3.4 Tivoli Provisioning Manager Web components

Tivoli Provisioning Manager Web components are installed by Tivoli Provisioning Manager Web Component Installer that deploys Change PMP, Change PMP fix packs, Base Services and Common PMP fix packs, ifixes, hot fixes, and Tivoli Provisioning Manager PMP.

This is the list of Process Solution Installers (PSIs) deployed during the Web components installation:

- MBS_7115_LAFIX.zip
- TPM_PSI_Package.zip
- change_pmp_7.1.1.5.zip (enable non-English languages)
- ToolboxWebReplayPackage_7.1.1.zip (enable non-English languages)

You must install the Web components on the same computer on which you installed the base services, either the provisioning server or the administrative workstation.

To install the Web components, follow these steps:

- 1. Start the launchpad.
- 2. In the launchpad navigation pane, click **Custom Installation** and click **Install Tivoli Provisioning Manager Web components**.
- 3. In the Welcome panel, click Next.
- 4. Accept the license agreement and click Next.
- 5. In the Process Solution Installer Packages Installation panel, specify all required fields and click **Next**. See Figure 4-19.

IBM Tivoli Provisioning Manager 7.1.1 Web components will be installed. Provide the required information.
* Database User ID
[maximo
* Database Password

* Confirm Password
* WebSphere Application Server Administrative User Name
 wasadmin
* WebSphere Application Server Password
++++++++
* Confirm Password
* WebSphere Application Server Remote Access User Name. If WebSphere Application Server is on a Windows system use Administrator, otherwise use tioadmin.
Administrator
*WebSphere Application Server Remote Access Password

* Confirm Password

* Base Services Installation Directory
C:NBMISMP
Browse
Divide

Figure 4-19 Solution Installer Packages Installation panel

6. In the Installation Preview panel, review your installation settings, and then click **Next**. See Figure 4-20.



Figure 4-20 Installation Preview panel

7. When the installation is complete, the Installation Summary panel is displayed. Click **Finish**. The Web components are now installed.

4.4 Other samples of integrated environments

In our environment, we chose to install, on the same system, Tivoli Provisioning Manager V7.1.1 on top of CCMDB and Tivoli Service Request Manager, but, as we have mentioned, you can also decide to install Tivoli Provisioning Manager V7.1.1 first and then CCMDB and Tivoli Service Request Manager.

In this section we give you the high level instructions to do the following tasks:

- "Installing CCMDB on top of Tivoli Provisioning Manager V7.1.1" on page 92
- "Installing Tivoli Service Request Manager on top of Tivoli Provisioning Manager 7.1.1" on page 97

4.4.1 Installing CCMDB on top of Tivoli Provisioning Manager V7.1.1

Here is the sequence of steps to follow to install CCMDB on top of Tivoli Provisioning Manager V7.1.1.

We assume that you already installed Tivoli Provisioning Manager V7.1.1 on your system, as described in "Tivoli Provisioning Manager V7.1.1 installation" on page 68.

Step 1: Run CCMDB V7.1.1 pre-installation steps

Run the following steps on the system where you installed Tivoli Provisioning Manager:

1. When Tivoli Provisioning Manager installation completes, by default, the SSL port is enabled.

Optionally, you can run the following steps to enable the non-SSL port also:

a. Log on to the WebSphere Application Server console as userid wasadmin at the URL:

https://<fully qualified hostname>:9043/ibm/console

- b. Navigate to Environment \rightarrow Virtual Hosts \rightarrow maximo_host \rightarrow Host Aliases.
- c. Click New.
- d. Specify the following values:

Host Name: * Port: 80

- e. Click OK.
- f. Click Save.

g. Restart Tivoli Provisioning Manager as follows:

```
%TIO_HOME%\tools\tio.cmd stop <wasadmin> <wasdmin_password>
%TIO_HOME%\tools\tio.cmd start
```

h. Verify that you can connect to the Tivoli Provisioning Manager user interface using a non-secure connection:

http://<fully qualified hostname>/maximo

2. Stop Tivoli Provisioning Manager as follows:

%TI0_HOME%\tools\tio.cmd stop <wasadmin> <wasdmin_password>

3. Start WebSphere Application Server as follows:

startManager.bat
startNode.bat

Attention: Keep the MXServer stopped.

4. As Administrator, run these steps to ensure that configuration changes are applied to the Maximo database and to drop any temporary tables.

Note: These are the steps to run to see if there are temporary tables to drop:

1. Open a DB2 command window:

db2cmd

2. Set the DB2 instance:

set db2instance=ctginst1

3. Connect to the maxdb71:

db2 connect to maxdb71 user maximo using password <maximo_password>

4. Run the following command to list existing temporary tables, if any:

```
db2 select count * from sysibm.systables where name like 'XX%' and creator='MAXIMO'
```

a. Open a command prompt on the CCMDB administrative system and issue the following commands:

cd C:\IBM\SMP\maximo\tools\maximo configdb.bat restorefrombackup.bat dropbackup.bat dropbackup.bat **Important:** The **dropbackup.bat** is run twice to ensure that there are no more changes to apply.

b. Optionally, you can restart the MXServer by running:

%WAS_HOME%\profiles\ctgAppSrv01\bin\startServer.bat MXServer

Then log into Tivoli Provisioning Manager user interface to check that all steps were correctly run up to this point.

- 5. Stop Maximo applications as follows:
 - a. Log on to the WebSphere Application Server console at the URL:

http://<fully qualified_hostname>:9060/ibm/console

- b. Navigate to Applications \rightarrow Enterprise Applications.
- c. Select MAXIMO and MAXIMOHELP, and click the Stop button.
- d. Log out from the WebSphere Application Server console.
- 6. Stop the IBM Tivoli Provisioning Manager light weight infrastructure: %TI0_HOME%/1wi/bin/1wistop.bat

Step 2: Install CCMDB V7.1.1

Run the following steps to install CCMDB V7.1.1:

1. From a command prompt, run:

set SKIPCHANGEPMP=yes

- 2. From the same command prompt, run the CCMDB installation as follows:
 - a. Run **install.exe** from the <binary_directory>\CCMDB directory to start the installer.
 - b. Choose the option, Upgrade to CCMDB.
 - c. When requested, provide Tivoli Application Dependency Discovery Manager server information.
 - d. Make sure that you select Do not run the configuration now.
 - e. When the installation completes, ignore the following error displayed in the GUI:

CTGIN2371E: The installation is finished, but some serious errors occurred during the install.

f. Exit the installer GUI.

3. Copy all files in:

C:\IBM\SMP\maximo\tools\maximo\mxintegration\taddm

into:

 $\label{eq:c:libm} maximo\applications\maximo\meaweb\webmodule\WEB-INF\MeaRegistrationFiles\taddm$

Note: You might need to create the destination directory.

- 4. Update the SyncTADDMLaunchEntries.xml file that was copied as follows:
 - a. Modify all occurrences of *\$taddmWebLaunchHostname\$* with your Tivoli Application Dependency Discovery Manager server fully qualified host name.
 - b. Modify all occurrences of *\$taddmWebLaunchPort\$* with Tivoli Application Dependency Discovery Manager Web Port = 9430.
 - c. Modify all occurrences of *\$taddmServerPort\$* with Tivoli Application Dependency Discovery Manager server port = 9530.
- 5. From the same command prompt from where you originally started the CCMDB installation, run the command:

<ccmdb_install_directory>\scripts\taskrunner CONTINUE STOPONERROR

Step 3: Install CCMDB V7.1.1 fix pack 5

1. Stop the MXServer by running the command:

%WAS_HOME%\profiles\ctgAppSrv01\bin\stopServer.bat MXServer -username wasadmin -password <wasadmin_password>

2. Follow the instructions provided in the fix pack readme file and run the installation.

Step 4: Run CCMDB V7.1.1.5 post-installation steps

Run the following steps to complete the CCMDB setup.

- 1. Verify the configuration settings in the WebSphere Application Server Console:
 - a. Log on as wasadmin to the WebSphere Application Server console at the URL:

http://<fully qualified_hostname>:9060/ibm/console

b. Navigate to:

Applications \rightarrow Enterprise Applications \rightarrow MAXIMO \rightarrow Class loading and update.

- c. Ensure that **Single class loader for application** is checked under the WAR class loader policy.
- d. Ensure that **Classes loaded with parent class loader** first is checked under Class loader order.
- e. If you applied any changes, click Save.
- f. Restart the WebSphere Application Server.
- 2. If a non-SSL port is not required, you can optionally disable it as follows:
 - a. Log on as wasadmin to the WebSphere Application Server administration console:

http://<fully_qualified_hostname>:9060/admin

- b. Select Environment \rightarrow Virtual Hosts \rightarrow maximo_host \rightarrow Host Aliases.
- c. Select the Host Alias with Port Number: 80.
- d. Click Delete.
- e. Click Save.
- f. Restart Tivoli Provisioning Manager as follows:

```
%TIO_HOME%\tools\tio.cmd stop <wasadmin> <wasdmin_password>
%TIO_HOME%\tools\tio.cmd start
```

Note: If you notice that Tivoli Provisioning Manager Deployment Engine does not start properly, run the following commands in a command shell:

```
cd "C:\ibm\SMP\maximo\deployment\default"
unzip maximo.ear businessobjects.jar
```

Then copy the businessobjects.jar file into the following directories:

%TIO_HOME%\eclipse\plugins\tpm_pmp\maximoLibs
%TIO_HOME%\lwi\runtime\tpm\eclipse\plugins\tpm_pmp\maximoLibs

As the last step, restart Tivoli Provisioning Manager as follows:

```
%TI0_HOME%\tools\tio.cmd stop <wasadmin> <wasdmin_password>
%TI0_HOME%\tools\tio.cmd start
```

g. Verify that you cannot connect to the Tivoli Provisioning Manager user interface using a non-secure connection:

http://<fully_qualified_hostname>:80/maximo

4.4.2 Installing Tivoli Service Request Manager on top of Tivoli Provisioning Manager 7.1.1

Here is the sequence of steps to install Tivoli Service Request Manager on top of Tivoli Provisioning Manager 7.1.1.

We assume that you already installed Tivoli Provisioning Manager V7.1.1 on your system as described in "Tivoli Provisioning Manager V7.1.1 installation" on page 68.

Step 1: Run Tivoli Service Request Manager 7.1 pre-installation steps

Run the following steps on the system where you installed Tivoli Provisioning Manager:

1. Stop Tivoli Provisioning Manager as follows:

%TI0_HOME%\tools\tio.cmd stop <wasadmin> <wasdmin_password>

2. Start WebSphere Application Server as follows:

startManager.bat
startNode.bat

Attention: Keep the MXServer stopped.

3. Run these steps to ensure that configuration changes are applied to the Maximo database and to drop any temporary tables.

Note: These are the steps to run to see if there are temporary tables to drop:

1. Open a DB2 command window:

db2cmd

2. Set the DB2 instance:

set db2instance=ctginst1

3. Connect to the maxdb71:

db2 connect to maxdb71 user maximo using password
<maximo_password>

4. Run the following command to list existing temporary tables, if any:

db2 select count * from sysibm.systables where name like 'XX%' and creator='MAXIMO''

a. Open a command prompt on the CCMDB administrative system and issue the following commands:

cd C:\IBM\SMP\maximo\tools\maximo configdb.bat restorefrombackup.bat dropbackup.bat dropbackup.bat

Attention: The dropbackup.bat is run twice to ensure that there are no more changes to apply.

b. Optionally, you can restart the MXServer by running:

%WAS_HOME%\profiles\ctgAppSrv01\bin\startServer.bat MXServer

Then log into the Tivoli Provisioning Manager user interface to check that all steps were correctly run up to this point.

- 5. Stop Maximo applications as follows:
 - a. Log on to the WebSphere Application Server console at the URL:

http://<fully qualified_hostname>:9060/ibm/console

- b. Navigate to Applications -> Enterprise Applications.
- c. Select MAXIMO and MAXIMOHELP, and click the Stop button.
- d. Log out from the WebSphere Application Server console.

Step 2: Install Tivoli Service Request Manager 7.1

Before you begin, ensure that the Tivoli Provisioning Manager middleware is up and running.

From the Service Request Manager launchpad, select **Install Service Request Manager** to start the installation.

Important: Make sure that you install the Tivoli Service Request Manager 7.1 refresh released later than March 2009.

Step 3: Install Tivoli Service Request Manager fix pack 4

Follow the instructions provided in the readme file to install the fix pack and run the installation.

Step 4: Run Tivoli Service Request Manager V7.1.0.4 post-installation steps

Run the following steps to complete the Tivoli Service Request Manager setup:

- 1. Verify the configuration settings in the WebSphere Application Server Console
 - a. Log on as wasadmin to the WebSphere Application Server console at the URL:

http://<fully qualified_hostname>:9060/ibm/console

b. Navigate to:

Applications \rightarrow Enterprise Applications \rightarrow MAXIMO \rightarrow Class loading and update.

- c. Ensure that **Single class loader for application** is checked under WAR class loader policy.
- d. Ensure that **Classes loaded with parent class loader first** is checked under Class loader order.
- e. If you applied any change, click Save.
- f. Restart WebSphere Application Server.
- 2. When Tivoli Provisioning Manager installation completes, by default, the SSL port is enabled.

Optionally, you can run the following steps to enable the non-SSL port also:

a. Log on as wasadmin to the WebSphere Application Server console at the URL:

https://<fully qualified_hostname>:9043/ibm/console

- b. Navigate to Environment \rightarrow Virtual Hosts \rightarrow maximo_host \rightarrow Host Aliases.
- c. Click New.
- d. Specify the following values:

```
Host Name: *
Port: 80
```

- e. Click OK.
- f. Click Save.
- g. Restart Tivoli Provisioning Manager as follows:

```
%TIO_HOME%\tools\tio.cmd stop <wasadmin> <wasdmin_password>
%TIO_HOME%\tools\tio.cmd star
```

Note: If you notice that Tivoli Provisioning Manager Deployment Engine does not start properly, run the following commands in a command shell:

```
cd "C:\ibm\SMP\maximo\deployment\default"
unzip maximo.ear businessobjects.jar
```

Then copy the businessobjects.jar file into the following directories:

```
%TIO_HOME%\eclipse\plugins\tpm_pmp\maximoLibs
%TIO_HOME%\lwi\runtime\tpm\eclipse\plugins\tpm_pmp\maximoLibs
```

As the last step, restart Tivoli Provisioning Manager as follows:

%TIO_HOME%\tools\tio.cmd stop <wasadmin> <wasdmin_password>
%TIO_HOME%\tools\tio.cmd start

h. Verify that you can connect to the Tivoli Provisioning Manager user interface using a non-secure connection:

http://<fully qualified_hostname>/maximo

Customizing Tivoli Provisioning Manager V7.1.1 after installation

In this chapter we provide detailed information for implementing a Software Distribution scenario in a customer environment. We also discuss additional customizations required after a standard installation of Tivoli Provisioning Manager V7.1.1, such as creating a new user by WebSphere Administration Console or creating the Software Distribution Infrastracture. Finally, we implement a simple scenario to validate our Tivoli Provisioning Manager installation by distributing a software package block to a target. If you are new to Tivoli Provisioning Manager, you will find this chapter helpful before proceeding into more complex scenarios with IBM Service Management integration.

We cover the following topics:

- "Customization after Tivoli Provisioning Manager V7.1.1 installation" on page 102
- "Implementing the scalable distribution infrastructure" on page 107
- "Tivoli Provisioning Manager: Software deployment and management" on page 121
- "Launching and configuring the Software Package Editor" on page 122
- Creating and saving a software package block by using SPE" on page 127
- "Distributing software" on page 131

5.1 Customization after Tivoli Provisioning Manager V7.1.1 installation

After the initial installation, you might want to customize the Tivoli Provisioning Manager by adding a new user and (or) a new security group. We start by explaining the security concepts in Tivoli Provisioning Manager V7.1.1.

5.1.1 Security overview

Tivoli Provisioning Manager V7.1.1 makes use of the Tivoli process automation engine security framework, in which it uses WebSphere security services. WebSphere security information specific to Maximo can be found under:

%WAS_HOME%\profiles\ctgDmgr01\config\cells\applications\MAXIMO.ear\depl
oyments\MAXIMO\maximouiweb.war\WEB-INF\web.xml.

Tivoli Provisioning Manager security binaries are packaged in the following locations:

► For user interface configuration:

%WAS_HOME%\profiles\ctgAppSrv01\installedApps\ctgCell01\MAXIMO.ear\b
usinessobjects.jar

► For Web services, there are binaries in two different locations:

```
%TIO_HOME%\lwi\runtime\tpm\eclipse\plugins\tpm_pmp\tpm_pmp_businesso
bjects.jar
```

```
%TIO_HOME%\lwi\runtime\tpm\eclipse\plugins\com.ibm.tivoli.tpm.securi
ty.realm\com.ibm.tivoli.tpm.security.realm.jar
```

The installation of Tivoli Provisioning Manager configures the WebSphere security automatically. The configuration settings can be found by looking at the web.xml file as seen in Example 5-1.

```
Example 5-1 web.xml
```

It can also be checked after logging into Tivoli Provisioning Manager, as follows:

Go To \rightarrow System Configuration \rightarrow Platform Configuration \rightarrow System Properties, type in mxe.useAppServerSecurity under Property Name filter, and click Search.

Global Properties 🛛 🔻	∕ Filter > 🏠 🕴 🛊 🐳 🕴 💠 1 - 1 of 1 🔶			Download ? =		
Prop	perty Name 🗢	Description		Current Value		
mxe.	e.useAppServerSecurity					
🗌 💌 mxe.	e.useAppServerSecurity	Indicates whether Maximo should use app serv		1 🗊		
	G	Global Properties Details				
Property	y Name mxe.useAppServerSecurity	File Override?	Security Level	SECURE P		
Desc	cription * Indicates whether Maximo should use app serv	Global Only?	✔ User Defined?			
Global	al Value 1	Instance Only?	Nulls Allowed?			
Current	t Value 1	Online Changes Allowed?	Data Type	YORN P		
Maximo E	Default 0	Live Refresh?	Domain	<i>م</i>		
		Encrypted?	Masked?			

Figure 5-1 Global properties

5.1.2 Creating a new user or security group and import these into Tivoli Provisioning Manager

You can customize the Tivoli Provisioning Manager by adding a new user or a new security group. In order to do that, start the WebSphere Admin Console by typing the following address in your browser:

https://<fully_ qualified_hostname>:9043/ibm/console/login.do?action=secure

At the Integrated Solutions Console (ISC) prompt, insert user and password (by default, wasadmin is the user).

Note: If the Instance Administration Tool is not already started, ensure that you are logged in as an Administrator on the system and then start the tool:

Windows:

 $\label{eq:Click Programs} \begin{array}{l} \rightarrow \text{ Ibm Tivoli Directory Server 6.2} \rightarrow \text{Instance} \\ \textbf{Administration Tool.} \end{array}$

► UNIX:

Type ./opt/IBM/1dap/V6.2/sbin/idsxinst at the command line.

To create a new user in WebSphere Administrative Console V6.1 using Tivoli Directory Server:

- 1. Go to Users and Groups, and choose to Manage Users.
- 2. Click Search to list existing users in the LDAP.

3. Click **Create**..., fill in all appropriate fields, and submit by clicking **Create**. See Figure 5-2.

Integrated Solutions Console Welcome wasadmin	
View: All tasks	
WelcomeMy Startup Pages	Manage Users
Guided Activities Guided Activities Guided Activities Subscript Activities Guided Activities Subscript Activities Guided Activities Subscript Activities Su	WIM User Management
	Create a User
Resources	*User ID
Security	RedbookUser1 Group Membership
Environment	*First name *Last name
	Redbook User1
Users and Groups	E-mail
Administrative User Roles	test@it.ibm.com
Administrative Group Roles	*Password *Confirm password
Manage Users Manage Groups	•••••
Monitoring and Tuning	Create Cancel
Dispervice integration	
1 Settings	

Figure 5-2 Create user

4. Click **Close** to return to user list, as shown in Figure 5-3.

Manage Users	
WIM User Management	
The user was created successfully.	
RedbookUser1	
Create Like Close	

Figure 5-3 Manage user feedback

Important: Consider that if LDAP is not running, you can get an exception. Verify this before creating the user.

The new user created should now be shown in the user list.

To assign the new user to a security group in WebSphere Administrative Console 6.1 perform these steps:

- 1. Go to **Users and Groups**, and choose to **Manage Users**. Click **Search** to list existing users in the LDAP.
- 2. Select the *user* that you want to assign from the list.
- 3. Click the Groups tab, click Add..., and Search.
- 4. Select the group to which you want to add the user, and click **Add**. See Figure 5-4.

Manage Users	
WIM User Management	
Add a User to Groups	
User ID RedbookUser1	
Specify the search criteria that you want to use to find the groups that you was Search by * Search for Too Search Search	int this user to be a member of.
18 groups matched the search criteria. MAXIMOUSERS PMCHANGEADMIN	
PMCHANGEANALYST PMCHANGEAPPROVER PMCHANGEIMPL PMCHANGEMGR PMCHANGEOWNER PMREQUESTER	
TPADMIN TPCOMPLIANCEANALYST TPCONFIGURATIONLIBRARIAN TPDEPLOYMENTSPECIALIST TPDEVELOPER WB ADMIN DEEMISSION	
Add Close	

Figure 5-4 Adding the new user to a group

5. Click **Close**. The group to which the user has been added is displayed.

In order to view the newly created users and groups in Tivoli Provisioning Manager, you must import them to the system by means of setting up synchronization between the Virtual Member Manager and the system.

For that purpose, use the option, Virtual Member Manager synchronization.

- 1. In Tivoli Provisioning Manager, click Go To \rightarrow System Configuration \rightarrow Platform Configuration \rightarrow Cron Task Setup.
- 2. Type the VMMSync into the Cron Task field and click **Enter**. This opens a tab with the cron task information.
- 3. Activate the Virtual Member Manager synchronization by clicking the **Active** check box.
- To keep the history of all the activities of the VMMSync cron task, check the Keep History check box and type 50 in the Max Number of History Records field. See Figure 5-5.

Cron Task Setup					C Web Replay	Bulletins: (0)	[≫] <u>G</u> o To <mark>Ш</mark> <u>R</u> eports
Find: Select Action	🗹 🖞 🖬 🗶 🌲 🔿						
List Cron Task							
Cron Task VIMMSYNC Invo Class psdi.security.vmm.VIMMSyr Access Level FULL P	kes WebSphere VIMM APIs to populate dat	1					
Cron Task Instances ➤ Filter > ₩ ☆ ↓ ↓ 1 • 1 of 1 →							^{EV} <u>Download</u> ? =
Cron Task Instance Name Schedule VIMMSYNC01 Sm	1	<u>Run as Us</u> MAXADMI	er N P	Active V	Keep History	Max Number of	History Records 50 1
Parameters History						Duplicate	New Row
Cron Task Parameters 🌶 Filter > 🚜 🚍 🛧 🍦 🔶 1 - 5 of 8 👄						[💐 <u>Download</u> ? 🗖
Parameter Credential	Value		Description VMM admin cr	edentials.		1	
▶ GroupMapping	xml version="1.0" encoding="UTF-8" ? <	DO	The USER XML	used by the	VMM task.		
GroupSearchAttribute	cn		VMM search a	ttribute to qu	ery group records.		
Principal	cn=wasadmin,ou=users,ou=SWG,o=IBM,c=	US	VMM admin pri	ncipal.			
SynchAdapter	psdi.security.vmm.DefaultVMMSyncAdapte	r	VMM synchron	nization adap	ter.		

Figure 5-5 Virtual Member Manager synchronization setup

5. To retrieve the user or security name from LDAP correctly, on the **Parameters** tab, click the *Next Page* arrow, select **userMapping**. Change the *displayName* value in the *Value* field from the expression <column name="DISPLAYNAME" type="ALN">displayName<column> to an appropriate attribute value defined in LDAP, such as uid, as in the following expression <column name="DISPLAYNAME" type="ALN">uid<column>.

Tip: For a list of all attributes available in LDAP, see the Person DataObject for user attributes and the Group DataObject for security group attributes.

- 6. Save the changes.
- 7. Restart Tivoli Provisioning Manager for all the imported items to be visible in the system.

The synchronization between Virtual Member Manager and the Tivoli Provisioning Manager is now active.

5.2 Implementing the scalable distribution infrastructure

Scalable distribution infrastructure (SDI) allows you to centrally manage software distribution from Tivoli Provisioning Manager using existing core services:

- Tivoli Common Agent Services (CAS): Provides agent management
- Dynamic Content Delivery (DCD): Provides content distribution
- Device Manager Service (DMS): Provides job distribution

The Tivoli Provisioning Manager installer silently installs the following management elements of the scalable distribution infrastructure on the provisioning server:

- ► The Tivoli agent manager
- ► The device manager federator
- The dynamic content delivery management center

Figure 5-6 shows the SDI Infrastructure.



Figure 5-6 SDI Infrastructure

Note: Refer to 2.2.2, "Tivoli Provisioning Manager V7.1.1 component architecture" on page 27 for a description of these components.

After a successful installation of Tivoli Provisioning Manager V7.1.1, in order to properly set up the distribution elements of the infrastructure, you must perform the following post-installation configuration tasks:

- Install the depot server.
- Install the common agent on the target computers.

5.2.1 Dynamic content delivery service

One of the SDI components is the IBM Tivoli Provisioning Manager for dynamic content delivery (DCD) application, which is a distributed, grid-like service that enables you to efficiently distribute large files around your network.

The dynamic content delivery service comprises a number of components, such as the dynamic content delivery service management center and the depot server. It also uses internal network grouping mechanisms, such as regions and zones.

Tivoli Provisioning Manager uses the following dynamic content delivery service features:

- Scalable design that allows you to add depot servers to accommodate the needs of your network
- Optional peer-to-peer file sharing
- Adaptive bandwidth control: Transfer rates throttled by both depot servers and peers to minimize the impact of downloads on existing network traffic from other applications
- Dynamic Depot Server Selection (DDSS) algorithm: Determines the best depots in which to cache the file, based on the target endpoints
- Message-Digest algorithm 5 (MD5) for file validation
- Advanced Encryption Standard (AES) for data encryption
- Resume-able downloads.
- Parallel downloads from a single depot and multiple peers.
- Load balancing and failover.
- Reports about download activity.
- Event console that displays important events and messages for the administrator

Dynamic content delivery service management center

The management center is the server component that is installed on the same machine as the Tivoli Provisioning Manager by default. It is the all knowing brain of the dynamic content delivery application. It provides centralized control of upload (publish), depot server management, depot server file replication, and client downloads. The management center maintains the catalog of files on peer servers in the network that is used to generate download plans.

Regions and zones

Before you can add a depot server, the region that it belongs to must be defined. Regions are used to group depot servers that are located near one another to optimize upload, replication, and download times. A depot server is manually mapped to a region before its registration. Clients and peer servers are mapped to a region using zones. A depot server can belong to only one region, but a region can have more than one depot server.

It is important to distinguish between regions and zones:

- A region is a geographical grouping of systems (depot servers, peer servers, and clients).
- A zone is an IP range or domain that is used to logically group computers into regions. You can define one or more zones for each region.



See Figure 5-7 for an example of a region.

Figure 5-7 Region example

Depot servers or peers will request to download a file in the following order:

- 1. Exact domain name (peers only)
- 2. IP Zone
- 3. Domain Zone
- 4. Region

Without regions and zones, endpoints connect to depot servers and other peers randomly.

In order to create a region, you must perform these steps:

- 1. Click Go To → Administration → Provisioning → Dynamic Content Delivery Configuration.
- 2. Click the **Regions** tab.
- 3. Click New Row.
- 4. Type a name and a description for the new region. See Figure 5-8.

Dyn	namic Content Delivery Config	uration				Øw	eb Replay 👎 <u>B</u> ulletins: (0)	♠ <u>G</u> o To ^{LLLL} <u>R</u> eports
Select Actio	on 🛛 🖌 🛃 🔶							
List	Depots Regions	Zones						
Regions	🕨 Filter > 🚳 🛛 🗐 🛧 🔶 🔶 1 -	1 of 1 🔶						📴 Download ? 🚍
	Region					Description		
-	Region1					Lazio region		Û
					Region D	etails		
			Region *	Region1				
			Description	Lazio region				
			Minimize traffic?					
			Block incoming requests?					
			Block outgoing requests?					
								New Row

Figure 5-8 Region creation

You can select from the following options:

- Incoming-blocked: This property is used to indicate that depot servers in this region cannot serve files to endpoints outside of the region. Depot exceptions to this can be specified as depot access entries. This property does not apply to peers in this release.
- Outgoing-blocked: This property is used to indicate that endpoints in this region cannot pull from depot servers outside the region. In order for the endpoints in this region to pull the file from depot servers outside the region, depot exceptions have to be specified as depot access entries. The incoming and outgoing blocked properties allow the dynamic content delivery management center to exclude depots from download plans if they cannot be reached by an endpoint or other depot that is trying to perform the download.

Minimize-traffic: This property determines whether traffic should be restricted in and out of the region. It is set to false by default. If the property is set to true, the management center will try to move the file only once into the zone, and all other endpoints in the region will wait to get it from that one source. Endpoints outside of the region will not pull from peer endpoints inside of this region. For depots, this flag is lenient, meaning that a depot server inside this region can be used by endpoints to download a file outside the region if it is the only available depot that has the file. This flag should be set to true (restricted) for all branch office regions. Preferred upload servers should not be in a restricted region. Preferred upload servers should be in an open region so other depot servers can replicate from them.

Note: You can also change these options after you have created the region.

5. Click Save.

Note: Before installing the common agent and the depot server, you might need to change the default polling interval from target computers and depot servers. To reduce network traffic, the default polling interval is set to one hour. You can change the default polling interval to something more appropriate to your needs.

You can change the polling interval in the TCA-Subagent JES configuration template, available in both the Tivoli Common Agent Stack and CDS_Depot_Stack configuration templates.

To change the polling interval:

- 1. Click Go To \rightarrow IT Infrastructure \rightarrow Software Catalog \rightarrow Software Stacks.
- Find the software stack called Tivoli Common Agent Stack or CDS_Depot_Stack and click it.
- 3. Under Configuration Templates, click TCA-JES Default.
- 4. Click the icon for the PollingInterval parameter and type the new interval in the Parameter Value field.
- 5. For example, if you want to set it to ten minutes, enter 00:10.
- 6. Click Save.

Creating a depot

Important: A depot cannot be created on the Tivoli Provisioning Manager server because the depot functionality is provided as a sub-agent of the Tivoli common agent, which is not supported on the Tivoli Provisioning Manager server.

In order to define a new depot server, follow these steps:

- Check the software and hardware prerequisites for the depot server on the IBM InfoCenter. In particular, ensure that you have enough disk space to store the Software Packages that will be distributed. Consider that if you have enabled IPv6 addressing support for the scalable distribution infrastructure, the operating system on depots must be able to communicate appropriately with other computers in your environment. For example, if you have both IPv4 and IPv6 target computers, the depot can be configured to support both IPv4 and IPv6 addressing. If all communication with the depot will use IPv6 addressing, the depot can be configured to support IPv6 only.
- 2. Run a discovery to add the server that hosts the depot into the Data Center Model. To do this:
 - a. Click Go To \rightarrow Discovery \rightarrow Provisioning Discovery \rightarrow Discovery Wizards. Click the List tab.
 - b. Use **Computer Discovery** to perform a network discovery of the computer in your environment where you chose to install the Depot Server.
- 3. Create the region to which the depot is assigned. This is specified when the depot is created. See how to create a region in the "Regions and zones" on page 110.
- From the Tivoli Provisioning Manager V7.1.1 Start Center interface, click Go To → Administration → Provisioning → Dynamic Content Delivery Configuration.
- 5. Click the **Depots** tab.
- 6. Click New Row.
- 7. Type a name for the depot server.
- 8. In the **Region** field, select the region that you have just created. This is the region to which the new depot server will be assigned.
- 9. In the **Computer** field, search for and select the name of the target computer that you want to configure as a depot server. The depot server must not be included in your group. If a new computer is being used, you can add credentials simultaneously.

10. In the IP Address field, specify the IP address of the depot server.

- 11. In the **Fully qualified host name** field, type the fully qualified domain name of the depot server that has already been discovered using the SMB discovery.
- 12. Select the **Install the depot agent services** check box and specify the credentials to install the depot agent services. If you do not select this option, the depot is only added to the data model.
- 13. Select the Preferred upload server check box. If using multiple depot servers, at least one depot must be selected as a preferred upload server.

Depots ▶ Filter > 🛞 📁 🛧 🐳 💠 1 - 1 of 1 →			
Depot	Description		Computer
 nc117175 	depot Rome region		nc117175.romelab.it.ibm.com
		Depot details	
Depot* nc117175	Computer* r	nc117175.romelab.it.ibm.com	
Description depot Rome region	IP Address *	9.168.117.175	Status Active
Region * Region1	P Fully qualified host name *	nc117175.romelab.it.ibm.com	
		Distribution Configuration	
Domain Zone Served Port* 2. Max connections Preferred upload server? Data Directory* dat Data Directory Limit (MB)* 2. Used space (MB)	2000 182	Bandwidth control C Adaptive . High C Static C None	priority 0 KB/s
		Depot Statistics and Files	

14.Leave all of the other default options unchanged. See Figure 5.6.

Figure 5-9 Depot creation page

15.Click Save ...

- 16. If you selected the **Install the depot agent services** check box, a task for adding the new depot server is created. You can click the task name to see details about its status and monitor its progress until the task has completed. Click **Refresh** to see an update on its status.
- 17. The newly added depot server with the specified properties is now listed on the Depots tab. If you want to check the status of a Depot more in detail, you can launch the **Dynamic Content Delivery (DCD) Administration Console**.
- 18. Click Go To \rightarrow Administration \rightarrow Provisioning \rightarrow Dynamic Content Delivery Configuration.
- 19. Click the **Depots** tab.
- 20. From the Select Action drill-down menu, select Start the DCD Console.

The dynamic content delivery administration console provides read-only access to additional information about regions, zones, depot servers, and files. You can also view file transfer information, download plans used during file distribution, and global configuration information. A number of reports are also available, which enable you to filter and display event details, and to obtain additional information about file downloads, an overview of the file traffic, or details about the file traffic per region or zone.

Note: The CDS depot implementation is based on several physical and enterprise criteria. You can find a detailed approach for calculating the number of depots to use in your environment in the *Tivoli Provisioning Manager V7.1: Capacity Planning Cookbook* at:

http://www-01.ibm.com/software/brandcatalog/portal/opal/details?cata
log.label=1TW101070

DCD settings by Command Line Interface

It is possible to create, update, and remove regions, zones, and depots by Command Line instead of using the Web Interface using the following utility:

- "%TIO_HOME%/tools/DcdAdmin/dcdCli.cmd (for Windows)
- "%TI0_HOME%/tools/DcdAdmin/dcdCli.sh (for UNIX/Linux)

The arguments for the scripts are:

- action: Create, update, or delete
- deviceType: tpm-region, tpm-depot, tpm-zone, target-list, and depot-access
- xmlFile: Fully qualified path for the xml file containing the DCD device definitions conforming to dcdAdmin.dtd
- user: The user to initiate the script
- password: Password to authenticate the user initiating the script

For example, you can use the following command to create a region:

Installing the Tivoli Common Agent

When you install the common agent from the provisioning server, the common agent is installed on the managed system with the related TCA-Feature Tivoli Provisioning Manager Base.

Note: Version 1.4.2.0 of the common agent is installed with version 7.1.1 of the provisioning server.

Before installing the common agent, review the "Requirements for common agent installation" available on IBM InfoCenter at the following URL:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp

Note: Installing the common agent on the provisioning server, where the agent manager is also installed, is not supported.

There are two main ways to install the common agent that it hosts:

- Using Tivoli Provisioning Manager
- Outside of Tivoli Provisioning Manager

In this chapter we install a Tivoli common agent using Tivoli Provisioning Manager on one of the Windows systems in our lab. This is done to verify our Tivoli Provisioning Manager V7.1.1 installation and configuration.

Tivoli common agent installation installs the common agent with default options. The following service access points (SAP) are created on the target computer during the common agent installation:

- Agent-Server (IPv4 / CommonAgent)
- SDI-SAP (IPv4/scalable distribution infrastructure)
- RXA-Server (IPv4/RXA)

Note: The RXA SAP is created only if you provide credentials and there is no default SAP assigned to the device. The *TCA.Create.EO.SAP* configuration parameter determines whether the SDI SAP is created as part of the agent installation. This parameter is set to true by default. To modify this parameter, click **Go To** \rightarrow **Administration** \rightarrow **Provisioning** \rightarrow **Provisioning Global Settings** \rightarrow **Variables**.

To install the common agent and subagents:

- 1. Click Go To \rightarrow Deployment \rightarrow Software Management \rightarrow Common Agent Installation.
- 2. Under **Common Agent Stacks**, click the common agent software stack for the task.
- Click Select → Computers and select one or more target computers for the task, then click OK.
- 4. If no default service access points (SSH or RXA) exist on the target computers, select **Create Credentials** and specify the credentials for creating a *Remote Execution and Access (RXA)* service access point on each target computer.
- 5. Click Schedule to schedule the task to run immediately.

- 6. Under Notification, configure the notification settings for the task.
- 7. Click the **Advanced** tab to set the configuration template parameters. See Figure 5-10.

Provis	ioning Task Install Common Agent 1857		
Common Agent Stacks 👂 Filter > 🛝 🗊 🛊 🍦 🗇	1 - 2 of 2 →		Et Download ? =
Stack			
Fivoli Common Agent Stack			
CDS_Depot_Stack			
Selected Targets 🛊 🖕 🐳 1 - 1 of 1 🐳			Et Download ? =
Farget		Description	
nc125095.romelab.it.ibm.com		Computer	×
			Select I 💌
		Create Cradentiale?	
Scheduling			-
lick Schedule to change options.	Sebeduled: New		
	cileadied, now		Schedule
lotification			-
Recipients 🕨 Filter 🛛 🦓 🗐 🛔 🛊 🔶 🗇 4 - 1 of 1 🔶 👘			El Download ? =
Re	cipient		
M M	AXADMIN		×
			Add Recipient Add E-mail
Events 🕨 Filter » 👋 🖽 🛧 🔶 🖘			🕞 Ostariors ? 🚍
Description			
		No rows to display	
			Add Event
			Submit

Figure 5-10 Installation of the Tivoli Common Agent

- 8. Click **Submit**.
- The task will take a while. After it has been successfully executed, you will find the computer entry under Go To → Deployment → Provisioning Computers, and under the column "Agent" you will now see "TCA-1.4.2.0" as shown in Figure 5-11.

Find:	👘 🔻 Select Action 🔽 🚯 🎽	a 214 4 2		
List Computer Hardware	Software Compliance Recommend	ations Credentials Workflows Vari	iables Deployment Properties	
🛱 Advanced Search 🔻 🥃 Save Query	🔹 🖗 Bookmarks			
Computers 🕴 🖉 Filter 🦓 🛱 🎼				B) Download ?
Computer 🗢	Operating System	Globally Unique Identifier	Agent	Compliance Status
nc125095.romelab.it.ibm.com	Windows Server 2003 Enterprise Edition SP2		TCA-1.4.2.0	No compliance checks configured 🛛 🗙 🚳
Select Records				

Figure 5-11 The new Tivoli Common Agent

Enabling and disabling peering

Peer-to-peer file sharing enables you to shift download traffic from the WAN to LANs and it allows reductions in the number of depot servers needed.

If peer-to-peer file sharing is disabled, endpoints can download files only from depot servers.

When peer-to-peer file sharing is enabled, endpoints can download files from endpoint peers as well as depot servers.

By default, peering is enabled when the agent is installed. If necessary, you can disable peering either before installing the agent or after installing it:

- Before installing the agent, you can disable peering by configuring the peering parameter directly in the configuration template of the dynamic content delivery client software configuration template.
- After installing the agent, you can disable peering by running the CDS_Set_Parameter:wkf provisioning workflow, which will turn peering off and update the configuration template for the TCA-Subagent CDS Client URL Handler software installation accordingly.

To disable peering in the configuration template, before installing the agent, you must set the value of the peering parameter in the *TCA-Subagent CDS Client URL Handler Default Parameters* template to *false*. The default value is true. When you install the agent, the peering will be turned off, based on your changes to the configuration template.

To disable peering after installing the agent, you can run the CDS_Set_Parameter provisioning workflow, which requires two parameters, the DeviceID of the target computer, and the ParameterName whose value needs to be set to peering, and its value, ParameterValue, set to false. Similarly, you can modify other client parameters. The provisioning workflow runs successfully, disables peering, and updates the configuration template accordingly. The subagent will be restarted automatically during the parameter change.


Figure 5-12 shows the Distributed Architecture (DCD) architecture.

Figure 5-12 DCD schema

On an endpoint, DCD subagent contacts one or more depots and peers and request file segments. When all parts of a file have been downloaded from the various depots and peers, the subagent reassembles the file and verifies that the download is complete.

If *peering* is enabled on the endpoint, the file is copied into the Tivoli Common Agent's cache directory. This endpoint can now act as a peer download server for other agents.

5.2.2 Device management service

The device management service provides a flexible solution for managing various devices mainly by performing actions called jobs which is targeted to individual Tivoli common agent devices or to groups of devices that are configured to use a SDI SAP.

Within software management, device management service is used to initiate software downloads, run installation actions and collect results. It can also be used for device configuration, inventory scanning and data collection.

The following components are part of the Device Management Service:

Device manager federator

The device manager federator can have either of the following deployments:

- Device manager deployment that communicates with either a DB2 or Oracle Database. The device manager deployment options are an unmanaged server (one computer running all servers and services required by the device manager, installed on a standalone WebSphere Application Server; the device manager database is installed on the same computer) or an unmanaged server with a remote database.
- Lightweight device manager server that communicates with either a DB2, or Oracle Database.

Device manager federated agents

A device manager federated agent can have either of the following deployments:

- Device manager deployment that communicates with either a DB2 or Oracle Database. The device manager deployment options are an unmanaged server or an unmanaged server with a remote database.
- Lightweight device manager server that communicates with either a DB2 or Oracle database.

DMS job flow

Periodically (1 hour by default), the DMS subagent on endpoint:

- 1. Contacts the DMS job federating agent or central DMS server.
- 2. DMS passes all pending jobs to the TCA.
- 3. Job contains the ID of a file and installation instructions.

DMS subagent passes download instructions to DCD subagent. The DCD subagent contacts the DCD management center and requests a download plan; this includes a list of depots and peers from which to download the file.

5.3 Tivoli Provisioning Manager: Software deployment and management

In this section, we review how to set up a typical Software Distribution scenario. To successfully deploy a SD scenario, the following prerequisites must be met:

► Users roles and requirements:

To perform the software distribution tasks, ensure that you have the required knowledge and access rights to perform your role.

Hardware and software prerequisites:

The computers that the provisioning server manages require some hardware and software prerequisites before you can perform software distribution and management.

In this software distribution scenario, we use the following components:

- A provisioning server
- A Windows depot server
- Windows Tivoli common agent
- Local File Repository

A *file repository* is a server that stores installable software images and other files that are installed on managed systems. File repositories holds operating system images or can link to external software catalogs such as Microsoft Windows Server Update Services to provide software updates.

This chapter addresses the use of file repositories to store software images in software package block (SPB) format.

When you install Tivoli Provisioning Manager, a local file repository called *LocalFileRepository* is created and associated with the TIO_HOME/LocalFileRepository directory on the provisioning server.

The properties of the local file repository, such as the root path and the IP address, are automatically configured. When software packages are imported into a file repository, the directory specified is relative to the repository path even though the import path has a leading forward slash.

5.4 Launching and configuring the Software Package Editor

Software Package Editor (SPE) is a Java-based graphical interface for creating and customizing software packages. It is supported on Windows, in an Eclipse environment, and on Windows, AIX, Linux, and Solaris platforms using the Java Web Start application.

5.4.1 Requirements

SPE requires IBM or Sun Java[™] Runtime Environment (JRE[™]) version 1.5. On AIX, Linux 64-bits, and Solaris platforms, it is supported on the latest level of operating system supported by Tivoli Provisioning Manager V7.1.1.

In order to create a new software package that will be distributed to and installed on target computers, it must set up the Software Package Editor environment and properties so that the Software Package Editor can communicate with the provisioning server.

In order to launch the Software Package Editor (SPE) from an Eclipse environment on Windows, use these steps:

1. Open Eclipse from the command line by running the eclipseLauncher.bat batch file from the C:\Program Files\IBM\tivoli\tpm\eclipse directory.

If you launch the SPE from an Eclipse environment running on Windows 2003 64-bit, you can get the following exception as shown in Figure 5-13.

Eclipse				×
An erro C:\Pro	or has occur gram Files\I	rred. See t BM\tivoli\t	the log fi pm\work	le space\.metadata\.log.
			ж)	

Figure 5-13 Eclipse error message

Within the .log file indicated in the foregoing error message, the following error is reported, as shown in Figure 5-2.

Example 5-2 .log file

```
!SESSION 2009-07-21 22:39:36.002
       ------
eclipse.buildId=M20070212-1330
java.fullversion=J2RE 1.5.0 IBM J9 2.3 Windows Server 2003 amd64-64
j9vmwa6423ifx-20080811 (JIT enabled)
J9VM - 20080809 21892 LEdSMr
JIT - 20080620 1845 r8
    - 200806 19
GC
BootLoader constants: OS=win32, ARCH=x86, WS=win32, NL=en US
Command-line arguments: -os win32 -ws win32 -arch x86
!ENTRY org.eclipse.osgi 4 0 2009-07-21 22:39:57.955
!MESSAGE Application error
STACK 1
java.lang.UnsatisfiedLinkError: C:\Program
Files/IBM/tivoli/tpm/eclipse/configuration/org.eclipse.osgi/bundles/305
\1\.cp\swt-win32-3236.dll (C:\Program
Files/IBM/tivoli/tpm/eclipse/configuration/org.eclipse.osgi/bundles/305
\1\.cp\swt-win32-3236.dll is not a valid Win32 application. )
   at java.lang.ClassLoader.loadLibraryWithPath(ClassLoader.java:986)
   at
java.lang.ClassLoader.loadLibraryWithClassLoader(ClassLoader.java:946).
```

Important: This error occurs because Windows 64-bit is not supported for Eclipse 3.2.2.

- 2. From the Eclipse interface, select Window \rightarrow Show View \rightarrow Other.
- 3. Select Software Package Editor under the Software Package Editor folder.
- 4. Click OK.

Bis Edit Norvigate Sageth Project Workforw Bun Window Help Plackage Explorer S Plackage Explorer S Plackage Explorer S Plackage Explorer S Plackage Copierer S Plackage Copierer S Plackage Copierer S Plackage Copierer S Plackage Copierer S Plackage Copierer S Plackage Copierer S Plackage Copierer S Plackage Copierer S Plackage Copierer S Plackage Copierer S Plackage Copierer S Plackage Copierer S Plackage Copierer S Plackage Copierer S Plackage Copierer S	Automation Package - build.xml - Eclipse SDK					_ 🗆 ×
Podoge Explore: 2 Podoge Explore: 2	Eile Edit Navigate Search Project Workflow Run W	jindow <u>H</u> elp				
<pre>Package Explorer 32</pre>	🗈 • 🖫 🖮 Ø 🕞 🕲 🦑 🖗 💁 • 🖄	🖌 🖉 🗠 די אין אין אין א	• 🖓 • 🤄 🔶	• 🔿 •		Automation P
Image: Second	📙 Package Explorer 🛛 🗖 🗖	😵 gf_java_test.wkf 🛛 🚺 Mar	nageStatusList	tc-driver.xm	nl 📄 gfjava.xml	🔝 build.xml 🗶 🎽 🗖
Writable Insert 1:1	← ← ← ★ ▼ Image: second	Show View <1- Sype Show View <1- Sype B General B Automation F C Cys B Cheat Sheet: B Cys C Cheat Sheet: B Cys B Debug B Help B Java Browsin B DP DE Runtime S Software Pat S Software Pat S Software Pat C Software Pat	ackage g kage Editor Package Editor	ston person person prop pert person prop packa prop packa prop packa prop packa packa prop packa prop packa prop packa prop packa prop packa prop packa prop packa prop packa prop packa prop packa prop packa prop prop packa prop packa prop packa propr	<pre>is" location=". is" location=". ige about used erties.exists" perties" /> location="class ige.output" loc is" if="build.p operties)" /> tcdriver file nic, jar"> tcdriver file tcdriver file tcdr</pre>	<pre>ar environment> ./build/build.properties build.properties file ' file="%(build.properti ses" /> ant.project.name).tcdri ant.project.name).tcdri </pre>

Figure 5-14 shows the Eclipse interface.

Figure 5-14 Eclipse interface

- 5. Now set the Software Package Editor properties as follows:
 - a. In the *Software Package Editor* window, click **Window** \rightarrow **Preferences** \rightarrow **Software Package Editor**.
 - b. On the Preferences page, specify the following settings:
 - In the Web Server hostname field, type the *fully qualified host name* of the provisioning server.
 - In the **Web Server port** field, ensure that it contains the default port number of the Web server, **9443**.
 - c. Type SPE in the Web Server root path field.
 - d. Select Use SSL if the provisioning server uses HTTPS over SSL.
 - e. In the Username field, type the provisioning user ID

- f. In the **Password** field, type the password defined at installation for this user ID.
- g. Type the *Default file path* used by the Software Package Editor each time you use the browse button (...) on a panel, or when you open or save software packages.
- h. Type a *path* to a temporary folder to where the Software Package Editor saves temporary files.
- i. Click OK.

Figure 5-15 shows the Software Package Editor preferences.

Preferences				
type filter text	Software Package	Editor		← → →
⊕- General ⊕- Ant ⊕- Automation Package	Web Server hostname	localhost		
⊕- Help ∓- Install/Update	Web Server port	9045		
±- Java ±- Plug-in Development	Web Server root path	SPE		
⊕ Run/Debug	Use SSL			
Software Package Editor 	Username	tioappadmin		
	Password			
	Default file path	C:\Program Files\IBM\tivoli\tpm\(eclipse	Browse
	Temporary folder path	C:\DOCUME~1\tioadmin\LOCALS	5~1\Temp\1\	Browse
			Restore <u>D</u> efaults	Apply
0			ОК	Cancel

Figure 5-15 Software Package Editor preferences

Now the SPE is configured to communicate with the Tivoli Provisioning Manager server.

Note: To be able to use the Software Package Editor with SSL enabled, you must create and import the SSL certificate into the Java runtime environmentTM (JRE) for Eclipse. To obtain a copy of the SSL security certificate from the provisioning server, and then import it, perform the following steps described in "Creating and importing the SSL security certificate" section of the *Tivoli Provisioning Manager V7.1.1 Administration Guide*: at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ib m.tivoli.tpm.scenario.doc/tpm_admin_guide.pdf

5.4.2 Software Catalog, Software Products and Software Definitions

The provisioning server stores information about all your software in a *Software Catalog*, which contains *Software Definitions*.

The Software Definitions contain:

- Installation and configuration parameters
- How software is configured when it is installed
- The requirements of the software
- The capabilities of the software.

In order to deploy a piece of software, the software must have an entry in the Software Catalog. You can also manually add software to the Software Catalog and configure software installation options. Some Tivoli Provisioning Manager processes update the Software Catalog automatically.

A *Software Product* is an object wrapping of one or more *Software Installable* binary files. For SPB type software products, the installable is the SPB file itself.

Software package blocks that you create can either be manually imported or imported automatically by uploading to the file repository by the Software Package Editor.

For each Software Product installed on a given target, a *Software Installation object* is created and stored. The entire set of Software Installation Objects associated to a computer represents its Software Catalog.

5.5 Creating and saving a software package block by using SPE

Start the Software Package Editor directly from the Tivoli Provisioning Manager WEBUI:

- 1. Click Go To \rightarrow IT Infrastructure \rightarrow Software Catalog \rightarrow Software Products.
- 2. From the Select Action menu, click **Start SPE**. The window in Figure 5-16 is opened:.



Figure 5-16 SPE

3. You can create a software package block using either the Software Package Editor or the Build_SPB_from_SPD workflow. This workflow builds the software package block from a software package definition file.

To save a *Software Installable* (SPB) to a *file repository* or to a *local file system* for later importing into a file repository, it should be saved in software package block (filename.spb) format. This file type includes both the definition of the package and the files within the package encapsulated into a single file. See Figure 5-17.

Software Package Editor - [C:\DOCUME~1\ADMINU~1\LOCALS~1\Temp\.tempspe\test]					
Fije Edit AutoPack Iools Settings Help					
	Add object Remove	object Program System action Container			
	A 🗄 🔒 🗖 🎆 🖏 🖏) 🦚			
test	Package - test		*		
φ 🗿 test	Object type	Object name			
C:\Redbook	Execute program	Execute the script: script.cmd			
	ALS~11Temp1 Lempspeltestopened	Select a file repository Xi Available repositories IIII Po-UX Server localFileRepository OK OK Cancel	File Type: SPE		

Figure 5-17 Saving a Software Installable (SPB)

If you have created the software package from the Software Package Editor, then perform the following steps in order to save the file in .spb:

1. Click Save as on the File menu. The Save dialog is displayed.

- 2. Select the appropriate *directory*, then enter a *file name* in the **File name** text box. The file name can be different from the package name.
- 3. In the **Files** of type list, select Software Package Block (.spb), then click **Save**.

Note: In our scenario we used the default local file repository. If you want to create an additional one, follow the instructions in the section, "Setting up new file repositories for the Software Package" in the *Tivoli Provisioning Manager V7.1.1 Administration Guide*, at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ib
m.tivoli.tpm.scenario.doc/tpm_admin_guide.pdf

4. Saving the software package in this format performs a local build of the software package. All source files must be stored on the local workstation for the build to be performed successfully. Depending on the size of the package, this operation might take several minutes. Upon completion of the build operation, a message asks you if you want to reload the package in the Software Package Editor main window.

Note: The procedure to reload the software package can take several minutes if the software package contains an add directory action with the Descend directories option selected. When the software package is reloaded, the structure might be different because the entire directory tree must be added to the software package by creating the related actions (add directory, add file).

- 5. To transform the software package file or software package block into a software package definition, open the file in the Software Package Editor, then save it in software package definition (.spd) format by selecting this option from the Files of type drop-down list. This procedure transforms the software package into text file format. The text file consists of a sequence of stanzas, each of which describes the actions contained in the software package.
- 6. The .spd file is the text version of the information that the Software Package Editor tree view displays. Using a text editor, you can view the .spd file, modify it, and then reopen it in the Software Package Editor and save it in another format.

Tip: You can use the .spd file as the basis to create a new software package or to edit an existing one.

5.5.1 Software product capabilities

You can assign *capabilities* to software to identify software attributes that can satisfy requirements of other pieces of software.

You can add capabilities to software definitions to help the provisioning server to identify and assess software dependencies. For example, a software definition for Windows 2000, Service Pack 1 could include the following capabilities:

- Capability type: The capability type OS.
- Capabilities: An os.version capability with a value of Win2000 and an os.servicepack capability with a value of SP1.

When the capabilities are defined, the provisioning server can then match them with software definitions that include Windows 2000, Service Pack 1 in their list of prerequisites.

5.5.2 Software product requirements

A requirement can identify a prerequisite or a co-requisite.

In a software definition, the requirements that you define apply to all installable files in the software definition.

For example, DB2 Universal Database[™] for Windows requires the Windows operating system. In an environment where DB2 Universal Database is installed on systems with Windows 2000, Service Pack 3, the following settings must be configured to define this dependency:

- In the software definition for DB2 Universal Database, configure a prerequisite for an operating system with Windows 2000 as the version number and SP3 as the service pack level.
- In the software definition for Windows 2000, Service Pack 3, configure an OS capability type, and two capabilities:
 - os.version with a value of Windows2000
 - os.servicepack with a value of SP3

You can assign a requirement type without a requirement name to define a less restrictive dependency. For example, you can assign the RDBRT:RDB requirement type without any requirement names if a database is required and any version or type of database will satisfy the requirement.

Tivoli Provisioning Manager includes some predefined requirement types and associated requirement names. If required, you can add new requirement types and requirements to define other types of software dependencies

5.6 Distributing software

In this section we discuss the steps required to install and uninstall software.

Checklist

Before performing an installation, check the following steps:

- 1. The Tivoli common agent is installed on the targets.
- 2. SDI SAP is created for all targets.
- 3. Zones, regions, and depot servers are correctly configured.
- 4. The software package is created.

Publishing software to depots

To enable faster download and software distribution to target computers, you can publish software products to selected depot servers at the branch office. A typical display is shown in Figure 5-18.

Before you publish a file, you should determine which users will download the file and their location in the network. This affects the target lists or regions to which you replicate the file. To minimize network traffic and download time, you should publish the file to depot servers that are near the users who need the file.

Files uploaded to a depot server are stored in a directory that is specified when the depot server is installed. Depot servers can replicate the uploaded files to other depot servers to optimize the efficiency of network traffic.

The files published on depot servers can then be downloaded by the target computers.

In order to publish software products to depot servers, follow these steps:

- 1. Click Go To → Deployment → Software Management → Software Product Publishing.
- 2. Select the **Encrypt File** check box if you want to enable encryption of the software installable.
- 3. Click **Select Software** and select the software modules to be published, then click **OK**.
- 4. Click **Select Depots** and select one or more depot servers for the provisioning task, then click **OK**.

Software Product Publishing				
Software Product Publishing				_
	Task * Software Product Publishing	1900		
	Encrypt File? 🔽			
Selected Software Products Filter	> 🖄 🔁 🛉 🔶 🗢 1 - 1 of 1 →		L) <u>D</u>	ownload ? =
Software Product				
test			×	
			Se	lect Software
Selected Depots 🎽 Filter > 🙈 🗐 🛧			2) <u>D</u>	ownload ? =
Depot		Description		
nc117	7175	TPM Depot	×	
			Se	elect Depots
Scheduling				-
Click Schedule to change options.	Scheduled; Now			Schedule
Notification				=
Recipients 👂 Filter 👬 🗦 🕴 🔶 🔹	1 - 1 of 1 🌩		22) <u>D</u>	wnload ? =
	Recipient			
•	MAXADMIN		×	
			Add Recipient	Add E-mail
Events 🌗 Filter 🦗 🔁 🛉 🔶 👄			Cit fa	anlond ? 🗖
Description				
		No rows to display		
				Add Event
				Submit

Figure 5-18 Software product publish

- 5. Click **Schedule** to run the task now or to specify the date and time on which the provisioning task is scheduled to start.
- 6. Under Notification, specify notification settings for the task.
- 7. Click Submit.

Installing the SPB on target computers

You will now install the already distributed software package block on all of the target computers in your group.

To install the software package block on the target computers in your group:

- 1. Click Go To → Deployment → Software Management → Software Product Installation.
- 2. Click **Select Software** and select the *software module* that you have created earlier, then click **OK**.
- 3. Click **Select** \rightarrow **Computers** and select the *name* of your *target*, then click **OK**.

See Figure 5-19 for the results of these operations.

Software Installation Advanced						
Autoroca						
Details						-
	Provisioning Task . Install Software 1	903				
Selected Software 🛊 🛊 💠 1 - 1 of 1 🜩					C/ <u>D</u>	ownload ? =
Software Module			Vendor	Version		
test 🍂			тсм	1.0		×
					Se	lect Software
				Validate Targets?		
				Targets missing selected software?	ä	
				rargets missing selected software?	0	
Selected Targets + + + 1 - 1 of 1 +					E) <u>D</u>	ownload ? -
Target			Description			
nc117217.romelab.it.ibm.com			Computer		×	
						Select : 👻
Scheduling						-
Click Schedule to change options.						
	Scheduled: Now					Schedule
Notification						=
Recipients 🌾 Filter > 👫 💷 🛉 🐳 🗇 1 - 1 of	1				Et De	wnload ? =
	Recipient					
•	MAXADMIN			×		
					Add Recipient	Add E-mail
Task Settings for Scalable Distribution Infrast	ructure					
2		Set the task priority and max	mum wait time for th	ne scalable distribution infrastructure,		
	Priority					
Maximum W	ait Time 2	Week		▼		

Figure 5-19 Software Package Block Installation panel

- 4. Set the **task priority** and **maximum wait time** for the scalable distribution infrastructure
- 5. Click **Schedule** and click **Run Now** to run the software installation task immediately, or schedule it to run at a specified date and time.

Note: While running a software installation task, there are workflow parameters that list the priority of the task only when the user changes it before running the task. When priority is not listed in the workflow parameters, the task runs with the priority that is defined in the global variable.

- 6. Under **Notification**, select the appropriate notification options.
- 7. Click Submit.
- 8. When you submit the task, the Provisioning Task Tracking page is displayed. You can click the task name to see details about its status and monitor its progress until the task has completed. Click **Refresh** to see an update on its status. The SPB is now installed on all of the target computers in your group.
- 9. In order to verify that the SPB is installed, click Go To → Deployment → Provisioning Computers. Find one of the target computers in your group and click the *computer name*. Click the Software tab. The software module that you have created is listed as installed software.

The results of these operations are shown in Figure 5-20.

Find:	🕅 🤝 Select Action 🔍 👀 🎽] 🗔 🧟 👍 🕫	<u>نې</u>			
List Computer Hardware	Software Compliance Recomm	nendations Crea	dentials Workflows	Variables Dep	oloyment Properties	
Computer nc117217.romelab.it.ibm.com		Operating System	Windows Server 2003 Enter	prise Edition SP2 🎤		
Last Scan		Agent	TCA-1420		Statistic	49 Products Installed / 0 Patches Installed
		, igoint				
C Software						
C Patches						
Software Installations	♦ ♦ 1 - 1 of 1 ♦					
Software Installation		Version Sol	tware Definition		installabl	e Status
□ ▼ test		1.0 tes	it		not_tes	ted
			Details			
Software Installation *	test			Locale		
Configuration Template	test.1.0.9465	1 2		coolio		
Software Installable	test	10		Version	1.0	
Software installable	logi					
3.2 de de la controle de construendo en de se de se de trate de de deserver.						Add Software

Figure 5-20 New software installation

Part 3

The new GUI and IBM Service Management integration scenarios

Since Version 7.1, Tivoli Provisioning Manager is built on top of the Tivoli process automation engine, a proved platform for service management. This has made possible many new capabilities, such as integrated process automation, where Tivoli Provisioning Manager is the *Do'er* of the process tasks from other IBM Service Management products, and improved user interaction experience, by using the powerful Start Center functionality.

Another advantage of this integration is the capability to use the powerful Tivoli process automation engine functions, such as uniform security, common BIRT reporting, common installation, automation tasks, escalations, and actions, which are available to all applications that utilize the Tivoli process automation engine platform.

In this part of the book, we first discuss the new Tivoli Provisioning Manager GUI, based on the Tivoli process automation engine Start Center functionality, which provides role-based access to functions and data for all IBM Service Management products. We show you how to accomplish some common Tivoli Provisioning Manager tasks using this new GUI. So, if you are not familiar with Start Centers, we suggest that you take a look at this chapter.

Then we delve into the details of several IBM Service Management integration scenarios with products such as IBM Tivoli Application Dependency Discovery Manager, IBM Tivoli Service Request Manager, and IBM Tivoli Change and Configuration Management Database. We show you how you can implement these scenarios, as well as why you would implement, in other words, the business value of these integrations.

Finally we devote a chapter to implementations with non-IBM Configuration Management databases and show how you can use Tivoli Provisioning Manager in such an environment.

6

Tivoli process automation engine based user interface

The Tivoli process automation engine Web-based user interface provides all IBM Service and Asset Management based products with an integrated powerful Web-based platform.

In this chapter we provide highlights of the setup of the Tivoli process automation engine Web-based user interface for products that exploit LDAP user configuration and security capability. First we give you an overview of how to customize it to your needs, followed by introducing the new predefined security groups added by the Tivoli Provisioning Manager V7.1.1. Finally, we show you GUI differences for some of the common functions in Tivoli Provisioning Manager V7.1.1 and Tivoli Provisioning Manager V5.1.1.2.

We cover the following topics:

- "Start Center configuration for LDAP users" on page 138
- "Start Center templates and instances" on page 138
- "Configuring the Tivoli process automation engine Web-based interface for users" on page 143
- "Tivoli Provisioning Manager Start Center templates" on page 159
- ► "Overview of the GUI differences" on page 167

6.1 Start Center configuration for LDAP users

This chapter provides details regarding the configuration and administration of the Start Centers after Tivoli Provisioning Manager has been successfully installed. The information provided in this section applies, in general, to all products using the Tivoli process automation engine Web-based user interface and exploiting LDAP functionality for user configuration and security.

The new user initial setup changes slightly if the product uses the Tivoli process automation engine User Configuration capability, rather than the LDAP functionality. For more information about this specific case, you can refer to the *Tivoli Provisioning Manager V7.1.1 Installation Guide* at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ibm.t ivoli.tpm.ins.doc/tpm_install_guide.pdf

In our implementation, we used LDAP.

6.2 Start Center templates and instances

Start Center templates are configurable dashboards that provide access to the applications, result sets, and Key Performance Indicators (KPI) that a user or administrator would like to quickly utilize.

A Start Center template is associated to a security group. This template is designed to display the activities, resources, and views that are key to the users that will belong to that group.

It is important to highlight that whenever a user logs in to the Tivoli process automation engine Web-based user interface at the URL:

https://<fully_qualified_hostname>:9443/maximo

What is displayed to that user is their own instance of the Start Center template associated to the group that the user belongs to. Each user can modify their own instance of the Start Center to tailor it to better fit their needs, while only administrators can modify or create Start Center templates.

6.3 Overview of main functionality in the Start Center

In the Tivoli Provisioning Manager Start Center, the following two types of applications are available:

- Simple power application
- Standard power application

A simple power application is a single-paged, full-functional application designed for the power user. It contains:

- ► The standard navigation bar
- Records displayed in table windows
- No tabs
- One page, with data displayed within table windows

Figure 6-1 shows an example of a simple power application.

ŝ	. A	ssignment	Managei		🗘 Web Replay 🕴 Bulletins: (0) 🤌 Go To 🛄 Beports 🄶 Start Center	≜ <u>P</u> rofile ¥ <u>S</u> ign	n Out ? <u>H</u> elp	IBM,
			Y Find:		n 🗸 🗸 Select Action 🛛 🖌 📄 🌉 I 🍋 🎠			
Ø	Adv	anced Searc	h 🔻 😡	Save Que	y • Second Contraction Contraction			
Wo	rk L	ist 🕴 🕨 Filter	> # 12	4 414	- 1 - 8 of 23 🥪		Download	? =
		Work Order	\$	Task 🕈	Description Labor Craft Skill Level Vendor Scheduled Date Lab Hrs	Asset Location	Calc Pri Stat	us
	•	1002	1	10			2	Û
	×	1002			Activity to address intranet bad performance		2	Û
	•	1006		10	Restart HTTP Server		2	Û
	•	1006			Scan Mail Server for Viruses		2	Û
	►	1008	1		Problem on Payroll System			Û
	•	1047		10	Create Implementation Tasks and assign Targets			Û
	×	1047	,	20	Schedule Implementation Tasks and Assign Owners			Û
	×	1047		30	Approve Implementation Schedule - Check for Change Window Conflicts			Û
					Filter Work to Match Labor	efresh Work List	New Ro	w
Lal	bor l	List 🐤 Filter	r>A D	14 +1	**		Download	? =
	Lat	oor Name	<u>Craft</u> SI	kill Level	Vendor Work Loc Shift 2009-09-09 2009-09-10 2009-09-11 2009-09-12 2009-09-13 : No rows to display	2009-09-14 2	009-09-15 %	Alloc
					Filter Labor to Match Work Refresh Labor List Select Work Date Select Labor	or Query	Show All Labo	or
								_

Figure 6-1 Simple power application

A standard power application, on the other hand, is a multi-tabbed, full-functional application designed for the power user. Most of the applications in Tivoli process automation engine are standard power applications, which contain:

- The standard navigation bar
- The List tab containing one table window that displays records found after performing a search; you can sort a table by clicking the column header

Note: Not all columns in the List tab are sortable. Columns based on database relationship are not sortable.

- The main tab showing the main properties of the object highlighted in the list tab.
- As many other tabs as are needed to display all remaining object properties.

Figure 6-2 shows an example of a standard power application.

Provisioning Computers	Web Repl	ay 📍 <u>B</u> ulletins: (0) 🎓 <u>G</u> o To 🔟 <u>R</u> eports	✤ Start <u>C</u> enter ▲ <u>Profile</u> × <u>Sign</u> Out ? <u>H</u> elp	IBM.
Find:	🔥 🔻 Select Action 🗸 😯] 🗟 🖉 1 🄄 🖗		
List Computer Hardware	Software Compliance Recomm	nendations Credentials Workflows	Variables Deployment Properties	
🕅 Advanced Search 🔻 🗟 Save Query 🔻	A Bookmarks			
Computers 🛛 🔻 Filter > 🚜 🕸 🗛 🗍 🧇	1 - 5 of 5 ↔			
Computer 🕈	Operating System	Globally Unique Identifier	Agent	Compliance S
nc117175.romelab.it.ibm.com	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	E172FE27C9BD3F45AA5450459EA4CF88	TCA-1.4.2.0	No complia
nc117177.romelab.it.ibm.com	Microsoft Windows Operating System 2003 server x64 Enterprise Edition SP2 [Version SP2]	2A978E3C949134DE8DB22A7D515D441D	TCA-1.4.2.0	Not complian
nc117217.romelab.it.ibm.com	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	C33948CC0D4537FABE459EF7206BF789	TCA-1.4.2.0	No complianc
nc117218.romelab.it.ibm.com	Windows Server 2003 R2 Enterprise x64 Edition SP2	852E294125263AA3B46F80CA29616AA6		No complianc
nc125095.romelab.it.ibm.com	Windows Server 2003 Enterprise Edition SP2			No complianc
Select Records				

Figure 6-2 Standard power application

Within these applications, the standard navigation bar is a section included at the top of the pages in power applications.

Figure 6-3 shows the standard navigation bar.

Provisioning Computers	O Web Replay
Computer Hardware Software List Computer Hardware Software Computer* Inc117175.romelat Globally Unique Identifier E172FE27C9B03F Configuration item NC117175.ROMEL	Instal Immendations Credentials Workflows Variables Deployment Properties Inistal Immendations Credentials Workflows Variables Deployment Properties Unistal Immendations Credentials Workflows Variables Deployment Properties Run Inventory Scan Immendations Immendations Immendations Immendations
Configuration Management P Address 91681 Operating System Window Computer Template Locale Datale	Add Credentials
Model Type VII ware Vir Architecture intel Serial Number VII ware. Snc Manufacturer VII ware. Inc	tual Platform Compliance Security Configuration required Ad 07 93 b4 3 Software Configuration required A 2 Software Configuration required A

Figure 6-3 Standard Navigation bar

The navigation bar contains:

- An application-specific icon
- ► The name of the application, for example, Provisioning Computers
- A link/action for Web Replay to let you automate repetitive tasks on the Web interface
- A link/action for Bulletins to view broadcast messages; this link is only displayed when there are rare active Bulletin Board messages
- A link/action for Go To, which lets you easily navigate across module and applications
- A link/action for **Reports** to let you select application-specific BIRT reports
- ► A link/action for Start Center to let you return to the Start Center
- A link/action for **Profile** to let you manage your personal information (address, phone, e-mail, and so forth), defaults, and Tivoli process automation engine password
- ► A link/action for Sign Out to log out from your Start Center
- A link/action for Help to let you display the help menu, when selected from the application pages, or context sensitive help, when selected from dialog boxes
- ► A Query drop-down, containing actions pertaining to queries
- ► A Find input field and a Find button, to perform a quick, exact match search

- ► A Select Action drop-down, containing application actions
- The **toolbar** buttons, to perform common application actions.

Figure 6-4 shows some of the available buttons. The buttons displayed depend on the application you are using and on the authorization assigned to you. The toolbar buttons shown in Figure 6-4 (from left to right) are:

- Add <object>
- Save <object>
- Clear Changes
- Previous <object>
- Next <object>

There are also any number of other application-specific buttons. These often have flyover text describing the button and also a keyboard shortcut.



Figure 6-4 Toolbar buttons

Field buttons also launch dialog boxes. These are the field buttons in the Tivoli process automation engine, as shown in Figure 6-5.

Button	Name and Function
*	Detail Menu— Displays a menu of actions available for the field. Specific choices vary by field.
	Long Description — Provides room for entering more data than can fit in a field. After a long description entry is created, the button changes
	color to indicate that more information is available.
	Select Date — Displays the Select Date dialog box. Click a date to return the selected value to the Date field.
B	Select Date and Time — Displays the Select Date and Time dialog box. Click a date to return the selected date and time to the Date field.
0	Select Value — Displays a page showing available values for the fields. Select Value pages are often lists of records created in other applications, for example, item records created in the Item Master application.

Figure 6-5 Field buttons

Dialogs launched by field buttons should also have a title that matches their name, with the exception of Select Date and Select Date and Time, both of which lack a title.

For additional information about the Tivoli process automation engine user interface functionality and capabilities, you can refer to the online Help.

6.4 Configuring the Tivoli process automation engine Web-based interface for users

After the product installation completes, the actions shown in Table 6-1 can be performed by the specified users to ensure that a new user can access and easily perform their tasks through the Tivoli process automation engine Web-based user interface:

User who runs the action	Action
WebSphere Application Server administrator	Create new users.
WebSphere Application Server administrator	Assign users to groups.
User belonging to MAXADMIN group	Activate VMMSYNC cron tasks.
User belonging to MAXADMIN group and authorized users	Create a new Start Center template.
User belonging to MAXADMIN group.	Assign permissions to a security group.
User belonging to MAXADMIN group on the Start Center template or the user on their own Start Center instance	Create a KPI.
User belonging to MAXADMIN group	Modify KPI cron task.
User belonging to MAXADMIN group on the Start Center template or the user on its own Start Center instance	Change content layout Modify a portlet.
Start Center template owner	Modify an existing Start Center template.
User on their own Start Center	Update Start Center.
Authorized users with multiple tabbed Start Center instances	Display settings.

 Table 6-1
 Actions to set up user interface and access

In the following topics you can find a brief description of how to run these actions.

6.4.1 Creating new users in LDAP and assign them to groups

Use the following steps to create new users in LDAP and assign them to groups:

1. You must first log in to the WebSphere Application Server Console using:

https://<fully_qualified_hostname>:9043/ibm/console/login.jsp

- 2. Click Users and Groups \rightarrow Manage Users.
- 3. Specify the required settings in the Manage Users panel and then click the **Group Membership** button, as shown in Figure 6-6.

Integrated Solutions Console Welcome wasadm	Help Logout	IEM.
View: All tasks	Sele	ct Action 😪
Welcome My Startup Pages	Manage Users	
Guided Activities	WIM User Management	3 - 0
	Create a line	
	Create a User	
Resources	*User ID	
Security	Group Membership	
Environment	*First name *Last name	
Users and Groups	E-mail	
 Administrative User Roles Administrative Group Roles Manage Users Manage Groups 	*Password *Confirm password	
Monitoring and Tuning	Create Cancel	
Service integration		
I UDDI		
E Settings		

Figure 6-6 Create a new user

4. In the Group Membership pane, you can select which group you will assign the user to. After you make your selection, you can close the Group Membership pane and click **Create** to add the newly defined user.

Note: You can connect to the Tivoli process automation engine UI with the new user ID after the time specified in the VMMSYNC cron task elapses.

6.4.2 Synchronizing Tivoli process automation engine users configuration with LDAP settings

In order to synchronize users definitions between LDAP and the Tivoli process automation engine, the VMMSYNC cron task must be set to active.

 To do this, you have to log in as administrator to the Tivoli process automation engine UI and select Goto → System Configuration → Platform Configuration → Cron Task Setup.

🔨 Welcome, maxadmin		🖸 Web Replay 🛛 Bulletins: (0)	📌 Go To 🛛 💷 Repor	ts 📫 Start <u>C</u> enter 🌲	Profile 🎽 Sign Out ? Help 📱
			🝓 Administratio	n +	
Automation Package Developer Compliance Analyst	Deployment Specialist	Process Management Requester Provis	🖉 Assets	•	uration Librarian
	DB Change C	ontent/Layout 🕮 Display Settings 😕 (Change		Template MR lindate Start Co
tomation dovelopment applications	Status of my recent	provisioning workflows = Silver 40	🙀 Deployment		
tomation development applications	Deployment Request I	Workflow Name	Discovery		Error Message
Provisioning Workflows			🗠 Financial		
-	12.033	SoftwareModule Insta	🕲 IT Infrastruct	ure +	
Provisioning Workflow Status	12 032	No operation	Integration		
	12.031	Compliance Validation	🐨 Inventory		
Provisioning Computers	12.029	Compliance Validation	🖻 Planning		
	12.027	Compliance Validation	Purchasing	•	
Provisioning Task Tracking	12,024	SoftwareInstallation.U	🔊 Release		
- A-	12,023	Compliance_Validation	- Security		
Provisioning Task Definitions	12,021	Compliance_Validation	Self Service		
	12,020	ComplianceRecommer	A Service Desi		
Virtualization Management	12,019	ComplianceRecommer	Service Leve	4 k	
 Image: A start of the start of	Set Graph Options		A Spaning Book	ant Managar Catalan	1 - 10 of 172 Next Pa
			Sy Sy	stem Properties	Platform Configuration +
visioning administration applications 🥢 🗌 👔	Status of my recent	provisioning tasks 👽 Filter > 🏟 📁 褅	Lo Lo	aging	Migration +
	Provisioning Task		Do Do	mains	s <u>Start Uate</u>
er configuration and development applications 🥒 🗖 👔			Da	abase Configuration	
	Install Patch 2,607		Ap	plication Designer	tarted
	Compliance Remediati	on [8/27/09 11:55 PM]	Co	mmunication Templates	itted 2009-08-27 23:55:21
	Install Patch 2,638		Ac	tions	ess 2009-08-26 03:29:11
	Run provisioning work	flow No_operation submitted at August 24, 20	09 10:19:0 Ro	es	ess 2009-08-24 22:19:10
	Compliance Scan and	Check	Es	calations	ess 2009-08-17 20:09:03
	Graphical View		Wo	orkflow Designer	1 - 5 of 146 Next Pa
			Wo	orkflow Administration	
	Data model object f	nder V Filter > dta 1 1 🖗	Cre	on Task Setup	/ -
	Ubject ID	Object	E-r	nail Listeners	Object Type
			We	b Services Library	
	1,399	VMware_VI3_VirtualCenter_Discovery	La	unch in Context	Device Driver
	1,004	Favorite Computers			Computer Group
	1,005	Favorite Software			Group
	1,007	Deployment Engine Service Access Point			Device Driver
	1,009	Son Service Access Point			Device Driver
	1,011	STUMP VI Service ACCESS Point			Device Driver
	1,015	Talast Seques Access Point			Device Driver
	1,015	Talaat TS Sanuica Access Point			Device Driver
		UNITED TO DRIVER ALLERNS PORT			Devied Driver
	1,017	Stack Of Databas			Davias Driver

Figure 6-7 Go To the cron task table

2. Select the task in the list tab and set it to active, as shown in Figure 6-8.

💮 Cron Task Setup		🕞 Web Rep	ılay <mark>₿</mark> ulletins: (0)	∲ <u>G</u> ото Ш	Reports 🕈 Start <u>C</u> enter	[▲] Profile X Sign Out	?Help IEM,
Find:	n 🕫 🗸 😽 😽) 🖪 🖉 🕸 🏟 🔊					
List Cron Task							
Cron Task VM Class psd Access Level FUL	MSYNC Invokes WebSphere VMM lisecurity.vmm.VMMSyncCronTask L P	APis to populate dat; 🗏					
Cron Task Instances > Filter > 🚜 🔮] ∲ ∳ ∲1-1 of 1 ∳					Cły	Download ? =
Cron Task Instance Name	Schedule Sm.,	ß	Run as User MAXADMIN 🔎	<u>Active</u> ⊻	Keep History	Max Number of His Duplicate	olimitation states and
Parameters History				_		NU	
Cron Task Parameters P Finer > m	1 µ ∳ ∳ + 1 • 0 0 i a				Description		ownload 8 =
Credential	value				VMM admin credentials.		
▶ GroupMapping	xml</td <td>version="1.0" encoding="UTF-i</td> <td>3" ?><!--D0</td--><td></td><td>The USER XML used by the</td><td>VMM task.</td><td></td></td>	version="1.0" encoding="UTF-i	3" ?> D0</td <td></td> <td>The USER XML used by the</td> <td>VMM task.</td> <td></td>		The USER XML used by the	VMM task.	
 GroupSearchAttribute 	cn				VMM search attribute to que	ry group records.	
Principal	CN=W	sadmin,ou=users,ou=SWG,o=	BM,c=US		VMM admin principal.		
 SynchAdapter 	psdi.s	ecurity.vmm.DefaultVMMSyncA	kdapter		VMM synchronization adapt	er.	

Figure 6-8 VMMSYNC activation

After the time specified has elapsed, you will be able to log in as the new user ID to the Tivoli process automation engine Web-based user interface. The Start Center instance that will open is the one associated in the Tivoli process automation engine to the security group that the user belongs to.

The following topics describe how to customize this setting.

6.4.3 Creating a new Start Center template

In this topic you can find the instructions to create a new Start Center template.

Not all users are allowed to create new templates. By default, all users belonging to Tivoli Provisioning Managers, except those belonging to the TPDEVELOPER group, are allowed to create new Start Center templates.

Note: When you create a template, it must be assigned to a group before users in a group can access it.

1. Click the following icon (Figure 6-9) to create a new Start Center template:

🔠 Create New Template

Figure 6-9 Create New Template icon

- 2. In the portlet selection panel, you can select:
 - How to show the layout: Narrow-Wide, Wide-Narrow or Equal-Width.
 - Which portlets to display.
 - Optionally, a user defined name for portlets. See Figure 6-10.

Layout [*] Narrow-Wide	
Left Column	*
Portlet	Display Name 🗢
Favorite Applications	Favorite Applications
Quick Insert	Quick Insert
Right Column 🌗 Filter 🖓 🕴 📰 🛉 🔶 🕴 🗢 1 - 3 of 3	÷
Portlet	<u>Display Name</u> ≑
KPI List	KPI List
Result Set	Result Set
Inbox / Assignments	Inbox / Assignments

Figure 6-10 Start Center Portlet Selection

You can also select which order to display portlets in the Start Center (Figure 6-11).

C Download ? =	
Order 🗢	
1 🍿	
2 🗊	
Select Content	
Et Download ? =	
<u>Order</u> ‡	
1 💼	
2 💼	
3 🏦	
Select Content	
Finished Cancel	

Figure 6-11 Start Center Portlet Ordering

- 3. Click Finished to display a preview of the new Start Center.
- To apply further modifications before saving the Start Center, click Change Content/Layout, otherwise click Save Template to confirm your choices and save the template.

6.4.4 Assigning permissions to a security group

After having created a Start Center template, the administrator has to specify which applications can be accessed from the Start Center template, and how to access them.

This step decides which resources will be available to see on the Start Center instance by the user and how they could manage those resources:

1. As administrator, select **Goto** → **Security** → **Security Groups** to access the Security Groups panel, as shown in Figure 6-12.

ို့ကို Security Groups		🕞 Web Replay 🛛 🥊	Bulletins: (0) 🌈 Go To 上 🗠	<u>R</u> eports 🕅 Start <u>C</u> enter 🔺 <u>P</u> rofile	X Sign Out ? Help	11
Y Fin	d: Select Action	✓ 3 2 4	•			
List Group S	ites Applications Users	Provisioning Permissions				
Advanced Secret	Caus Quant - Realization					
uni Auvanceu Search 🔻 la	a Save query 🗸 🗸 Bookillarks					
Groups 🛛 🔻 Filter > 🕅 📋	🛉 👙 🛶 1 - 20 of 48 🧼				E/ Download	?
Group 🗘 🛛 Desi	<u>cription</u>	ndependent of Other Groups	Authorize Group for All Sites	Authorize Group for All Storerooms	Authorize Group for All Labo	<u>1</u>
		P	P		P	
DEFLTREG New	/User					4
EVERYONE AILM	laximo Users]				4
MAXADMIN	E	2		\checkmark	¥	4
MAXIMOUSERS						4
MAXREG Self	Registration Process Access	Ž				4
PMCFGADM		2		D		-
PMCFGAUD	E	Z				4
PMCFGLIB	E	2				-
PMCFGMGR	E	2				
PMCHANGEADMIN	[1
PMCHANGEANALYST						4
PMCHANGEAPPROVER	[V			-
PMCHANGEIMPL	[V			-
PMCHANGEMGR	[V			
PMCHANGEOWNER	[V			-
PMINCADM	E	2	V	V	✓	4
PMINCANAL	E	2	V	V	V	-
PMINCMGR	E	Z	V	V	V	-
PMINCOWN		7	V	\checkmark	¥	4
PMPRBADM	E	<i>i</i>	V	V	¥	4
Select Records						

Figure 6-12 Security Groups panel

2. Click the Group for which you want to tailor the access to enter its definition.

Let us suppose that you click the DEFLTREG entry. DEFLTREG is the default group assigned to a new user; its definition is shown in Figure 6-13.

Û _L Û	Security Groups		🕑 Web Replay	Bulletins: (0)	₱ <u>G</u> o To <u>IIII R</u> eports	n Start <u>C</u> enter	[≜] <u>P</u> rofile	× <u>S</u> ign Out	? <u>H</u> elp	IBM.
	🖌 Find:	Select Action	💌 🖬 🧶 I	💠 🏟						
Lis	st Group Sites Applications	Users P	Provisioning Permission	IS						
	Group Start Center Template Independent of Other Groups?	DEFLTREG	New User							

Figure 6-13 DEFLTREG group entry

- 3. In this tab, by clicking the magnifying lens, you can specify which Start Center the new user will access after logon.
- 4. In the Site tab, you can select which site the new user will belong to, for example Roma, as shown in Figure 6-14.

		Action	*	
st Group Sites	Applications User	s Provisioning Permissions		
Group DEFLTREG	lew User			Authorize Group for All Sites?
s 🕨 Filter > 🚲 😂 🛧 🔶 🔶	1 - 1 of 1 ->			E Download
Site =	Description		Organization	Active Authorized
м		Detail	a	
•			Organization	Sherizedbuk Science
	i ne Filter	49. 17 1 A 1 - 1 - 2 - f 2 - A		
	Filter	dRa ⊇ ; + , + 1 - 2 of 2 → Description	Download (?) =	
	Site	ana 1 + + + + + + + + + + + + + + + + + +	Creanization Active	
	Filter Site PMSCRTP	Bit and a state of PMSC in America	Creanization Active	-
	PMSCRTP ROMA	An and a site of PMSC in America	Cranicadio Active	-

Figure 6-14 DEFLTREG group site

5. In the Application tab, you can specify the permission that the user will have to access that application and the resources it manages through their Start Center instance.

Note: From their own Start Center instance, the user will be able to modify the layout of the portlets by selecting the applications accessible for the group that they belong to, but they will not be able to grant themselves additional access to applications and their managed resources.

ຖູ່ຜູ້ Security Groups	🕞 Web Replay 🕴	Bulletins: (0) 🎓 Go To 🔟 R	eports 🕈 Start <u>C</u> enter 🔺 <u>P</u> rofile × Sign Out ? <u>H</u> elp	IBN
Find:	🔻 Select Action 💉 🖬 🧷 💠	\$		
List Group Sites Applications	Users Provisioning Permissions			
Group DEFLTREG New User				
Applications 🛛 👂 Filter > 🚜 😓 🔤 🍦 🦆 🥪 1 - 10 of	199 🧼		Download	2 =
		Grant Listed Applications :	Revoke Listed Applications : 🔻	
Description 🗢	Main Object/Table		Original Application (if copied)	
Access Control Lists	TPM View Acl			
Actions	Table to hold actions.			
Activities and Tasks	The WOACTIVITY view.			
Actual Configuration Items	Actual CI Table			
Adapter Conversion	Deployed Assets Adapter Conversion Targets			
Application Designer	The MAXAPPS Table			
Application Tiers	TPM View Cluster			
Asset Link Results	Asset Link Result view.			
Asset Reconciliation Results	Asset Result of Link and/or Comparison			
Assets	The ASSET Table			
Options for Assets > Filter > 2% 🗊 🛧 🍦 🔶 1	- 4 of 4 🐡		Download	. =
			Grant Listed Options for This Application	
Description ≑	Grant Acces	s	Condition	1
Delete Asset			1	
New Asset			1	
Read access to Asset			1	
Save Asset			P	
> Filter > ∞ □ + + + 1 - 10 of 51 →			E/ Download	2 =
Description 🗢		Grant Access	Condition	
Add Assets to Collections			P	
Add/Modify Conversions			8	
Add/Modify Linear Referencing Methods			1	
Add/Modify Units of Measure			P	
Apply Item Assembly Structure			1	
Asset Details				

Figure 6-15 shows a sample layout of the Application tab.

Figure 6-15 DFLTREG group application

6. By clicking an application, such as **Assets** in the Applications pane, you get the list of available accesses that you can grant in the Options for Assets pane.

For example, by clicking the specific option, you can decide to grant the read access only for assets such as host platform, as shown in Figure 6-16.

Optio	ons for Assets	≽ Filter > 🏠 📋 🗍 🍦 🛊 🕹 - 4 of 4 →		Et <u>Dow</u>	nload 🕴 🗧
				Grant Listed Options for This Applicat	ion
	Description	★	Grant Access	Condition	
•	Delete Ass	et		1	
•	New Asse			1	
•	Read acce	ss to Asset	V	TPISHOST 🎤	
•	Save Asse	t		1	
			Details		
	Description Grant Access? Condition Type Expression	Read access to Asset TPISHOST The computer is a host platform EXPRESSION D in (select HOST_PLATFORM_D from HOST_PLATFOR			
	Condition Class				

Figure 6-16 Read option selection

7. You can also grant modify Save access, which means the ability to modify an existing object, for non-host platform computers, as shown in Figure 6-17.

		Grant Listed Options for This Ap	nlication
			phoation
Grant Access		Condition	
		1	
		1	
		TPISHOST 🍠	
V		1	
Details			=
	Either S Ph. 1 M.	1 1 9 of 9 -	V Deventered
	Condition	Department	Tuno
	Condition	computer	Type
		Furthering Mitter annullance about /	
	TPISSRVDSE	Evaluates if the compliance check is assigned to a computer	CLAS
	N TRISHOST	The computer is a host platform	EVDDE
	TPNOHOST	The computer is not a host platform	EXPRE
	TPNOOWNER	Show the membership section of Computers	EXPRE
	- Internities	The Third Description Reserves	
	TPM RXA OPT	Discover Computers using RXA sigOpt	EXPRE
	TPM SNMP OP	The Tivoli Provisioning Manager	EXPRE
		routers) using SNMP sigOption	270112
		Display the IMACE TV/DE when a source	
	TPSRCCOMPSE	computer has been selected.	EXPRE
	▶ TPDEDCOMP	Is dedicated computer	CLASS
	TPOVERFLOW	Display overflow computer section	CLASS
		Details	
	Condition	TPNOHOST The computer is not a host p	atform
	Type	EXPRESSION	
	Expression	ID not in (select HOST PLATFORM ID from	
		HOST_PLATFORM)	
	Class		
	Class		
	Aiways Evaluate?		
	Origin Pocess Origin		Conduct TPISHOST TPICOUVIER Show the membership section of Computers TPISHOST TPINOWNER TPINOWNER TPINOWNER TPINOWNER TPINO

Figure 6-17 Save option selection

8. You open the *Select Value* pop-up window by clicking the redirecting arrow beside the Condition field in the option's details. The details of your choice are automatically copied in the option's details fields as you click the value.

Note: If you grant no access by unselecting the **Read** option, the application will not even be listed among the available applications on the Start Center instance portlets.

9. In the Users tab, the details of all users belonging to that security group are listed. In the Provisioning Permissions tab, you can authorize users belonging to that security group to manage the real implementation of a specific IT process by running workflows.

6.4.5 Creating a Key Performance Indicator

Key Performance Indicators (KPIs) provide the ability to track critical performance variables overtime.

Before displaying a KPI within the Start Center, you must first create one from the **KPI Manager** application.

To access the KPI Manager select Go To \rightarrow Administration \rightarrow Reporting \rightarrow KPI Manager.

Within the KPI Manager, select the **New KPI** icon on the toolbar as seen in Figure 6-18.



Figure 6-18 New KPI icon

To create a KPI, the user must define a select statement for the query and set the following parameters:

- Target: The target value
- Caution At: The caution value that will be displayed in yellow
- Alert At: The alert value that will be displayed in red

Figure 6-19 shows a sample KPI graph.



Figure 6-19 Sample KPI graph

6.4.6 Modifying a Key Performance Indicator cron task

In order for a KPI to stay current with live data, a cron task must be established to facilitate and poll on a schedule.

To access the Cron Task Setup application, select, Goto \rightarrow System Configuration \rightarrow Platform Configuration \rightarrow Cron Task Setup.

A cron task named *KPICronTask* is available out of the box to use for keeping KPI data current.

To enable this cron task, select the task from the list tab, then within the instance, define the schedule (the default is 1 day) for the administrative user to run the cron task under, and set it to active as shown in Figure 6-20.

Cron Task Instances	ilter > 💦 🚍 🛧 🐳 ⇔ 1 - 1 of 1 ⇒		
Cron Task Instance Name	Schedule	Run as User	Active?
KPINONREALTII	1d,0,0,0,*,*,*,*,*	🗈 MAXADMIN	₽□

Figure 6-20 KPI Cron Task Instance

The KPI data will now be updated on the schedule that you have established.
6.4.7 Choosing which portlets to display in your Start Center instance

If authorized to run the command, click the icon shown in Figure 6-21.

hange Content/Layout

Figure 6-21 Change Content/Layout icon

You can add, remove, or to reconfigure the portlets displayed on your Start Center instance.

6.4.8 Modifying the content of a portlet within your Start Center instance

After you have selected which portlets you would like to use in the Start Center, you have to edit them by selecting **Edit Portlet** as shown in Figure 6-22.



Figure 6-22 Start Center Edit Portlet

Within each type of portlet, there are several configurable options. For example, the result set portlet has the ability to select a user defined or public query and then display its results with colored conditions or a bar or pie graph.

The following tabs are available within the Result Set setup:

- Available Queries: Lists all queries from which you can select one to display.
- ► Column Display: Here, you select which columns to display and their order.
- Display Options: Here, you can set a color to indicate a status level.
- Chart Options: Here, you set the parameters for a graph, if you choose to display one.

For example, if a user would like to display all NEW work orders in the color red, they would configure the color parameters with an expression of *equal to*, an *expression value* of *NEW*, and a color of *red* as seen in Figure 6-23.

	Current Query	OWNER IS ME - My Wo	ork Orders			
Co	ondition Attribute	STATUS		P		
Color Parameters	≽Filter > 🔥 📁	∲ ∳ ⊕ 1 - 1 of 1 →	,		C)	Download
Expression	Expres	ssion Value			Color	
	NEW				#FF0000	Û
			Details			
Expression Equal Te	•	Expression Value NE	N		Color Red	~
						Add Color Alert
					Finished	Save Cance

Figure 6-23 Result Set Setup Color Parameters

When the results are returned in the Start Center, those work orders with a status of *NEW* will be shown in the color *red*.

6.4.9 Modifying an existing Start Center template

The Administrator or the template owner are allowed to modify an existing Start Center template:

1. Click the icon shown in Figure 6-24 to modify an existing Start Center template.

A Modify Existing Template

Figure 6-24 Modify Existing Template

2. Choose the Start Center template to modify from the list of Start Center templates you are authorized to access (see Figure 6-25).

🗣 Modify A Template			:?:[
Start Center Templates	≽ Filter ⇒ 🏤 📋 🛊 🝦 🐳 4 - 10	of 20 🧼 💽 Downlos	ad ? =
Start Center Template	Description 🗢	Created On	
Template-5	Administration	8/11/04	×
Template-36	Asset Manager	3/2/05	×
Template-8	Contracts	8/11/04	×
Template-39	Executives	8/22/07	×
Template-38	Finance	8/22/07	×
Template-37	HR	8/22/07	×
Template-12	Inventory	8/11/04	×
Template-2	Maintenance	3/2/05	×
Template-3	My Service Requests	8/11/04	×
Template-11	Operations Manager	8/11/04	×
			Cancel

Figure 6-25 Start Center - Modify a Template

3. After you have applied your changes to the template, choose **Save Changes** to save your modifications.

Important: The changes that you did are automatically applied to new instances of the template. Existing instances are updated when the user that the instance is associated to clicks the **Update Start Center** button.

6.4.10 Updating your Start Center instance according to the template

To sync up your Start Center template instance with the Start Center template, either to update it accordingly to the template or to revert to the template after instance configuration, click the icon shown in Figure 6-26.

Update Start Center

Figure 6-26 Update Start Center icon

Attention: Whenever you click this icon, your Start Center instance personalization is lost, and the template that your Start Center instance is based on is reapplied.

6.4.11 Choosing how to display a multi-tabbed Start Center

If a user belongs to more than one security groups, they will see a tabbed view of their Start Centers, one for each security group that they belong to, as shown in Figure 6-27.



Figure 6-27 Multiple Start Center Templates

The user is able to navigate between their own Start Centers and can also select not to display a particular Start Center or to set their user default Start Center. To do this, select **Display Settings** (Figure 6-28).



Figure 6-28 Display Settings Icon

Then click the check boxes beside the available Start Centers (Figure 6-29).

🗟 Display Settings		:?:⊠
Start Centers 👔 🕨 Filter 🔌 👘 👘 👘 👘 🔶 1 - 3 of 3 🔶	Ely Downlo	ad ? =
Description	Display?	Default?
Administration	V	
Inventory	V	
Process Management Requester	V	
	ОК	Cancel

Figure 6-29 Display Settings

If you uncheck one of the Display check boxes, the tab containing the corresponding Start Center is removed.

6.5 Tivoli Provisioning Manager Start Center templates

When you install Tivoli Provisioning Manager V7.1.1, the following new groups are added:

- TPADMIN
- ► TPDEPLOYMENTSPECIALIST
- TPCOMPLIANCEANALYST
- ► TPCONFIGURATIONLIBRARIAN
- ► TPDEVELOPER

Each group has a predefined Start Center template associated with it and is dedicated to a specific role within the provisioning activities.

Tivoli Provisioning Manager Start Center templates can be thought as the user's *morning headlines*. They are tailored to provide users with a launching point for a rich set of system content needed to conduct their provisioning tasks.

The individual data or system concerns that the user might have from this initial summary allows them to drill down for further details and product interaction.

In the following topics, we provide a brief description of the new groups added by Tivoli Provisioning Manager, the roles of the users belonging to each group, and their Start Center templates.

6.5.1 Provisioning Administrator

The Provisioning Administrator user has full control over all provisioning resources and activities.

The Provisioning Administrator's user ID is assigned to the TPADMIN group. Figure 6-30 shows their Start Center template.

	Change Conte	nt/Layout 📲 Display	Settings 📲 Create New	Femplate 🔏 Modify Existing Tem	iplate UB Updat	e Start Ce
box / Assignments 🥔 🖗	🕈 💼 🛛 🥊 Bulletin Board	🔻 Filter 🦚 😕	_	_		
E	Refresh Subject	Message	Post Date	Expiration Date	Viewed?	
escription Due Date Route	<u> </u>				N	
No Assignments found for MAXADMIN			There are currently no bulleti	n board messages to view.		
vorite applications	My favorite repor	ts :	2	<u> </u>		1 -
Provisioning Computers	ing faronto ropor					·
	Successful, faile	d and in-progress pro	visioning tasks			10
Virtualization Management						
	All recent provisi	oning tasks 🛛 💙 Filter :	a 🗅 🖗			10
Software Products						
	Agents status					10
Patches	0.0					
	Software distribu	ition infrastructure co	ommunication status			0
Provisioning Task Tracking	Dopot status					
LAA .	Depor status					* L
	Data model object	t finder i 💗 Filter > 🚜	510			1 =
ovisioning administration applications 2 -	Object			Object Type		
Provisioning Groups						
	Windows Millenniu	n Edition		Software Definition		
Provisioning Permission Groups	Favorite Computers	•		Computer Group		
	Favorite Software			Group		
Provisioning Global Settings	Deployment Engine	Service Access Point		Device Driver		
	SSH Service Acce	ss Point		Device Driver		
Provisioning Workflows	Set Graph Options				1 - 5 of 484	Next Pac
_						
Dynamic Content Delivery Configuration						
Work Order Tracking						
Activities and Tasks						
Discovery Configurations						

Figure 6-30 Provisioning Administrator Start Center

The Provisioning Administrator's main provisioning tasks are:

- To run initial discovery scans and to configure discovery scans needed to maintain the network inventory
- To view and group servers and software according to the needs of the environment
- To import the necessary tools to enable endpoints for receiving deployments, a task that can be run in cooperation with the Deployment Specialist
- To work with a Deployment Specialist to determine the appropriate set of patches required for a specific platform or software product and then to approve the patches that are needed
- To design and test deployments to ensure that they are ready for production, and to work with the Deployment Specialist to prepare for regular deployment into the production environment
- To perform many complex tasks critical to the setup and operation of the deployment environment

- To regularly monitor the deployment environment to ensure that everything is going smoothly, including summary reports
- When troubleshooting is needed, to determine the cause of any problems using available tools and information

6.5.2 Deployment Specialist

The Deployment Specialist is the user who performs the day-to-day deployment tasks using Tivoli Provisioning Manager. Their role can be defined for an area of responsibility, such as specific groups or computers that the user is responsible for maintaining. Many of these tasks can be repetitive, so this user would need a simple and quick Start Center.

The Deployment Specialist's user ID is assigned to the TPDEPLOYMENTSPECIALIST group.

Velcome, new_deployment_specialist		🕑 Web Replay 🕴	<u>B</u> ulletins: (0)	₱ <u>G</u> o To <u>III R</u> eports ₦	Start <u>C</u> enter ¹ <u>P</u> rofile	× Sign Out ?	Help TEM.
	📴 Change Conten	t/Layout 📳 Displ	ay Settings 🕴	Create New Template	A Modify Existing Te	mplate 🛛 🖓 🖓	pdate Start Center
Inbox / Assignments 🥒 🗖 🟦	🔒 Bulletin Board 💘 Filler 🍈 🌾						Ť
Refresh	Subject Messa	ige	Post Date	Expiration I	Date	Viewed?	
Description Due Date Priority Start Date Route						N	
No Assignments found for new_deployment_specialist		Ther	e are currently	no bulletin board messages t	o view.		
Favorite applications 🥒 🖻 👔	Status of my recent provisioning	taska i m Eilen - A	almida				a m m
Provisioning Computers	Status of my recent provisioning	Itasks V Hiter > d	Statue		Start time		
B	TUSK		Julua				
E Provisioning Groups		No Data Found					
Provisioning Task Tracking	Task and compliance KPIs						/ 🗆 🕯
C Discovery Configurations	My Tasks 🔻 Filter > 🕅 🗊 褅						/ 🗆 î
Discovery Wizards	My recent failed provisioning tas	iks ♥ Filter⇒dA	b l i i i i i				/ 🗆 🕯
	My in-progress provisioning task	(S 💗 Filter > dPa 🗄	10				/ 🗆 🖬
Software management applications	My non-compliant computers	Filter v 🗛 🗄 🐂 🕯 🍰					100
Patch management applications	ing non-compliant compaters i						e
	Data model object finder i v Filte	0481512					100
OS management applications	Name			Object Type			
My favorite reports 🗸 Filter > 🏟 🕽 褅 🥒 🔎 🗇 🏦	Favorite Computers			Computer G	oup		
Description	Favorite Software			Group			
	RXA Platform Discovery			Discovery T	/pes		
Are computers compliant with their compliance checks?	TPC Discovery			Discovery T	/pes		
Do Windows computers comply with the patch policy?	TPC Servers			Computer G	oup		
Do Windows computers comply with the patch policy?	Set Graph Options					1 - 5 of 8	62 Next Page >>
How many tasks are in a specific state?							
What computers have never had a compliance check run on them?							
Set Graph Options 1 - 5 of 24 Next Page >>							

Figure 6-31 shows their Start Center template.

Figure 6-31 Deployment Specialist Start Center

The Deployment Specialist performs a limited set of tasks repeatedly and wants a user interface that is simple and fast to use, with no wasted clicks or unnecessary steps.

The Deployment Specialist's main provisioning tasks are:

- To perform day to day deployments of software (OS, patches, software) to computers
- ► To enable computers for Patch Management
- ► To install patches and validate that patches are installed correctly
- To view tasks in progress and monitor problems
- ► To review computer or group compliance
- To perform visual inspection of a computer's inventory and launch a new scan to validate data progress

6.5.3 Compliance Analyst

The Compliance Analyst is the user who checks compliance of resources for which he is responsible.

The Compliance Analyst's user ID is assigned to the TPCOMPLIANCEANALYST group. Figure 6-32 shows their Start Center template.

Welcome, new_compliance_analyst	🕑 Web Replay 🛛 🖡 <u>B</u> ulletins	s:(0) ₱ <u>G</u> oto №1	<u>R</u> eports *	Start <u>C</u> e	nter 🎍 <u>P</u> rofile 🎽 <u>S</u> ign	Out ? <u>H</u> el	° <u>IIM</u> ,
Da Chan	ge Content/Layout 📳 Display Settin	igs 🍓 Create New	Template	🔏 Mo	dify Existing Template	<mark>ଧ</mark> ୍ୟଳ Upda	te Start Center
Favorite applications	👂 Bulletin Board 🛛 💘 Filter 🛛 🏟 👘						Ť
Provisioning Computers	Subject Message	Post Date		Expirat	on Date	Viewed	?
						N	
Provisioning Groups	Т	There are currently no	bulletin boa	rd messa	ges to view.		
Software Configuration Templates	Favorite Compliance Analyst Report	tsivyFilter⇒añAlta	10				/ = =
	Report Description						
Patches							
	Are computers compliant with their comp	pliance checks?					
. Discovery Configurations	Do Windows computers comply with the	e patch policy?					
St creation of the second seco	Do Windows computers comply with the	e patch policy?					
Discovery Witzerde	What computers have never had a comp	pliance check run on th	iem?				
	What computers have patches approved	d for installation?					
	What computers have patches approved	d for installation?					
Provisioning Task Tracking	What is the compliance result of all provi	isioning servers?					
	Set Graph Options					1 - 7 of 18	Next Page >>
Status of my recent compliance tasks 🛛 Filter > 🆓 🕽 🏈 🛛 🥒 🚍 👔	Nen compliant Computers and Crau						4
Provisioning Task Status Task Type Start Date	Non-compliant Computers and Grou	uha					Undata
No Data Found	2.0 -		Related Report	Status	(PI	Actual T	arget Variance
	1.5 -		%1	-	lon-compliant computers (%)	0	0 0
Compliance status of my computers and groups			(i)	- 4	lon-compliant groups	0	0 0
Computer of Group	1.0 -				%)		
cc117177 romelab it ibm com Computer Not compliant							
Sat Graph Ontione	-0.0						
	0	0					

Figure 6-32 Compliance Analyst Start Center

The Compliance Analyst's main provisioning tasks are:

- To guide policies for compliance within the organization and ensure that they are being followed to meet goals
- ► To check the compliance of resources for which that user is responsible
- To assist with specific compliance issues from both a technical and business-related view
- To analyze a list of missing patches and approve, reject, or ignore it for a group or a computer
- ► To review new items in the Catalog and approve, reject, or ignore them for installation on a group or a computer
- ► To restrict patches to a group or a computer
- ► To define groups for compliance

6.5.4 Provisioning Configuration Librarian

The Provisioning Configuration Librarian is the owner of the Inventory Database and is responsible for maintaining its currency and accuracy.

The Provisioning Configuration Librarian's user ID is assigned to the TPCOMPLIANCEANALYST group. Figure 6-33 shows their Start Center template.

아이 Welcome, new_prov_cfg_librarian			🕒 Web Replay	🕴 Bulletins: (0) 🛛 🧖 Go To	In <u>R</u> eports Distart <u>C</u> enter	Profile X Sign Out ? Help	IBM.
		∐ ^{ta} Cha	ange Content/Layout 📳 [Jisplay Settings 🔏 Create	New Template 🔏 Modify Ex	isting Template 🛛 Update Sta	art Cente
Discovery and task applications	/ = 1	👂 Bulletin Board 🛛 🔻 F	liter 🚓 🗇				Û
Discovery Configurations		Subject	Message	Post Date	Expiration Date	Viewed?	
20						N	
Discovery Wizards				There are currently no bulletin	board messages to view.		
Co Patch Acquisition		My favorite reports	🔻 Filter > 🚜 😩 🖗			1	
		Description					
Provisioning Task Tracking							
an an		How many computers a	are installed with which opera	ating systems?			
		How many virtual serve	ers are created on a specific l	host platform server?			
avorite applications	1 = 1	How many virtual serve	ers are created on a specific	host platform server?			
Provisioning Computers		What are the computer	details, including networking	and other resource details?			
8		What computers are in	the data model?				
Virtualization Management		Set Graph Options				1 - 5 of 15 <u>Nex</u>	t Page >
Desulation or guine		Status of my recent p	provisioning tasks 🔻 Filte	er>df0. [D]@		1	- 1
Provisioning Groups		Task		Status	Start time		
Catturara Braduata							
D SUILWAIG FIOLDULA			No Data F	ound.			
Software Configuration Templates							
		Data model object fin	ider 🛛 🔻 Filter > 🏟 🗊 🖓	Nama		1	
Patches		Object Type		ixailie			-
		Device Drives		Default Device Made	1		
		Device Driver		Eavorte Computers	1		
Networking applications	200	Computer Group		Favorite Colliputora			
		Group Device Driver		Deployment Engine 9	Cervice Access Point		
Infrastructure applications	/ 🗆 🖬	Device Driver		SSH Service Access	e Pnint		
		Device Driver		SNMP V1 Service A	ccess Point		
		Device Driver		FTP Service Access	Point		
		Device Driver		Telnet Service Acce	ss Point		
		Device Driver		Telnet TS Service A	ccess Point		
		Device Driver		Stack Of Patches			
		Set Graph Options				1 - 10 of 1165 Nex	kt Page
		and another a provide					

Figure 6-33 Provisioning Configuration Librarian Start Center

The Provisioning Configuration Librarian's main provisioning tasks are:

- To perform various scans as appropriate
- To update records within the database to ensure accuracy
- To edit and run or schedule discovery scanning and inventory tasks
- To create and run reports

6.5.5 Automation Package Developer

The Automation Package Developer is the user who accesses all the Software Packaging Tools and creates automation and packages for deployment.

The Automation Package Developer's user ID is assigned to the TPDEVELOPER group. Figure 6-34 shows their default Start Center template.

utoma	tion development applications 🥒 🖻 🏦	Status of my re	cent provisioning workflows 🔻 Filter > 🕅	1510		/ = 1
101	Provisioning Workflows	Deployment Requ	vest ID Workflow Na	ame	Error Mess	age
0	Provisioning Workflow Status	10,000	Device.Exec	uteCommand		
		Set Graph Option	15			1 - 1 0
Ħ	Provisioning Computers	Status of my re	cent provisioning tasks 🔻 Filter > 🚜 🕽	0		/ = 1
		Provisioning Task	5	Status	Start Date	
40	Virtualization Management					
en.		test@2009/09/18	15:36:25	Success	9/18/09 3:36 PM	
Ĩ,	Provisioning Task Tracking	Graphical View				1 - 1 0
Ê	Provisioning Task Definitions	Data model obje	ect finder 🔻 Filter > dta 🕽 🔗			1 = 1
		Object ID	Object		Object Type	
~	Assignment Manager					
₿\$°		1,419	Windows Millennium Edition		Software Definition	on
		1,004	Favorite Computers		Computer Group	
rovisio	oning administration applications	1,005	Favorite Software		Group	
	Software Products	1,007	Deployment Engine Service Access Point		Device Driver	
10		1,009	SSH Service Access Point		Device Driver	
		1,011	SNMP V1 Service Access Point		Device Driver	
50	Software Product Installation	1,013	FTP Service Access Point		Device Driver	
		1,015	Telnet Service Access Point		Device Driver	
色	Provisioning Groups	1,017	Telnet_TS Service Access Point		Device Driver	
		1,019	Stack Of Patches		Device Driver	
2	Discovery Configurations	Set Graph Option	<u>15</u>		1 - 10 0	of 484 Next Page
6	Device Driver Categories					
•	Device Drivers					
	Dynamic Content Delivery Configuration					

Figure 6-34 Automation Package Developer Start Center

As you can see, this default Start Center is not filled in with customized portlets, as it is for as those associated to the other provisioning groups. In this case, no default application authorization is added for the group, because it is not designed to be used on its own.

Appropriate application authorization can be added by assigning the users in this group to the TPADMIN security group.

Whenever assigned to the TPADMIN security group, the Automation Package Developer's main provisioning tasks are:

- To access to all the software packaging tools and create automation and packages for deployment
- To use the Software Package Editor
- ► To view inventory, workflows, and task status

6.6 Benefits of the new GUI

The Tivoli process automation engine based GUI, available with Tivoli Provisioning Manager V7.1.1, provides a number of benefits compared to the Tivoli Provisioning Manager V57.1.1 GUI.

Role based access

Start Centers can provide focused and role-based access to functions and data.

Powerful customization capabilities

The new GUI enables powerful customization capabilities. It is very easy to customize the Start Centers for different business requirements using drag and drop functionality, such as adding a new KPI graph or adding a new portlet.

For more advanced customizations, you can also use Application Designer, a tool for configuring the user interfaces for Tivoli process automation engine applications. The easy-to-use Application Designer interface enables you to change the appearance of Tivoli process automation engine applications without editing a line of code. The drag and drop functionality built into Application Designer greatly simplifies the process of using this tool.

Application Designer lets you perform the following common modifications to a selected application's user interface:

- Moving fields and sections
- Adding new fields, tabs, and tables with columns and rows

Advanced capabilities include:

- Creating or duplicating applications
- Defining signature options
- Editing the Toolbar or the Select Action menu.

Routing capabilities

The new GUI also provides multi-user routing and work item approval and management capabilities. You can use the GUI for defining multi-user and automated routing assignments and actions, escalations, notifications, and condition-based assignment. These functions are possible thanks to the underlying Tivoli process automation engine platform.

BIRT based reporting

With this version, you get many BIRT-based reports out of the box. You can also create your own reports easily.

Rich security

You also get richer set of security control capabilities for the user interface and data.

Simplified operations

Finally, the new GUI enables stream-lined and simplified operations for some tasks. For example, simple software upload, distribution, and installation is easier compared to V5.1.1.

6.7 Overview of the GUI differences

In the following sections, we compare the Tivoli Provisioning Manager Version 5.1.1.2 and Tivoli Provisioning Manager Version 7.1.1 Graphical User Interfaces.

We compare some of the most common views. The user that we use to compare the graphics is **tioappdmin** on both provisioning servers (V7.1.1 and V5.1.1.2).

6.7.1 Welcome to Tivoli Provisioning Manager versus Start Center

Use this link to access the page:

https://<fully_qualified_hostname>:9045/tcWebUI

See Figure 6-35.



Figure 6-35 Welcome to Tivoli Provisioning Manager

Use this link to access the page:

https://<fully_qualified_hostname>:9443/maximo

See Figure 6-36.

💽 - C 🗙 🏡 🚺 9.168.47.12 http	os://9.168.47.12:9443/maxim	o/ui/login					습 · 😵	• Google		
1ost Visited 🔆 Firefox Help 🔚 Firefox Support 🤌 V	Vindows Live Hotmail 💹 Pluş	g-in FAQ 🖑 playonline.	ntml 🐠 Riepilogo d	e Il mio eBay	@ Canon E(os 400 0 / Di	📄 Contac	t Reference F	ile	
Start Center 🔶										
Welcome, tioappadmin		🕑 Web Reple	ky [●] <u>B</u> uletins: (0)	🖗 <u>G</u> o To	Unt Reports	Start Cente	r Profile	X Sign Out	? Help	IB
	🕼 Chan	ge Content/Layout 🖷	Display Settings	Reate I	lew Templat	te 🔏 Modi	fy Existing T	emplate 🔱	8 Update 9	Start Cent
x / Assignments 🥒 🖙	👔 🛛 🕫 Bulletin Board 🛛 🔻	Filter 🛱 🗇				(and the second				
Re	resh Subject	Message	Post Date)	Expiratio	on Date	_	View	/ed?	
cription Due Date Route				1				N		
No Assignments found for tioappadmin										
			There are curren	ay no pulletin i	board messag	es to view.				
rite applications 🥢 🖻	My favorite reports	Filter ath i th i 🖗								200
Provisioning Computers	ing recorder opento									* 🗆 🗤
	Successful, failed a	nd in-progress provisi	ioning tasks							100
Virtualization Management										
40	All recent provisioni	ng tasks 💗 Filter > 🏤	12 10							100
Software Products										
D Contrate i reducid	Agents status									/ 🗆 🕯
Patches	Software distributio	n infrastructure comr	nunication status							100
Provisioning Task Tracking	Depot status									100
Lac,										
	Data model object ti	nder i V Filter > (Pa 2)	100			Object Trees				2 - U
visioning administration applications 🛛 🥒 🗏	Direct Contex			10 million and		Object Type				
👫 Provisioning Groups	Defer # Device Model					Deutoe Drive				
	Windows Computers					Computer Gr	oup			
Provisioning Permission Groups	AIX Computers					Computer Gr	oup			
Н,	Red Hat Linux Compute	ers				Computer Gr	oup			
	HPUX Computers					Computer Gr	oup			
Provisioning Global Settings	Set Graph Options							1-50	f 1200 N	ext Page
Provisioning Workflows										
Dynamic Content Delivery Configuration										
Work Order Tracking										

Figure 6-36 Start Center

6.7.2 Tracking Tasks

Use this path to access from the GUI:

Task Management \rightarrow Track Tasks.

See Figure 6-37.



Figure 6-37 Track Tasks in 5.1.1.2

Use this path to access from the GUI:

Go To \rightarrow Task Management \rightarrow Provisioning Tasks \rightarrow Provisioning Task Tracking or Favorite Applications \rightarrow Provisioning Task Tracking from the Start Center.

See in Figure 6-38.

🔮 Provisioning Task Tracking - Mozilla Firefo	4).				
Elle Edit View History Bookmarks Tools	Help						
🔇 🔊 - C 🗙 🏠 🛄 5.666	7.12 https://9.16	68.47.	12:9443/maximo/ui/log	in		🗘 🔹 🔀 🕻 Google	Ş
🧟 Most Visited 🔆 Firefox Help 🔚 Firefox Supp	ort 🧳 Windows	Live I	totmail 💹 Plug-in FA	Q 🕃 playonline.html 💇 Riepilogo de	il mio eBay 🛞 Canon	EOS 400D / Di 📄 Contact Reference File	
Provisioning Task Tracking	÷						
Provisioning Task Tracking				🗘 Web Replay 🤚 <u>B</u> ulletins: (0)	r≉ <u>G</u> o To ^{Un} <u>R</u> eports	♥ Start Center ▲ Profile > Sign Out ? Help	IBM.
Find:	🎁 🤝 Select Ac	tion	💌 🚯 📓				
List Task							^
🚵 Advanced Search 👻 🎴 Save Query 👻 🔗	Bookmarks						
Provisioning Tasks 🔻 Filter > 🏟 🗊 🛧 🤞	💠 1 - 20 of 34 🌲					B	> Download
Provisioning Task	Task ID		Status	Start Date 🜩	Created By	Туре	
Run provisioning workflow TCA_PingAgent submitted at August 24, 2009 7:10:21 PM <u>CEST</u>	2,601		Success	8/24 /09 7:10 PM	TIOAPPADMIN	Provisioning Workflow	
Run provisioning workflow. <u>TPM711Migration</u> Security submitted at August 24, 2009 6:19:28 PM CEST	2,600		Success	8/24/09 6:19 PM	MAXADMIN	Provisioning Workflow	
Run provisioning workflow No. operation submitted at August 24, 2009 2:19:40 PM CEST	2,200		Success	8/24/09 2:19 PM	MAXADMIN	Provisioning Workflow	
Install Depot Agent: vmachine8 rot.it.ibm.com	1,405		Success	7/31/09 2:27 PM	TIOAPPADMIN	Provisioning Workflow	
Tivoli Provisioning Manager Inventory Discovery	1,404		Success	7/31/09 1:34 PM	TIOAPPADMIN	Provisioning Workflow	
Initial Discovery	1,403		Success	7/31/09 12:06 PM	TIOAPPADMIN	Provisioning Workflow	
Initial Discovery	1,402		Success	7/31/09 9:37 AM	TIOAPPADMIN	Provisioning Workflow	
Initial Discovery	1,401		Success	7/31/09 9:15 AM	TIOAPPADMIN	Provisioning Workflow	
Install Common Agent	1,023	8	Failed	7/30/09 9:18 PM	TIOAPPADMIN	Provisioning Workflow	
Initial Discovery	1,022		Success	7/30/09 9:17 PM	TIOAPPADMIN	Provisioning Workflow	
Tivoli Provisioning Manager Inventory Discovery	1,400		Success	7/30/09 7:58 PM	TICAPPADMIN	Provisioning Workflow	
Tivoli Provisioning Manager Inventory Discovery	1,021		Success	7/30/09 5:33 PM	TIOAPPADMIN	Provisioning Workflow	4
Tivoli Provisioning Manager Inventory Discovery	1,020		Success	7/30/09 4:41 PM	TIOAPPADMIN	Provisioning Workflow	
Tivoli Provisioning Manager Inventory Discovery	1,050	8	Failed	7/30/09 3:44 PM	TIOAPPADMIN	Provisioning Workflow	
Tivoli Provisioning Manager Inventory Discovery	1,049		Success	7/30/09 3:40 PM	TIOAPPADMIN	Provisioning Workflow	•

Figure 6-38 Track Tasks in 7.1.1

6.7.3 Managing Computers

Use this path to access from the GUI:

Inventory \rightarrow Computers.

See Figure 6-39.



Figure 6-39 Manage Computers in 5.1.1.2

Use this path to access from the GUI:

Go To \rightarrow IT Infrastructure \rightarrow Provisioning Inventory \rightarrow Provisioning Computers or Favorite Applications \rightarrow Provisioning Computers from the Start Center, as shown in Figure 6-40.

🕙 Provisioning Computers - Mozill	la Firefox			
Ele Edit View History Bookma	arks Iools Help			
🕢 🗙 🖯 🐨	9.163.47.12 https://9.168.47.12:9443/maximo	/ui/login		☆ • 🚷 Google
🙍 Most Visited 🔆 Firefox Help 🐜	Firefox Support 🤌 Windows Live Hotmail 💹 Plug	r-in FAQ 🖑 playonline.html 🐠 Rieplic	go de Il mio eBay 🕐 Canon EOS 400D /	Di 📄 Contact Reference File
Provisioning Computers	*			
Provisioning Computers		🕑 Web Replay 🤚 Bulletins	(0) 🍖 Go To 💷 Reports 🕈 Start Qa	nter Albrofile Xign Out ? Help IEM.
Y Find:	🔥 🤝 Select Action 🖌 🔇	🎦 🗟 🧶 🔅 🔶 🔗		
List Computer Hardwa	are Software Compliance Reco	mmendations Credentials	Workflows Variables Deplo	ment Properties
🖄 Advanced Search 🔻 🎴 Save G	Query 🔻 🛷 Bookmarks			
Computors 🛛 🔻 Filter > 💏 🛛 💱 🕴 🛊	🍦 🐳 1 - 3 of 3 ⇒			E Downlos
Computer +	Operating System	Globally Unique Identifier	Agent	Compliance Status
vmachine*				
<u>vmachine4.rot.it.ibm.com</u>	Red Hat Enterprise Linux AS release 4 (Update 6)		TCA-1.3.2.29	No compliance checks configured
vmachine5.rot.it.ibm.com	Red Hat Enterprise Linux Server release 5.1		TCA-1.3.2.29	No compliance checks configured
vmachine8.rot.it.ibm.com	Windows Server 2008 Enterprise Edition		TCA-1.3.2.29	No compliance checks configured
			R,	

Figure 6-40 Manage Computers in 7.1.1

6.7.4 Managing Depots

Use this path to access from the GUI:

Inventory \rightarrow Infrastructure Management \rightarrow Depots.

See Figure 6-41.



Figure 6-41 Manage Depots in 5.1.1.2

Use this path to access from the GUI:

Go To \rightarrow Administration \rightarrow Provisioning \rightarrow Dynamic Content Delivery Configuration or Provisioning administration applications \rightarrow Dynamic Content Delivery Configuration from the Start Center, as shown in Figure 6-42.

😴 Dynamic Content Delivery Configuration - Mozilla F	irefox		- 0
Ele Edit View History Bookmarks Icols Help			
C X 🔬 9.168.47.12 http	ps://9.168.47.12:9443/maximo/ui/login	습 • 😣	🔽 Google 🖉
Most Visited 🔆 Firefox Help 🛸 Firefox Support 🤌	Windows Live Hotmail 💹 Plug-in FAO 🛷 playonline.html	eV Rieplogo de Ilmio eBay 🖗 Canon EOS 400D / Di 📄 Conta	ct Reference File
Dynamic Content Delivery Configura	and a set of the set o		(
Dynamic Content Delivery Configuration	🕑 Web Replay	Pulletins: (0) 🏓 Go To 🔤 Beports 🌴 Start Center 🔺 Brofie	×Sign Out ? Help IEM.
Select Action			
List Depots Regions Zones			
Reports : Filter : A : - + + + + + + + + + + + + + + + + + +			Pi Download 2 📼
Depot	Description	Computer	Status
dyn-9-168-42-96.rot.t ibm.com	dyn-9-168-42-96 rot it.lbm.com	dyn-9-168-42-96 rot it.iom.com) û
vmachine8.rot.it.ibm.com	vmachine8.rot.it.ibm.com	vmachine8.rot.it.ibm.com	Û
			New Row

Figure 6-42 Manage Depots in 7.1.1

6.7.5 Computer Details: Software

Use this path to access from the GUI:

Inventory \rightarrow **Computers**, then search for the computer name. After it is opened, click the **Software** tab. See Figure 6-43.

le Edit View History Bookmarks To	is Help			_
200. C × 🛆 🕅	bitns://risc40	a rot it ihm com 9045/tr/Webi II/index isn/naneId=home	Star Google	
	independing of		M Toroge	
Most Visited 🔅 Firefox Help 🔚 Firefox Si	ipport 🦄 Window	vs Live Hotmail 划 Plug-in FAQ 🖑 playonline.html 🖤 Riepilogo de Il mio eBay 🧶 Canon EOS 400D /	Di 🔄 Contact Reference File	
] Tivoli Provisioning Manager	+			
Tivoli. Provisioning Manager				IBI
tioappadmin 🚴 Log off		🗄 Home 🌟 Welcome 👔 V	Neb Replay 👔 About 💡 i	Information Ce
Collapse All	Co	mputer: vmachine8.rot.it.ibm.com		
Find:	General	Hardware Software Compliance Recommendations Credentials Dis	workflows	(ariables A
Task Management	Edit	riardware compliance recommendations credendals Dis	Soft as Home 6	Refrech 21
Software Management	- colt		Sec as nome 4	With an and a state of the stat
Inventory	Oneratin	system Last Scan Statist	tics	
Manage Inventory	Nindo Windo	ws Server 2008 Enterprise Edition July 31, 2009 1:47:57 PM CEST 19 Pro	ducts Installed / 0 Patche	s Installed
📓 Groups	Agent			
🗄 Computers	CTCA-1.	3.2.29		
Environments				
Access Control Lists	View		Name	
Firewalls	Software P	roducts 🔄 🗖 Show Dependencies	*	Search
In Load Balancers	QG	Delete Uninstall		+
Switches	Select	Name	^ Version	^
Subnetworks		Microsoft .NET Framework	2.0.50727.42	
📇 Virtual LANs			1.2.2.20	
🖧 Storage Area Networks		TCA-1.5.2.29	1.5.2.29	
C Storage Subsystems		TCA-Subagent CDS Axis	1.3.2102	
Storage Pools		TCA-Subagent CDS Client URL Handler	1.3.2102	
Storage Managers		TCA-Subagent CDS Depot	1.3.2102	
		TCA-Subagent CIT Scanner	5.1.5	"
Manage Discovery		TCA-Subagent Common Inventory Technology	2.5.1026	_
Infrastructure Management		TCA-Subagent DMS OSGi Client	182	
Annlications		TCA Culorgent DMC OCCI Client Eutencies for TBM	1.0.2	
		rex-subagencions OSGI Clenc Extension for TPM	1.8.2	8
Reports		TCA-Subagent DMS OSGI Client Http Adaptor	1.0.0	
Reports System Management				
Reports System Management Automation		TCA-Subagent DMS OSGi Client Https Adaptor	1.0.0	
Reports System Management Automation		TCA-Subagent DMS OSGi Client Https Adaptor TCA-Subagent Event Administration	1.0.0 5.1.1000	
Reports System Management Automation		TCA-Subagent DMS OSGI Client Https Adaptor TCA-Subagent Event Administration TCA-Subagent JES	1.0.0 5.1.1000 5.1.2000	
Reports System Management Automation		TCA-Subagent DMS OSGI Client Https Adaptor TCA-Subagent Event Administration TCA-Subagent JES TCA-Subagent SCM	1.0.0 5.1.1000 5.1.2000 5.1.3	

Figure 6-43 Computer Details - Software in 5.1.1.2

Use this path to access from the GUI:

Go To \rightarrow IT Infrastructure \rightarrow Provisioning Inventory \rightarrow Provisioning Computers or Favorite Applications \rightarrow Provisioning Computers from the Start Center, then search for the computer name. After it is opened, click the Software tab, as shown in Figure 6-44.

Provisioning Computers - Mozilla Firefox le Edit View History Bookmarks Tools Help				
C Ear Ten UTen Economica				
S C X 🔬 🛄 9.165.47.12 https://9.16	58.47.12:9443/maximo/u	i/login	값 • Google	
) Most Visited 🔆 Firefox Help 🔚 Firefox Support 🧳 Windows	Live Hotmail 💹 Plug-ir	ı FAQ 🖉 playonline.html 💇 Riepilogo de Il mio eBay 🧟	Canon EOS 400D / Di 📄 Contact Reference File	
Provisioning Computers				
Provisioning Computers		🗢 Web Replay 👎 Bulletins: (0) 🎤 Qo To 💷	Reports 🕈 Start Center 🌲 Brofic 🗶 Sign Out 📍 Help	IBM
💌 Find: 🛛 🧑 🤝 Select Ac	tion 💌 🚯] 🖬 🧶 🍬 🍦 🤪		
List Computer Hardware Software Co	mpliance Recom	nendations Credentials Workflows Va	riables Deployment Properties	
Computer ymachine8.rot.it.ibm.com Last Scan	Operating Syste Age	Mindows Server 2008 Enterprise Edition	Statistics 19 Products Installed / 0 Patches Installed	
¶ All ○ Software ○ Patches				
oftware Installations 🕴 🔻 Filter > 🆚 🗄 🗁 🕴 🔶 🛛 🗢 1 - 10 of 19	*		Et Da	unioad ?
Software Installation	Version	Software Definition	Installable Status	
Windows Server 2008 Enterprise Edition	2008	Windows Server 2008 Enterprise Edition		Û
Microsoft .NET Framework [Version 2.0.50727.42]	2.0.50727.42	Microsoft .NET Framework 2.0.50727.42		Û
TCA-1.3.2.29	1.3.2.29	TCA-1.3.2.29	tested	Û
TCA-Subagent Event Administration	5.1.1000	TCA-Subagent Event Administration	tested	Û
TCA-Subagent SyncML Core	2.5.0	TCA-Subagent SyncML Core	tested	Û
TCA-Subagent SyncML DM	2.5.0	TCA-Subagent SyncML DM	tested	1
TCA-Subagent DMS OSGi Client	1.8.2	TCA-Subagent DMS OSGi Client	tested	Ü
TCA-Subagent DMS OSGi Client Http Adaptor	1.0.0	TCA-Subagent DMS OSGi Client Http Adaptor	tested	û
Adaptor	1.0.0	TCA-Subagent DMS OSGi Client Https Adaptor	tested	Û
TCA-Subagent Tivoli Provisioning Manager	5.1.2000	TCA-Subagent Tivoli Provisioning Manager	tested	Û
			Add software unneta	ISOTWARE
			\$	

Figure 6-44 Computer Details - Software in 7.1.1

6.7.6 Workflow Status

Use this path to access from the GUI:

Automation \rightarrow Workflow Status. See Figure 6-45.



Figure 6-45 Workflow Status in 5.1.1.2

Use this path to access from the GUI:

Go To \rightarrow Task Management \rightarrow Provisioning Tasks \rightarrow Provisioning Workflow Status, as shown in Figure 6-46.

🔇 🚬 🗸 C 🗶 🏠 📑 9.168.47.12 https://9.168.47.12:9443/maximo/ui/login							
Most Visited	lp 🔚 Firefox Support 🧦 Windows Live Hotm	ail 💹 Plug-in FAQ 🛛	🛞 playonline.html 🛯 🕸 Riepilogo de	Il mio eBa	y 😢 Canon EOS 4000) / Di 📄 Contact Reference F	ile
Provisioning Workflow 9	Status ÷				and the second		
Provisioning Workflo	w Status		C Web Replay Puletins: (0)	<i>Ф</i> <u>Q</u> о То	La Reports 🏟 Stert	Center 🏾 Profile 🛛 Sign Out	? Help II
Y Find:	👘 🔻 Select Action	💌 \Rightarrow 🔹 🖸					
st Execution Logs							
Advanced Search 👻 📓	Save Query 🔻 🛷 Bookmarks						
olovment Requests 🛛 💌	Filter⇒n∰n i⊒ i∳ 🎍 i⇔ 1 - 20 of 70 🍝						El Download i ?
Deployment Request	Workflow Name		Start Date 👙		Status		
		1					
13,601	TCA_PingAgent	1	8/24/09 7:10 PM		Success	1	>
13,600	TPM711Migration_Security	1	8/24/09 6:19 PM		Success	1	>
<u>13,200</u>	No_operation	1	8/24/09 2:19 PM		Success	1	
12,800	master_tcdriver_update_	1	8/11/09 1:38 AM		Success	1	
12,404	MS_SDI_Config_Offline	1	8/4/09 11:02 PM	- 63	Failed	1	>
12.403	TivoliCommonAgent_Upgrade_DeviceModelHel	1	8/4/09 11:01 PM		Success	1	>
12,402	YUM_Configure_TCDriver	1	8/4/09 10:54 PM		Success	1	>
<u>12,401</u>	TCAupgrade_CreateSPBs	1	8/4/09 10:50 PM		Success		>
12,400	UnzipSWDCLI	1	8/4/09 10:48 PM		Success	1	>
12,020	TCA_PingAgent	1	7/31/09 7:06 PM		Success	1	>
12,005	Instail_CDS_Depot	1	7/31/09 2:27 PM		Success		>
12,004	Discovery.OnDevice	1	7/31/09 1:34 PM		Success	1	>
<u>12,003</u>	InitialDiscovery	2	7/31/09 12:06 PM		Success		>
<u>12,002</u>	InitialDiscovery	1	7/31/09 9:37 AM		Success	1	>
12,001	InitialDiscovery	1	7/31/09 9:15 AM		Success	1	>
11,664	Instail_Agent	1	7/30/09 9:18 PM	8	Failed	1	>
<u>11,663</u>	InitialDiscovery	1	7/30/09 9:17 PM		Success	1	>
<u>12,000</u>	Discovery.OnDevice	1	7/30/09 7:58 PM		Success	1	>
<u>11,662</u>	Discovery.OnDevice	1	7/30/09 5:33 PM		Success	1	>
<u>11,661</u>	Discovery.OnDevice	1	7/30/09 5:33 PM		Success	1	>
11,661 Select Records	Discovery.OnDevice	,	7/30/09 5:33 PM		Success	,	:

Figure 6-46 Workflow Status in 7.1.1

180 IBM Tivoli Provisioning Manager V7.1.1: Deployment and IBM Service Management Integration Guide

7

Integrated Service Management with IBM Service Management Software

In this chapter we provide an overview of an integrated approach to the IBM solution set, which can provide faster time to value, scalability, and a preservation of your investment.

We describe a sample customer scenario and the various integration points of Tivoli Provisioning Manager with the other IBM Service Management products. We only give a high level overview of these integrations. Detailed scenarios of these integrations can be found in subsequent chapters of this part of the book.

We cover the following topics:

- "IBM Service Management solutions" on page 182
- "For details about such benefits, see Tivoli Provisioning Manager integration with IBM Service Management at:" on page 182
- "Tivoli Provisioning Manager in the context of Service Management" on page 183
- "Customer scenario" on page 185

7.1 IBM Service Management solutions

As discussed in 2.1.5, "An integrated Service Management portfolio on top of the Tivoli process automation engine" on page 23, IBM Service Management offerings provide a complete solution, automating the full life cycle of service requests, incidents, and trouble tickets from their creation through to the environmental changes that they produce.

IBM Service Management products are integrated to capture incoming requests, incidents, and problems; route them to the correct decision-makers; and expedite resolution with enterprise-strength server and desktop provisioning tools. They do this while keeping an accurate record of all the Configuration Items in a federated management database and a real-time picture of the deployed infrastructure, thus matching hardware and software services with the business needs that they fulfill.

By automating change, configuration, provisioning, release, and asset management tasks, IBM Service Management software helps to reduce cost and eliminate errors.

Hence, with such a solution, an example of anticipated results would be:

- Improved resource utilization, resulting in a 50% decrease in the need for new additional equipment
- Labor savings of 10-20% (reduced man-hours due to task automation and software distribution)
- Increased productivity of supported services by 10-25%
- Improved success rate for change and release deployments by 10-30%
- 10-20% reduction in deployed application rollbacks
- 84% reduction in time taken to inventory physical and software assets
- IT staff cost savings of \$120 per PC/device/year through the use of Packaging Tools and Automated Software Distribution.
- Reduced labor cost of 10-40% to maintain multiple configuration databases

For details about such benefits, see *Tivoli Provisioning Manager integration with IBM Service Management* at:

http://www-01.ibm.com/software/tivoli/solutions/service-delivery/

Tivoli Provisioning Manager can be integrated with IBM Service Management by creating entries in the IBM Service Management user interface, called launch entries. These entries, which are menu items, can be configured to connect to a Tivoli Provisioning Manager server.

In doing this, you can select the menu item to open Tivoli Provisioning Manager from the IBM Service Management user interface to view the details of a particular Configuration Item or actual Configuration Item, for example, the details for a computer.

IBM Service Management provides an integrated platform for IBM products and external products to provide the users with consistent information about their IT resources and repeatable processes, that are used to manage their infrastructure. The benefits of this are improved service efficiency and the maintenance of accurate configuration data throughout the various products used.

7.2 Tivoli Provisioning Manager in the context of Service Management

The integration of Tivoli Provisioning Manager with IBM Service Management can be achieved by using the *launch in context* application within IBM Service Management. This allows you to open an external application from within IBM Service Management, in this case, Tivoli Provisioning Manager, which will result in automatically taking you to the correct details page of the Configuration Item that you require information about.

As an example, suppose that a request for change is received by the service desk to install some software on a particular computer. The operator would then search for the computer system within the actual Configuration Item list, in the IBM Service Management application and from there would use the defined menu item to start the Tivoli Provisioning Manager application and go directly to the details page for the computer system, from where they can then carry out the deployment process.

Figure 7-1 shows possible use cases where Tivoli Provisioning Manager delivers the task automation in the context of a service request, initiated by Tivoli Service Request Manager.



Figure 7-1 Use cases

Tivoli Service Request Manager provides an integrated service desk and catalog for a *one touch* IT experience. This integrated service desk software unifies and automates key service support and asset management processes. It also:

- Manages both call-based and catalog-based requests in one solution with integrated service desk software and service catalog.
- Takes problem and incident management software to another level with best practice incident and problem processing.
- Enables users to obtain IT services through published service offerings.
- Takes advantage of proven workflows and for fast time to market.
- Employs change and configuration management software features, such as easy drag and drop window, workflow customization and simple configuration tools for on-the-fly changes.
- Combines upgradeability, easy configuration, customer-built customizations and data preservation during updates/upgrades so you never rebuild your service desk again.

7.3 Customer scenario

Our fictitious sample customer, Redbooks-Inc, is an outsourcing company that is managing multiple customer accounts. As part of their delivery commitments, Redbooks-Inc is providing a service management solution to their customer. This solution has to include the following elements:

- Workflow/task management
- End-to-end service provisioning
- Resource provisioning
- Agentless resource discovery
- Configuration Management and Change Tracking Database
- Performance and availability reporting

The first customer of Redbooks-Inc has the following environment:

- There are two data centers, each with 500-1000 servers, and each with localized administration teams.
- Location 1 is the customer headquarters, where the procurement, helpdesk, and majority of business decisions makers and project delivery leaders are located. This location is the heart of the Redbooks-Inc Strategic Business operations.
- Location 2 is where the majority of Redbooks-Inc employees are located. The employees sitting here would access the management solutions across a high speed network link to Location 1.



Figure 7-2 Redbooks-Inc environment

All work requests from users have to be entered into the in-house *Process Request* system, or into the in-house procurement systems.

7.3.1 Service provisioning scenario using TADDM, CCMDB, Tivoli Service Request Manager, and Tivoli Provisioning Manager

With an integrated solution, the following steps show how the processes can be integrated to provide operational value to the customer:

- 1. The customer has deployed TADDM, CCMDB, Tivoli Service Request Manager, and Tivoli Provisioning Manager in the environment.
- 2. The thousands of components in the environment are discovered using TADDM. The components include resource such as servers, operations systems, database applications, Web servers, application servers, and middleware. The various relationships between these components are also discovered.

- 3. A business user makes a service request to commission a new service. This service consists of three new servers, two VLANs, and a software application stack. The service request is created in Tivoli Service Request Manager.
- 4. The approval steps in this process are performed, and an Incident, work order, and job plan are created. This then drives Tivoli Provisioning Manager to perform the resource provisioning of the servers, VLANs, and software.

7.3.2 Outage remediation scenario using Tivoli Provisioning Manager and Tivoli Service Request Manager

This scenario shows integration across people, processes, data, and products, hence providing one end-to-end solution for the customer:

- 1. An end user experiences a problem with the their payroll application. The payroll application is timing out and showing severe performance problems when navigating between different windows.
- 2. The end user calls the help desk and a service request is created,
- 3. The Incident Analyst diagnoses the user's problem and determines that the WebSphere Application Server used by the payroll application is running out of memory. The analyst does an emergency restart of the WebSphere Application Server. This activity is then logged with the Incident.
- 4. To determine the root cause of this application issue, a Problem is now created in the Tivoli Service Request Manager, which is related to this Incident.
- 5. The Problem Analyst investigates this Problem and determines that the memory leakage is occurring due to the WebSphere Application Server missing a patch.
- 6. A Change Request is then created to install the appropriate patch on the WebSphere Application Server.
- 7. The Change Manager reviews the Change Request, documents the impact of the Change, and schedules the patch install to a Change window.
- 8. The Deployment Specialist then dispatches the Tivoli Provisioning Manager operation, which causes a Tivoli Provisioning Manager task to install the patch successfully.
- 9. The Problem and Incident are then resolved, by the Problem Specialist and Incident Specialist, causing the service request to automatically be resolved.

These steps are illustrated in Figure 7-3.



Figure 7-3 Outage remediation scenario using Tivoli Provisioning Manager

See Chapter 10, "IBM Service Management integration scenarios: Incident Management integration with Tivoli Service Request Manager and ITIL" on page 271 for detailed coverage of an Incident Management scenario using Tivoli Provisioning Manager and Tivoli Service Request Manager.

7.3.3 Tivoli Provisioning Manager TADDM Discovery and synchronization process

As shown in the Figure 3 below, the Tivoli Provisioning Manager TADDM Discovery will programmatically insert, update, and synchronize the following resources and the associations without requiring additional manual process:

1. Network elements (switch and routers with NIFs, as well as a GUID for the network elements).

Note: The term *GUID* stands for *Globally Unique Identifier*. It is a special type of identifier used in software applications to provide a reference number that is unique in any context.

- 2. Computer Systems (IP, Macaddress, NIF: set a management interface, hardware/system resources: machine model/serial number/manufacture, processor type/size/frequency, disk partition/size/model/manufacturer, floppy/ CDROM information, memory size, Computer System GUID)
- 3. Operating System Information (OS name/version/fix pack/capability/ requirements, OS installation GUID, OS installation and OS device model association, OS software definition association with OS software installation, OS software installation SRTs synchronization
- 4. Software Installations (Software installation and software model association, Software installation GUID)
- 5. Composite Applications (Software installation/instances/SRTs and software installation and software definition association, device model/workflow association for the following applications: WebSphere Application Server, Oracle, DB/2, http server, Apache, Web logic, IIS, set Software installation and software instance level GUID)
- 6. Service access point (create SAP based on the access list received from TADDM for the computers)
- 7. TADDM computer groups
- 8. TADDM business application and tier mappings in Tivoli Provisioning Manager



Figure 7-4 Tivoli Provisioning Manager TADDM Discovery and synchronization

Managing discovered resources

The following scenario use cases can be run without additional manual steps after the discovery:

- 1. Run an inventory report for collecting targets, OS, software, and hardware information.
- 2. On WebSphere Application Server, by using the existing WebSphere Application Server automation package:
 - a. Run the WebSphere Application Server updateDCM workflow to update the current WebSphere Application Server running states.
 - b. Start and stop the WebSphere server instance using the Tivoli Provisioning Manager console.

Note: If WebSphere Application Server security is on, the user only needs to set the WebSphere Application Server admin userid /password inside SRT; if WebSphere Application Server security is not on, no manual steps are required.

c. Upgrade WebSphere Application Server to the latest fix pack using the Tivoli Provisioning Manager console.

Note: The user only needs to manually configure file repository to include the fix pack binary and the location to get the fix pack.

- d. Clone a new WebSphere Application Server base installation to a new target based on the discovered SRTs.
- e. Uninstall WebSphere Application Server.
- 3. On Oracle, by using the existing Oracle automation package:
 - a. Run the Oracle updateDCM workflow to update the current Oracle running states.
 - b. Start and stop the Oracle server instance using the Tivoli Provisioning Manager console.
 - c. Uninstall Oracle (assuming that the current Oracle AP supports the uninstall operation).
- 4. On DB2, by using the existing DB2 automation package:
 - a. Run the DB2 updateDCM workflow to update the current DB2 running states.
 - b. Start and stop the DB/2 server instance using the Tivoli Provisioning Manager console.
 - c. Clone a new DB2 base installation to a new target based on the discovered SRTs (software resource templates).
 - d. Uninstall DB/2 (assuming that the current DB2 AP supports the uninstall operation).
- 5. On IBM HTTP Server, by using the existing HTTP server automation package:
 - a. Run the IBM Http Server updateDCM workflow to update the current HTTP server running states.
 - b. Start and stop the IBM HTTP server instance using the Tivoli Provisioning Manager console.
 - c. Uninstall the IBM HTTP server installation.
- 6. On Apache Server, by using the existing Apache server automation package:
 - a. Start and stop the Apache server instance using the Tivoli Provisioning Manager console.
- 7. On the operating system:
 - a. Run and check OS compliance.
- 8. Manage TADDM computer groups and TADDM business applications from the Tivoli Provisioning Manager console.

See Chapter 8, "IBM Service Management integration scenarios: TADDM Discovery" on page 195 for implementation details about Tivoli Provisioning Manager and TADDM Discovery.

7.3.4 Software installation, compliance, and remediation scenario

In this scenario, we can use Tivoli Provisioning Manager for compliance and remediation management:

- 1. Define Software compliance rules for software installations. (What is the desired states and what are the recommendations and workflows to be run for remediation?)
- 2. Run TADDM Discovery.
- 3. Run a software compliance check for software installations against the desired states.
- 4. Approve recommendations and run the remediation workflow—for example, upgrade the software level or uninstall software.



Figure 7-5 Software installation, compliance, and remediation scenario

See Chapter 9, "IBM Service Management integration scenarios: Compliance and remediation with TADDM" on page 217 for a compliance and remediation scenario.

7.3.5 Change scenario using Tivoli Provisioning Manager and Change Management

Here we describe a typical scenario to implement a Request For Change (RFC) to install an anti-virus update to a computer:

- 1. Change Requester: Submits RFC to install anti-virus update on a computer.
- 2. Change Manager: Accepts RFC and assigns owner.
- 3. Change Owner: Assigns a Job Plan.
- 4. Change Owner: Initiates the activities in the change plan.
- 5. Change Owner: Confirm Tivoli Provisioning Manager task and targets.
- 6. Deployment Specialist: Implements the Change by using Tivoli Provisioning Manager to Install the anti-virus update on the computer.
- 7. Change Owner: Review Change Implementation.
- 8. Change Manager: Close RFC.

See Chapter 11, "IBM Service Management integration scenarios: Problem and Change Management integration with Tivoli Service Request Manager and CCMDB" on page 325 for a Change Management scenario.



8

IBM Service Management integration scenarios: TADDM Discovery

In this chapter we discuss the integration of Tivoli Provisioning Manager 7.1.1 with Tivoli Application Dependency Discovery Manager 7.1.2. This chapter contains information about discovering and working with computers and software applications in Tivoli Provisioning Manager using information leveraged from Tivoli Application Dependency Discovery Manager.

We cover the following topics:

- "Introduction to TADDM integration with Tivoli Provisioning Manager" on page 196
- "Discovering applications in Tivoli Provisioning Manager" on page 203
- "Working with discovered applications in Tivoli Provisioning Manager" on page 209

8.1 Introduction to TADDM integration with Tivoli Provisioning Manager

With the ever growing complexity of today's applications, keeping track of which applications are installed on which servers, and how they relate to one another, can be a cumbersome task. Tivoli Application Dependency Discovery Manager (TADDM) provides the ability to find detailed information about applications and their relationships to each other in your infrastructure. Through the various levels of sensor discoveries provided out-of-box, TADDM discovers information about the structure and configuration of applications in your environment. This information is consolidated in a single Configuration Manager Database (CMDB).

After this complex data has been gathered by TADDM, it can be imported into Tivoli Provisioning Manager by running a *TADDM Discovery*, which will probe the TADDM CMDB and map software configuration data to software resources in Tivoli Provisioning Manager's Data Center Model. Doing this allows you to view information about computers and associated software applications, and gives you the ability to control them from the same interface.

Integration with TADDM is just one of the IBM Service Management integration scenarios made possible in Tivoli Provisioning Manager v7.1.1. In this chapter, we introduce a complete picture of IBM Service Management Integration in Tivoli Provisioning Manager v7.1.1. We then take a closer look at TADDM Discovery, illustrated by a scenario in which we discover computers through TADDM with Oracle WebLogic Server installed.

8.1.1 Lab environment: IBM Service Management integration scenarios

Figure 8-1 represents the lab environment used for all IBM Service Management integration scenarios described in this Redbooks publication. The diagram shows the details about the installed components.

NC117218 hosts the main IBM Service Management components:

- Tivoli Change and Configuration Management Database (CCMDB)
- Tivoli Services Request Manager
- Tivoli Provisioning Manager

NC125095 hosts Tivoli Application Dependency Discovery Manager (TADDM). The TADDM server is used to discover Windows targets (NC117177 in the picture) through a Windows Gateway installed on NC117217, and UNIX/Linux targets (LINUXTGT in the picture) through a direct ssh connection.

Discovered Configuration Items (CIs) are imported to the Configuration Management Database (CMDB) hosted by NC117218 through IBM Tivoli Integration Composer (ITIC) installed on NC117175. TADDM data regarding software levels and software configurations are imported to Tivoli Provisioning Manager using the "TADDM Discovery" method, which leverages TADDM APIs to create computers and related information in the Tivoli Provisioning Manager data center model (DCM).

As a consequence of such integration, a computer that has been defined in the CMDB by ITIC and in the Tivoli Provisioning Manager Data Center Model by TADDM Discovery will be univocally identified in both CMDB and the Data Center Model by its Globally Unique Identifier (GUID).



Figure 8-1 Lab environment for the IBM Service Management Integration scenarios

Deployment activities leveraging the Tivoli Provisioning Manager scalable distribution infrastructure (SDI) exploit a Tivoli Provisioning Manager Depot installed on NC117175. As shown in the picture, such architecture implies a polling activity from Tivoli Common Agent to Tivoli Provisioning Manager server

in order to retrieve the list of active jobs (inventory scans, software distribution, or endpoint tasks related to the specific Tivoli Common Agent). Software deployment activities are then performed through the Depot designated for the Region that includes the specific Tivoli Common Agent.

8.1.2 Installed components

Next we describe the installed components on each system:

- NC117218 (Windows Server R2 Enterprise x64 Edition SP2):
 - Middleware components:
 - IBM DB2 Enterprise Server Edition v9.5 plus fix pack 3a
 - IBM WebSphere Application Server Network Deployment v6.1 plus fix pack 23
 - IBM HTTP Server v6.1 plus fix pack 23
 - IBM Tivoli Directory Server v6.2 plus interim fix 2
 - Tivoli Change and Configuration Management Database 7.1.1 plus fix pack 5, which includes:
 - Base Services 7.1.1.5
 - Tivoli Service Request Manager 7.1 plus fix pack 4, which includes:
 - Tivoli Service Request Manager Service Desk 7.1.0.4
 - Tivoli Service Request Manager Service Catalog 7.1.0.4
 - Tivoli Service Request Manager Search 7.1.0.3
 - Tivoli Provisioning Manager 7.1.1, which includes:
 - Base Services 7.1.1.5

Important: Tivoli Provisioning Manager Base Services includes the same components as Tivoli Change and Configuration Management Database 7.1.1 (CCMDB), except for Toolbox Web Replay. Therefore, the installation of Tivoli Provisioning Manager Base Services on a system that already hosts CCMDB Base Services will only add Toolbox Web Replay 7.1.1.

- Core Components 7.1.1
- Web Components 7.1.1
- NC125095 (Windows Server 2003 EE SP2 32-bit)
 - Middleware components:
 - IBM DB2 Enterprise Server Edition v9.5 plus fix pack 1
 - Tivoli Application Dependency Discovery Manager 7.1.2 plus fix pack 1

- NC117175 (Windows Server 2003 EE SP2 32-bit)
 - IBM Tivoli Integration Composer 7.1.1 plus fix pack 4
 - Tivoli Provisioning Manager 7.1.1 Depot
- NC117217 (Windows Server 2003 EE SP2 32-bit)
 - TADDM 7.1.2.1 Windows Gateway
 - Bitvise WinSSHD 4.26

Note: Bitvise WinSSHD allows Windows Gateway to connect to TADDM by SSH. Cygwin sshd 4.x is supported as well for this function. TADDM Windows Gateway binaries are downloaded automatically on the system during the first discovery. Therefore, there is no need to install it on the system.

- NC117177 (Windows Server R2 Enterprise x64 Edition SP2)
 - Tivoli Common Agent 1.4.2.0
- LINUXTGT (Red Hat Enterprise AS release 4 update 5)
 - Oracle WebLogic Server 9.2
 - Oracle WebLogic Server 10.3

8.1.3 Tivoli Provisioning Manager and TADDM life cycle

Now that we have introduced the IBM Service Management integration environment, we take a closer look at the TADDM integration life cycle. The environment illustrated in Figure 8-2 contains Tivoli Provisioning Manager V7.1.1), Tivoli Application Dependency Discovery Manager V7.1.2, a TADDM Windows Gateway, one Windows target and one Linux target.

In step one, TADDM sensors are used to discover information about devices. Active targets contained within the user-defined scope are first detected by attempting to establish a connection over several TCP ports. By receiving a response on any port, TADDM is able to determine that the device exists.

Following this assertion, TADDM attempts to establish an SSH connection with each device, either directly, or through a Windows Gateway server if one is available. After a connection is established, a computer sensor is run to determine which operating system is installed. Operating system and application specific sensors are used to discover operating system and software application details. If TADDM fails to establish an SSH connection, an SNMP sensor is launched.



Figure 8-2 Tivoli Provisioning Manager-TADDM life cycle

The next step is to import data discovered by TADDM into Tivoli Provisioning Manager, which is done by running a TADDM Discovery from the provisioning server. The TADDM Discovery requires communication between the Tivoli Provisioning Manager server and the TADDM server on a single port (the default is 9530). Data discovered in the previous step is extracted from the TADDM database and mapped to Tivoli Provisioning Manager's Data Center Model. No communication between Tivoli Provisioning Manager and target computers takes place during a TADDM Discovery.

The third step is to enable direct communication between the provisioning server and target computers in order to take advantage of Tivoli Provisioning Manager's ability to control discovered computers and software applications. Methods to establish this communication will be discussed later in this chapter.

Important: In cases where there is a firewall between the provisioning server and the TADDM server, TADDM Discovery data might not be brought into DCM. In this case, you need to configure the provisioning server and the TADDM server to be able to pass the firewall first, before the discovery can be run.

A simple test to verify this is to ping the IPs between the TADDM and provisioning servers and make sure you can get the positive response back.

8.1.4 Supported applications in Tivoli Provisioning Manager

The TADDM Discovery mechanism in Tivoli Provisioning Manager V7.1.1 provides two types of discoveries: hardware discovery and software discovery.

Note: Additionally, the TADDM Discovery can also discover TADDM collection objects and bring them into Tivoli Provisioning Manager as the static groups. At the time of writing this book, the only collection object brought into Tivoli Provisioning Manager was the computer collection.

The TADDM Discovery can also discover the business applications from TADDM and then create Tivoli Provisioning Manager customer, application, and application tier structure in DCM.

With the hardware discovery, the network and system resources are imported from the TADDM server. With the software discovery, the installed software, as well as configuration details for applications such as DB2, Oracle, Web servers, WebSphere Application Server, WebLogic Server, and VMWare ESX, can be imported.

More specifically, the versions of out-of-the -box discoverable applications are:

- ► DB2:
 - IBM DB2 Universal Database Enterprise Server Edition Version 7
 - IBM DB2 Universal Database Enterprise Server Edition Version 8
 - IBM DB2 Universal Database Enterprise Server Edition Version 9
- Oracle Database:
 - Oracle Database 9i
 - Oracle Database 10g
- Web Servers:
 - Apache Web Server Version 1.3
 - Apache Web Server Version 2
 - IBM HTTP Server Version 1.3
 - IBM HTTP Server Version 6
- WebLogic Server:
 - Oracle WebLogic Server 8.1
 - Oracle WebLogic Server 9.2
 - Oracle WebLogic Server 10.3

- WebSphere Application Server:
 - IBM WebSphere Application Server Version 6.0
 - IBM WebSphere Application Server Version 6.1
 - IBM WebSphere Application Server Network Deployment Version 6

Additionally, the TADDM Discovery will define the operating system for discovered computers for the following platforms:

- ► AIX:
 - AIX 4.3
 - AIX 5.1, 5.2, 5.3
- ► HP-UX:
 - HP-UX 11.0
 - HP-UX 11i v1, v2
- ► Linux:
 - Red Hat Enterprise Linux AS release 3, 4
 - Red Hat Enterprise Linux ES release 3, 4
 - Red Hat Enterprise Linux Server release 5, 5.1, 5.2
 - Red Hat Linux release 7.3, 8.0, 9
 - SUSE Linux Enterprise Server 8, 9, 10
- ► Sun:
 - Solaris 5.8, 5.9, 5.10
 - Solaris 7, 8, 9, 10
- ► Windows:
 - Windows 2000 Server, Advanced Server
 - Windows 2000 Server SP4, Advanced Server SP4, Professional SP4
 - Windows Server 2003 Standard Edition, Enterprise Edition, Data Center Edition
 - Windows Server 2003 SP1 Standard Edition, Enterprise Edition
 - Windows Server 2003 SP1 R2 Enterprise Edition
 - Windows XP Professional
 - Windows Vista® Ultimate, Enterprise
 - Windows 2008 Standard, Enterprise

Tivoli Provisioning Manager is flexible in its ability to discover operating systems and applications that are not supported by default. You can discover unlisted operating systems by editing the discovery-resource-map.xml (included in the *TADDMDiscovery automation package*) to include the desired operating system mapping.

Tip: When adding additional mapping for operating systems or applications in discovery-resource-map.xml, you need to restart the provisioning server to pick up the changes. You can use the following commands to stop it:

```
cd $TI0_HOME/tool
./tio.sh stop -t
```

After the provisioning server is stopped, you can run the following command to start it:

./tio.sh start -t

Tivoli Provisioning Manager also provides a mechanism that allows you to plug in your own discovery implementation for custom composite applications.

In this chapter, we focus on the process of discovering WebLogic servers on a Red Hat Enterprise Linux AS 4 computer.

8.2 Discovering applications in Tivoli Provisioning Manager

Discovering applications in Tivoli Provisioning Manager is a two-step process. First TADDM is used to discover the applications, and then Tivoli Provisioning Manager is configured to use TADDM. We explain these steps in the following sections:

8.2.1 Discovering applications in TADDM

Prior to running a TADDM Discovery from Tivoli Provisioning Manager, the environment details must first have been discovered by the TADDM sensors. Within TADDM, running a sensor discovery involves first creating a scope specifying which computers to discover in the network, as well as an access list detailing authentication for computers and applications in your infrastructure. In some cases, a custom discovery profile might need to be created in TADDM to capture useful configuration details about applications. For example, WebSphere requires a "deep" discovery on the cell level for many of its configuration details to be discovered by TADDM. Most applications of interest, such as DB2, Oracle, Web servers and WebLogic servers, can be discovered using the default *Level 3 Discovery* sensor discovery in TADDM.

For more information about TADDM sensors, see the IBM Tivoli Application Dependency Discovery Manager 7.1.2 product documentation.

8.2.2 Configuring Tivoli Provisioning Manager to use TADDM

In order to import data from TADDM, you need to configure Tivoli Provisioning Manager to communicate with your TADDM server. By default, a discovery configuration called *Tivoli Application Dependency Discovery Manager Discovery* is created during the Tivoli Provisioning Manager installation. This can be configured to communicate with your TADDM server.

In some cases, you might require multiple discovery configurations for the same discovery method. For example, if your infrastructure contains more than one TADDM server, or there is a need for different scopes for multiple sets of computers, a new discovery configuration can be created.

Creating a TADDM Discovery

Perform the following steps to create a TADDM Discovery:

- 1. From the *Discovery Configurations* application, click the **New Discovery Configuration** icon from the application menu bar. An Add Discovery Configuration form is displayed as a pop-up.
- 2. Enter a name and description for your discovery.
- 3. Then, under the Discovery Configuration heading, select the appropriate Category. Because TADDM Discovery has the ability to discover both hardware and software resources, it can be found under both the Hardware Discovery and Software Discovery categories.

- 4. After you have the correct category selected, click the magnifying class icon to select a discovery method. This produces a new pop-up displaying the available discovery methods for the selected category, as shown in Figure 8-3.
- 5. In the Select Value pop-up, click **TADDM Discovery**.
- 6. Click **OK** to create the discovery.

		SelectValue
🖣 Add Discov	very Configuration	
		Method > Filter > 🚜 📰 🛧 🥥 🔶 1 -6 of 6 🔿 📑 <u>Download</u> - ? 🚍
		Device Model
		Discover Devices (computers, switches,
Discovery D	etails	routers) using SNMP
	Name* IADDIVIDIs covery	Discover Computers using RXA
	Description Discover applications from IADDM	Microsoft Active Directory Discovery
Discovery C	onfiguration	Tivoli Provisioning Manager Inventory
Category		<u>Discovery</u>
Hardwar	e Discovery	TADDM Discovery
 Software Other 	Discovery	TADDM Discovery On Device
		Cancel
Method	TADDM Discovery	
Description	Discovers resources from Tivoli Application Depend Resources that can be discovered include compute operating systems, software components, composite server, ND server, DB2, Oracle, Web Servers (IBM Htt Server etc. The discovery can be run against a set of against one or more computers based on fully quali	dency Discovery Manager. rs, computer hardware and network resources, a applications such as webSphere standalone by Server, Apache Server, MS IIS), Weblogic f selected components. It can also be run fied computer names.
	ANAY.	OK Cancel

Figure 8-3 Creating a new TADDM Discovery configuration

Tip: In Tivoli Provisioning Manager V7.1.1, a new feature has been added for TADDM Discovery to allow processing TADDM endpoints for discovery in batch, to control how many computers in TADDM that TPM/TADDM discovery will process in a batch, because if Tivoli Provisioning Manager queries TADDM to get the information about a number of computers, in cases where there are large numbers of computers to be processed, a TADDM query might time out and result in the failure of running TPM/TADDM discovery.

The default value for the batchSize is 100. It means to process 100 computer systems from the TADDM server at a time. However, you can change it by updating the properties file called /resource/io_tuning.properties under the TADDMDiscovery automation package (the same location as discovery-resource-map.xml).

The properties file can be found under:

%TIO_HOME%/lwi/runtime/tpm/eclipse/plugins/TADDMDiscovery/resource/

Configuring TADDM Discovery

From the **Discovery Configurations** application, search for the TADDM Discovery that you want to configure. You can search for all TADDM Discovery configurations by filtering "TADDM" on the Method field. Click the discovery configuration that you want to edit.

On the **Server Information** tab of the TADDM Discovery configuration, as shown in Figure 8-4, provide details about your TADDM Server. Tivoli Provisioning Manager will use the fully qualified host name, port number, and user login information provided here to communicate with your TADDM server. After you have entered the required information, click the **Save** icon on the application menu bar to save your configuration.

SQ Discov	very Confi	gurations		C Web Repla	y 🌵 <u>B</u> ulletins: (0)	^е <u>G</u> о Т	o lla <u>R</u> eports	Start <u>C</u> en	ter ¹ Profile	¥Sign Out ?He	• IBM.
	~	Find:	🕅 💙 Select A	ction	🕶 🔁 🗔 🧶	🌩 🌼					
List	Discovery										
Discovery Cor	nfiguration	TADDM Discovery			iscover applications	from TAD	DM	Calanaa	Hardware a	nd Coffigure Discours	
	Method	TADDM Discovery						Category	naluwale a	no Soltware Discove	i y
Server Info	ormation	Computer to be Dis	scovered Si	cope							
Name	nc125095	5.romelab.it.ibm.com			Por	t number	9530				
User Id	administra	ator			Pa	assword	•••••	<u>i</u> .			
										Run	Discovery

Figure 8-4 Configuring TADDM Server information

If you have more than one TADDM server in your infrastructure, create a new TADDM Discovery configuration for each server.

Defining scope and running a TADDM Discovery

The scope of a TADDM Discovery can be defined on two separate levels. This allows you to optionally define which computers to discover, as well as what information to discover about those computers.

Defining computer scope

Computer scope can be optionally defined by specifying the systems you want to discover by host name. To do this:

- 1. Click the **Computers to be Discovered** tab of the TADDM Discovery configuration.
- 2. From here, you can add computers one at a time by clicking the **New Row** button and entering each host name you are interested in discovering. Alternatively, you can add multiple host names at once by clicking the **Add from File** option to browse for a file containing a list of host names. This action is shown in Figure 8-5.

Q Disco	very Configurations	🕑 Web Re	eplay 👎 <u>B</u> ulletins: (0) 🏞 <u>G</u> o To	In Reports ♠ Start Cen	ter ¹ <u>P</u> rofile ¹⁴ Sign Out ? <u>H</u> elp 13 16
List	Find:	Select Action	V 🕽 🖬 🖉 🔶 🌣		
Discovery Co	Infiguration TADDM Discovery TADDM Discovery		Discover applications from TADDM	/ Category	Hardware and Software Discovery
Discovery P Server In	arameters formation Computer to be Discovered	d Scope			
Computer	to be Discovered 1 4 of 4 Fully-qualified Server Name linuxtgt.romelab.it.ibm.com	e import from text	1	🖬 i ? i	Download 121 =
•	windowstgt.romelab.it.ibm.com	_			Û
	aoxtgt.romelao.it.iom.com	-			
•	solaristgt.romelab.it.ibm.com	Browse for a file:	C:\targetList.txt	Browse	Add from File New Row

Figure 8-5 Defining computers to discover

If you choose not to define a list of computers to be discovered, all qualifying resources on the TADDM server will be imported into Tivoli Provisioning Manager.

Defining discovery scope

Discovery scope allows you to further filter discovery results by limiting what information is imported about discovered computers. You can filter out hardware, software, business applications, or computer collections by selecting or deselecting the appropriate checkbooks on the **Scope** tab of the TADDM Discovery configuration.

If you choose to discover software, you can further define the scope of the discovery by selecting which software products are of interest. By default, TADDM Discovery configurations will discover hardware as well as installed software components, DB2, Oracle, Web servers, WebSphere Application Server, and WebLogic servers. VMWare ESX is deselected by default.

If you narrow the scope of the discovery by software application, Tivoli Provisioning Manager will discover only computers with the specified applications installed, and will discover only the operating system and the details about the specified application.

Solution Discovery Confi	gurations	🕑 Web	Replay 🦊 <u>B</u> ulleti	ns: (0) 🤌 <u>G</u> o To	IIII <u>R</u> eports n Start <u>C</u> en	ter ¹ <u>P</u> rofile	X Sign Out ? Help	IBM.
¥	Find:	n v Select Action	💌 🖞 🖬	24				sousous and
List Discovery]							
Discovery Configuration Method	TADDM Discovery TADDM Discovery		Discover appli	cations from TADDM	Category	Hardware an	d Software Discovery	
Discovery Parameters Server Information	Computer to be Dis	covered Scope						
Scope Hardwa Softwa	re Discovery? 🗹							
		Installe	ed Software Compo	inents?	Web Server	2	VMWare ESX?	
		WebS	phere Application S	Server?	WebLogic Server	?		
Busines: Comput	s Applications?				082			
							Run Disc	overy

Figure 8-6 Defining discovery scope

For example, if you select only WebLogic Server from the list of software applications, as show in Figure 8-6, Tivoli Provisioning Manager will import all computers from the list of computers to be discovered on which TADDM has found WebLogic installed. Computers in the list that do not have WebLogic installed will not be imported. Likewise, additional software products on the discovered computers will not be imported.

TADDM Discovery scope can be reconfigured and saved at any time. To remember your scope settings for subsequent runs, click the **Save** icon on the application menu bar to save your configuration before running the discovery. Scopes can also be defined at runtime for one time only situations by selecting the desired settings and running the discovery without saving.

8.3 Working with discovered applications in Tivoli Provisioning Manager

After running a TADDM Discovery in Tivoli Provisioning manager, you will be able to view detailed application data and to control discovered computers and their applications from a single location. In this section, we discuss how to access discovered data from the Tivoli Provisioning Manager Web interface, as well as how to configure communication between Tivoli Provisioning Manager and target computers in order to manage these resources remotely. Discovered data can also be used to monitor compliance on both an application and configuration level. We discuss this feature in the next chapter.

8.3.1 Viewing the application configuration data in Tivoli Provisioning Manager

Computers discovered through TADDM Discovery in Tivoli Provisioning Manager are identified by a Globally Unique Identifier (GUID). This ensures that integration between products maintains consistent identification of each device across Tivoli Provisioning Manager, TADDM and ITIC databases. This also makes it easy to search for computers in Tivoli Provisioning Manager on which TADDM Discovery has been run.

From the **Provisioning Computers** application, you can filter the list of computers by using the wildcard * in the Globally Unique Identifier field. The results will display all computers for which this field is populated.

Figure 8-7 shows the computers discovered by running the TADDM Discovery configured in "Defining scope and running a TADDM Discovery" on page 207 to discover WebLogic on a list of computers. Notice that only the two computers with WebLogic installed were discovered, even though there were additional computers listed to be discovered.

Provisioning Computers	🕞 Web Replay 🛛 🖗 U	lletins:(0) 🎓 <u>G</u> o To 🔝 <u>R</u> eports 👘 Start <u>C</u> ente	er ¹ <u>P</u> rofile X Sign Out ? <u>H</u> elp IBM.
Find:	🚮 🔝 Select Action 💌 👀	🖞 🗟 219 9 0	
List Computer Hardware	Software Compliance Recor	mmendations Credentials Workflows	Variables Deployment Properties
🕅 Advanced Search 🔻 🗟 Save Query 🦄	Pookmarks		
Computers 🛛 🛩 Filter > 🚜 🛛 💱 🛛 🎸 🌲 😽	1-2 of 2 🗼		
Computer [®]	Operating System	Globally Unique Identifier	Agent
linuxtgt.romelab.it.ibm.com	Linux - Red Hat Enterprise Linux AS release 4 (Nahant Update 5)	8813DEDBF7E433D392340C4C373724A8	
windowstgt.romelab.it.ibm.com	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	430F0A2B89BB387B9AD54DDD3FDCEBDC	
Select Records			

Figure 8-7 Provisioning Computers imported using TADDM Discovery

Hardware and software for each computer can be viewed by clicking the **Hardware** and **Software** tab for the computer respectively. The Software tab of the Linux computer imported through TADDM Discovery is shown in Figure 8-8.

In the Tivoli Provisioning Manager Data Center Model, software resources are split into software installations and software instances. In some cases, additional configuration details are discovered for each software instance. Parameters for each layer of the software resource are stored in a software resource template.

To view the software resource templates for a particular software installation or nested software instance, click the link found in the list of installations on the Software tab of the computer that you are looking at.

8	Pro	visioning Computers		Web Replay	V <u>B</u> ulletins: (0) <u>~G</u> o⊺o ≞	n <u>R</u> eports	Start C	enter <u>P</u> rofil	e 🌁 <u>S</u> ign Out	s Heb IEI	H.
		🖌 Find: 🕅 🤝	Select Action	V 0	1 🗟 🗶	4 4 6						
List	. 1	Computer Hardware Software	Compliance	Reco	mmendations	Credentials	Work	kflows	Variables	Deploym	ent Properties	
Com Last :	outer Scan	linuxtgt.romelab.it.ibm.com	Operating Sys	stem Red H	iat Enterprise Linu	ix AS release 4 ((Update 🎤	Statistics	3 Products In:	stalled / 0 Patch	nes installed	
04	A.II											
0 5	oftw	are										
OF	atch	es										
Softv	ware	Installations 🥐 Filter 🖓 🗐 💠 🔞 💠 1	-3 of 3 🍁								Download ?	=
		Software Installation	Version	Software D	efinition		_	Installab	ele Status			
				-								
	+	Linux - Red Hat Enterprise Linux AS release 4 (Nahant Update 5)	4.0	Red Hat En (Update 5)	nterprise Linux	AS release 4					ť	1
	•	WebLogic Server - WebLogic Server 9.2 MP3 Mon Mar 10 06:28:41 EDT 2008 1096261 - base domain	9.2	Oracle Web	bLogic Server 9.2						ť	Ì
	×	WebLogic Server - WebLogic Server 10.3 Fri Jul 25 16:30:05 EDT 2008 1137967 - base domain	10.3	Oracle Web	bLogic Server 10g	Release 3					ť	Ì
								Ad	d Software	Unins	stall Software	

Figure 8-8 Software installations imported using TADDM Discovery

To illustrate, we now take a deeper look at one of the discovered WebLogic servers. Notice that in Figure 8-8 there are two WebLogic installations listed, because this computer has both Oracle WebLogic Server 9.2 and Oracle WebLogic Server 10g Release 3 installed. In the following example, we look at the Oracle WebLogic Server 9.2 installation.

The software tree is displayed on the top left corner of the application. This particular software resource consists of three levels: an installation containing two instances, one on port 7001 and the other on port 7110. Each instance has its own set of discovered configuration parameters.

On the software installation level (not shown) you can find the install-related information, such as the installation directory, BEA home, and temporary directory used during the installation.

On the software instance level (not shown) there is another set of parameters, including the root directory, domain name, and listening port. Username and password for the WebLogic instance are also configured within this software resource template. We discuss this in the next section.

Drilling down from the software instance, the last software resource template in the tree contains configuration parameters. Here, you will find timeout values, log levels, security settings, and other configuration details captured by TADDM about the instance configuration. The first page of configuration data for the WebLogic instance on port 7001 is shown in Figure 8-9.

Software Resources		The state of the second	<u>R</u> eturn	<u>TE</u>
Y Find:	t Action			
List Software Resource		and a second		
Software Resources		and the second state of th	one sense and a sense of the se	
WebLogic Server - WebLogic Server 9.2 MP3 Mon Ma	Details Workflows	/ariables		
Configuration Data:7001	Software Resource Details			-
🗈 🔳 linuxtgt.romelab.it.ibm.com:7110	Computer Name	inuxtgt.romelab.it.ibm.com	8	
	Software Module		1	
	Software Installable			
	Status	Unknown		
	Requirements	10 0 000	Drumland 12	
	Requirement Type		Requirement	
	neges onen: type	No rows to display	nequienen	
			New Requirement	
2	Capabilities > Filter > () = (+	1 4] 4 4	Deventored 1 ?	[= .
	Capability Type	Capability	Capability Value	
	Configuration Template:	Web	Logic 9.2 Application Server Configuration Data 1	8012
	Template Parameters > Filter	🖄 🔯 🖢 🎍 🔶 1 - 10 of 49 🦀	Download ?	
	Parameter	Description	Value	
	ConfigFileName	The name of the configuration file.	config.xml	×
	ConfigFileURI	The full URL of the configuration file.	file://9.122.127.180/var/bea/user_projects/dom	×
	CompleteHTTPMessageTimeout	The maximum number of seconds that this HTTP server waits for a complete message to be received.	-1	×
	CompletellOPMessageTimeout	The maximum number of seconds that this server waits for a complete IIOP message to be received.	4	×
	CompleteT3MessageTimeout	The maximum number of seconds that this T3 server waits for a complete message to be received.		×
	DefaultProtocol	The default communication protocol	13	×
	DefaultSecureProtocol	The default secured communication protocol	t3s	×
	DefaultTGIOPUser		guest	×

Figure 8-9 Software Resource Templates populated using TADDM Discovery

8.3.2 Configuring communication to the discovered computers and applications

Due to security considerations, the access information for computers and applications is not imported into Tivoli Provisioning Manager during a TADDM Discovery. Therefore, as a prerequisite step to controlling discovered applications, you must first set up credentials for both the applications and the computers on which they are hosted.

Adding credentials for computers through discovery

For a large number of computers, the easiest and most accurate way to add credentials is to discover them. This can be done by running the *Initial Discovery* from the **Discovery Configurations** application, which uses the discovery method, *Discover Computers using RXA* (Figure 8-10).

Confi	gurations	🕑 Web Replay 🤩 <u>B</u> ulletins: (0) 📌 <u>G</u> o To	Lt Reports n Start Cente	r * <u>P</u> rofile * <u>S</u> ign Qu	t ? Help IRM.
 Image: Second sec	Find: Select Action	🔍 🖸 🗟 🖉 🔍 🔶			
List Discovery					
Discovery Configuration	Initial Discovery	This discovery retrieves network and OS infor	Add Computers to Group	TPM71Endpoints	6
Method	Discover Computers using RXA		Category	Hardware Discovery	
Discovery Parameters	Address Denses	attentials Advanced Dependence			
computers #	Address Ranges Subnetworks	Advanced Parameters			
Credentials i 🛊 🤞 i	+ 1 - 3 of 3 →				Download ? =
User Name	Password		Protocol		
root			SSH mechanism	n selection	Û
root			SSH mechanism s	election	Û
Administrator			SMB mechanism s	selection	â
					New Row
					Run Discovery

Figure 8-10 Defining Credentials for Initial Discovery

Initial Discovery takes a list of computers as input, either by host name on the **Computers** tab, or by IP on the **IP Address Ranges** tab. Both tabs accept individual entries as well as import of values from a file, as seen in "Defining scope and running a TADDM Discovery" on page 207, where we discussed defining the list of computers to be imported during a TADDM Discovery.

On the **Credentials** tab of the Initial Discovery configuration, enter the list of username and passwords for the computers. For each, you can specify the protocol to use (SSH or SMB), or leave the protocol field as default to attempt discovery using both SSH and SMB protocols.

After all computer and credential information has been defined, click the **Run Discovery** button to run the discovery. The initial discovery will create the missing service access points for existing computers that it discovers successfully. Initial Discovery can also be run prior to running TADDM Discovery to create computers with the required service access points in the Tivoli Provisioning Manager Data Center Model before importing TADDM Discovery information.

Adding credentials for computers manually

For a small number of computers, you might want to add computer credentials manually. To do this, perform the following steps:

- 1. From the *Provisioning Computers* application, navigate to the *Credentials* tab of the computer missing credentials.
- Click the Add Credentials button at the bottom of the application, and select the appropriate credential type. For UNIX computers, select SSH and SCP, for Windows computers, select RXA.
- 3. Fill in the search key, user name, and password as shown in Figure 8-12. Click **OK** to create the service access point for the computer. You will need to repeat this process for each computer missing the necessary service access points to communicate with the provisioning server.

🗟 Add Credential Pair			?
Credential Pair Type	SCP		
Source Computer	nc117218.roi	melab.it.ibm.com	P
Targets 🖊 Filter	1214+	+ 1 - 1 of 1 + Download	2 5
Target		Description	
linuxtgt.romelab.it.i	bm.com	Computer	×
		Select Target Devi	се
O Create Basewar	Crodential		
Create Password	ential		
O create RSA crea	ential		
Search Key*	master		Ĩ
User Name*	root		Ĩ
Password ••••••			1
Confirm Password			Ī
Confirm Password	•••••]
		ОК	Cancel

Figure 8-11 Add Credential Pair pop-up

Setting credentials for software instances

Some applications require application credentials in order to perform a task within or against the application. For example, the WebLogic server discussed in previous sections requires a WebLogic username and password (Figure 8-12).

Username	Username of the operator who is connecting WLST to the server	weblogic
Password	Password of the operator who is connecting WLST to the server	·····
	Paramete	r Details
Parameter	Password	Password of the operator who is connecting V
Parameter Value*		
Parameter Type	String ¥	
Multiplicity Type	Zero or on 🛩	
Can be Changed?		
Encrypted?		
Hidden?		
		New Parameter
	a second s	

Figure 8-12 Instance-level software resource template

During a TADDM Discovery, placeholders for application credentials are created in the software resource template on the software instance level. Figure 8-12 shows the Username and Password parameters from the software resource template of one of the Oracle WebLogic Server 9.2 installations explored earlier. The password field is populated with a dummy password. To change this password, expand the parameter by clicking the arrow icon on the left to display the parameter details. Edit the Parameter Value field, and click the Save icon on the application menu bar.

8.3.3 Controlling software applications from Tivoli Provisioning Manager

After you have run a TADDM Discovery in Tivoli Provisioning Manager and configured computers and software to communicate with Tivoli Provisioning Manager, you are able to fully take advantage of the product integration. One of the advantages here is that you now have the ability to see and control computers and installed applications from the same interface. For example, the discovery and configuration of the WebLogic server discussed in the previous sections allows you to not only view configuration details, but also to stop and start WebLogic instances remotely.

To start or stop a software instance:

- 1. Navigate to the instance-level software resource template as described in 8.3.1, "Viewing the application configuration data in Tivoli Provisioning Manager" on page 210.
- 2. You will see two buttons labelled **Start** and **Stop**, as displayed in Figure 8-12 on page 215.
- 3. Click these buttons to start or stop the software instance.

When you do, you will see a pop-up message "The provisioning task has started. Do you want to go to the Provisioning Task Tracking application to monitor the task?".

Clicking **Yes** will direct you the *Provisioning Task Tracking* application, where you can monitor the task to completion.

Additional control of discovered applications can be added through the development of custom workflows and automation packages for any actions that are not supported out of the box.

9

IBM Service Management integration scenarios: Compliance and remediation with TADDM

In this chapter we describe a typical scenario for Compliance Management that, with the other scenarios reported in the following chapters, shows the powerful integration capabilities of IBM Service Management products.

We cover the following topics:

- "Overview of Compliance Management" on page 218
- "Compliance and remediation features" on page 218
- "The compliance and remediation process" on page 223
- "Scenario: Compliance and remediation with TADDM" on page 225

9.1 Overview of Compliance Management

Compliance Management is a critical component of the internal control process for any business and a prerequisite for assessing compliance with corporate performance standards. To meet today's strict regulatory and internal compliance requirements, IT managers need to assess system configurations against predefined, authorized baselines—such as authorized Configuration Items versus installed Configuration Items—and they need the ability to consistently integrate, enforce, and verify compliance policies.

A common reason for system downtime is improper configurations, which are often caused by unauthorized changes. Sometimes required changes such as applying software patches are not implemented, or servers are adjusted on the fly to get them running, but in doing so, security or availability exposures can be generated. IT administrators need to understand the software and configurations that are deployed to their infrastructure as well as changes that result in deviations from standards.

Compliance Management eases and automates the tasks of ensuring that each computer in the IT environment meets the required security standards and matches the software configuration that is appropriate to its role in the enterprise. Software or security related deviations can be automatically remediated to force the systems back to standards. This helps organizations to comply with corporate standards as well as with industry regulations such as Sarbanes-Oxley.

9.2 Compliance and remediation features

Many organizations are overwhelmed by the need to verify that all devices are properly managed and meet a desired configuration. Because the state of the device changes over time, the verification that a device is in compliance is a never-ending process. When the configuration of a device is noncompliant, organizations often manually take steps to remediate the device. The Compliance Management solution offered by Tivoli Provisioning Manager, leveraging the power of automation, enables you to eliminate manual, time-consuming, and error-prone processes so that you can reduce risks, maintain service levels, and deliver world-class IT services. More specifically, Tivoli Provisioning Manager enables the creation of compliance checks—which define an organization's corporate security and software standards—and then compare the software and security set up on the clients and servers in the organization against those standards. If computers are noncompliant, Tivoli Provisioning Manager provides recommendations about how to fix the noncompliance issues (remediation), which can be automatically remediated through the use of automated workflows and applied immediately or at a later time.

Tivoli Provisioning Manager includes both compliance capabilities out of the box as well as the ability to write your own compliance workflows. This gives you the flexibility to support your unique interpretations of the particular regulations that you face, and makes it easier to implement your best practices consistently.

9.2.1 Compliance checks

The desired setup of a computer system or a group of computers is defined using compliance checks. The Compliance Management functionality provided by Tivoli Provisioning Manager v7.1.1 allows you to create the following types of compliance checks:

► Security:

Security compliance checks can be used to check for a variety of security issues. It is possible to select from a list of predefined security checks. For example, you can check for the existence of hard disk and power-on passwords or for the values of firewall settings. You can also define your own security checks to cover situations that are not included in the predefined list.

Note: For more details regarding the list of the predefined security checks and how to create user-defined security compliance checks, refer to the Tivoli Provisioning Manager v7.1.1 documentation available at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp

Software installation:

Software installation compliance checks are used to ensure that computers have the appropriate software products or software stacks, that the required patches are installed, or that inappropriate software is not installed. It is also possible to define groups of software and specify that one software product from the group must be installed. For example, a software group can include all approved antivirus software, and a compliance check can ensure that all target computers have one of the approved antivirus products installed.

Software configuration:

Software configuration compliance checks can ensure that applications installed in the environment maintain the desired configuration settings. The standard software configurations (reference configuration) for the specific application can be discovered by Tivoli Provisioning Manager or by utilizing Tivoli Application Dependency Discovery Manager (TADDM). It is also possible to create your own discovery method to obtain configuration information from a different source.

Note: Configuration information collected by Tivoli Application Dependency Discovery Manager can be replicated in the data center model (DCM) using a discovery method delivered with Tivoli Provisioning Manager (the TADDM Discovery configuration).

It is possible to define compliance checks for individual computers or for groups of computers. For example, all computers running Windows operating systems can be grouped together for Windows security compliance checks. After selecting the compliance checks to be performed on a computer or group of computers, compliance checking can be run immediately or scheduled to run at a later date and time, with the option to repeat checks on a regular basis.

When compliance checks are executed, the system performs a discovery that collects the information required for the specified compliance checks. If any noncompliance issues are detected, recommendations are generated. Recommendations can be reviewed and approved as appropriate and applied afterwards.

9.2.2 Built-in auto-remediation

Tivoli Provisioning Manager v7.1.1 provides built-in remediation workflows that automate the actions required to resolve some non-compliance issues.

Note: Auto-remediation is performed by workflows that implement the logical management operations, ComplianceRecommendation.Remediate or ComplianceRecommendationGroup.Remediate.

The following noncompliance issues can be automatically resolved:

► Software and patch:

Remediation by:

- Installation of software and patches
- Uninstallation of software

Note: Automatic installation and uninstallation can be performed for software and patches that have been installed using Tivoli Provisioning Manager (that is, software products that have a software definition implementing the SoftwareInstallation.Install and SoftwareInstallation.Uninstall logical management operations).

Details about software remediation actions are shown in Table 9-1.

Table 9-1Software remediation actions

Compliance check	Remediation action
Require a software module.	Install the software.
Prohibit a software module.	Uninstall the software.
Require one of software within a software group.	Install any software in the group.
Require all software within a software stack.	Install the software stack -> install all software in the group.
Prohibit a software stack.	Uninstall the software stack -> uninstall all software in the group.
Restrict unknown software installation.	Uninstall the software.

Software configuration:

Reconfiguration actions relating to the following applications:

- IBM DB2
- IBM WebSphere Application Server
- IBM HTTP Server
- Oracle

Note: If an application is not supported out of the box for the software configuration remediation, you can modify the custom remediation configuration xml file under:

%TIO HOME%/config/remediationConfigurationCustom.xml

You can register a new application in this xml file, and then create your own remediation workflow to implement the remediation for the custom application configuration settings. If the configuration parameters in a custom application are based on the name value pair (similar to the IBM HTTP server configuration, httpd.conf), the same name/value pair remediation workflow can be used for remediation. In this case, the user can register this new application in the remediationConfiguration.xml under the %TIO_HOME%/config/ folder.

Security:

Reconfiguration of settings relating to:

- Windows Antivirus
- Windows screen saver
- Windows power-on password
- Windows user password policy

When recommendations related to these types of issues have been approved, they can be run immediately or scheduled to run at a convenient time. When running or scheduling an approved recommendation, a workflow is created to resolve the noncompliance issue. For example, if software that should not be present is detected, an uninstall activity is created.

Note: Automation packages for some of the non-compliance issues that are not covered by Tivoli Provisioning Manager workflows are available on OPAL at:

http://catalog.lotus.com/wps/portal/topal

You can also create your own automation packages to perform user-defined compliance checks and remediation actions. Tivoli Provisioning Manager includes a sample automation package (sample-compliance-validation) for compliance validation that you can use as a starting point for defining your compliance check. For more details, refer to the Tivoli Provisioning Manager v7.1.1 documentation available at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp

9.3 The compliance and remediation process

As already stated, regulations such as Sarbanes-Oxley—and the wide variety of corporate policies designed to address them—demand that IT teams bring clients and servers into alignment with corporate security policies and IT configuration standards. IT staff must be able to quickly identify noncompliant issues and promptly take the steps necessary to bring the devices back into compliance.

Leveraging the integration of Tivoli Provisioning Manager and Tivoli Application Dependency Discovery Manager products, the following diagram depicts a typical Compliance Management process to determine whether the installed software, software configurations, and security settings on the computers in the enterprise match the required set up. Of course, if systems are noncompliant, Tivoli Provisioning Manager will make recommendations to fix them.



Figure 9-1 Compliance and remediation process

The compliance and remediation process includes the following steps:

1. Discover computers:

The Tivoli Provisioning Manager Data Center Model must include information about all the computers for which you want to check compliance. Information can be added to the DCM by running a computer discovery or, if using Tivoli Application Dependency Discovery Manager as the discovery method (as in our scenario), by running a TADDM Discovery configuration from the Provisioning server. This operation will import the gathered information from TADDM to the Tivoli Provisioning Manager database. Usually this is done when any new computer is added to the environment and it is repeated periodically to maintain the collected information up-to-date.

2. Install the Tivoli Common Agent:

The Tivoli Common Agent stack is required to perform security compliance checks and some remediation actions.

3. Discover software configurations:

Using Tivoli Application Dependency Discovery Manager for discovering computers, you can leverage the software configuration information that it collects to perform software configuration compliance checks. To do this, from the Provisioning server, a TADDM Discovery must be run or scheduled to import the up-to-date information collected by Tivoli Application Dependency Discovery Manager into the Data Center Model.

4. Create software configuration templates:

Software configuration templates represent the desired configuration settings for an application. A template is created by copying the application configuration from a computer where the application is correctly and appropriately configured. The computer has to be monitored by Tivoli Application Dependency Discovery Manager and its configuration must have been imported to the Data Center Model using a TADDM Discovery.

5. Create provisioning groups:

Compliance checking can be defined for groups of computers as well as for individual computers. If the same set of compliance checks applies to several computers, it can be useful to define a provisioning group to include the computers with the same compliance requirements.

6. Create compliance checks:

Compliance checks define the compliant state of the computer or group of computers to which they apply. Compliance checks can include:

- Security requirements, supassword rules, and firewall requirements
- Required software and patches
- Prohibited software

- Requirement to install one software product from a group
- Required software configurations

7. Run compliance checks:

Compliance checks can be run immediately or scheduled to run at a convenient time with the option to repeat checks on a regular basis. Compliance checking can also include a scan of the target computers, to ensure that the information against which the checks are made is completely up-to-date. Depending on the types of compliance checks requested, a series of discoveries are performed to collect all the relevant information. If you already have regular discoveries scheduled, you can choose to perform the compliance checking without a scan.

8. Review and approve recommendations:

When the compliance checking process detects a noncompliance situation, it generates a recommendation that specifies the actions required to resolve the issue. Recommendations must be approved before any automated action can be taken to resolve the noncompliance issue.

9. Implement recommended actions:

Tivoli Provisioning Manager provides workflows to automate the actions required to resolve several noncompliance issues, but you can also create your own automation packages to perform user-defined remediation actions.

10. Verify compliance:

When actions have been taken to apply approved recommendations, the compliance checks can be rerun to ensure that all recommended actions have been successful. If a repeating schedule has been created, the success of the actions taken is automatically checked the next time that the compliance checks are scheduled to run.

9.4 Scenario: Compliance and remediation with TADDM

This section describes the setup and execution of a simple scenario highlighting the powerful integration capabilities of IBM Service Management products. In today's IT environments, one key strategy to maximize the business value lies in automating central functions and tasks as much as possible.

Tivoli Provisioning Manager helps a company to automate its own datacenter procedures and processes either by modifying automation packages or creating new packages that match company's best practices. In this case, Tivoli Provisioning Manager allows automation of many steps involved in compliance efforts, helping IT staff to quickly identify when devices become noncompliant and take the steps necessary to bring the devices back into compliance. In particular, this scenario focuses on the integration of Tivoli Provisioning Manager with Tivoli Application Dependency Discovery Manager and how they can be used together to provide a complete process solution for discovering and tracking all the deployed resources for software and configurations, and matching them against established policies.

9.4.1 Scenario introduction

Using a very simple example, our purpose is to guide you through the process of ensuring that computers in your organization meet the required security standards and match the software configuration that is appropriate to their role in the enterprise. Of course, considering that the state of the computers changes over time, verification that each computer is in compliance is a never-ending process.

In this scenario, we consider a single computer (a Windows system called nc117177) that will be assigned to a provisioning group (the *Windows Application Servers* group) for which we create a set of compliance checks in order to ensure that a particular software module is installed, that a certain application is properly configured, and that a screen saver is defined, active, and password protected.

Note: For the lab environment used in this and all other IBM Service Management integration scenarios, refer to 8.1.1, "Lab environment: IBM Service Management integration scenarios" on page 196.

More specifically, our set of compliance checks includes:

- A Software check to ensure that the software module ITM v6.2.1 OS Agent is installed on our target computer.
- ► A Software Configuration check to verify that the application *IBM HTTP* Server v2.0.47.1 installed on the target computer is properly configured.

Note that in this case, we need to create a software configuration template to define the standard settings against which the software configuration check is made. This template is created by copying the configuration of that application from a computer that has been configured with the approved settings (the nc117118 system in the scenario).

 A Security check to make sure that on our target computer, a screen saver is defined, active, and password protected.
9.4.2 Setting up users and permissions

To run a such scenario, you typically need to have a set of users configured to properly manage all the involved resources in the system. Alternatively, you can use a "super administrator" user (such as maxadmin) to execute all the steps.

Tivoli Provisioning Manager provides predefined security groups that can be used as is or can be modified to suit your enterprise environment. The groups are aligned with the user roles defined for the product and compatible with IBM Service Management principles.

The following users are utilized in this scenario.

Provisioning Administrator

The Provisioning Administrator user is responsible for executing all the tasks related to the discovery of computers and their software configurations, including some preparation steps such as the installation of the Tivoli Common Agent.

Tivoli Provisioning Manager provides a security group for the role of the Provisioning Administrator (TPADMIN), so all you need to do is to create a user and assign it to that group.

Compliance Analyst

The Compliance Analyst user controls all the policies for compliance and ensures they are followed to meet goals. More specifically, this user defines the groups for handling compliance, defines the compliance checks, and verifies the compliance of the managed resources.

Tivoli Provisioning Manager provides a security group for the role of Compliance Analyst (TPCOMPLIANCEANALYST), so all you need to do is to create a user and then assign it to that group.

Provisioning Configuration Librarian

The Provisioning Configuration Librarian user is used to run scans and compliance checks on the managed resources.

Tivoli Provisioning Manager provides a security group for the role of Provisioning Configuration Librarian (TPCONFIGURATIONLIBRARIAN), so all you need to do is to create a user and assign it to that group.

Deployment Specialist

The Deployment Specialist is responsible for executing all the tasks needed to implement the recommended actions to meet compliance.

Tivoli Provisioning Manager provides a security group for the role of Deployment Specialist (TPDEPLOYMENTSPECIALIST), so all you need to do is to create a user and assign it to that group.

Automation Package Developer

The Automation Package Developer has access to all the software packaging tools (including the Software Package Editor that we use in the scenario to create software packages) and is responsible for creating automation and packages for deployment.

Tivoli Provisioning Manager provides a security group for the role of Automation Package Developer (TPDEVELOPER).

Note: This security group is only configured for the Start Center. No application authorization is added for the group because it is not designed to be used on its own. Appropriate application authorization can be added by assigning the users in this group to the TPADMIN security group.

So in this case you need to create a user and assign it to both the TPDEVELOPER and TPADMIN groups.

Tip: To create the above mentioned users and assign them to the proper predefined security group, you can use Tivoli Directory Server from the WebSphere Administrative Console 6.1.

Log on to the WebSphere Administrative Console with the "wasadmin" user by specifying:

https://fully_qualified_hostname:9043/ibm/console

Figure 9-2 highlights the predefined security groups provided by Tivoli Provisioning Manager.

Integrated Solutions Console Welcome wasadmin Help | Logou IBM View: All tasks My Startup Pages Guided Activities Search for Groups Servers Applications Search by *Search for *Maximum results Group name 💓 * 100 Resources Search Security Environment 42 groups matched the search criteria. System administration Create... Delete Select an action... Users and Groups 0074 ~ Administrative User Roles
 Administrative Group Roles Select Group name Description
 Select
 Group name
 Description
 Unique Name

 PMUSRAMAL
 cn=PMUSRAMAL.ou=groups.ou=SWQ.o=18M,c=US

 PMUSRAMAL
 cn=PMUSRAMGR.ou=groups.ou=SWQ.o=18M,c=US

 SMSELDSERVICE
 cn=SRMSELESERVICE.ou=groups.ou=SWQ.o=18M,c=US

 TPAOMIN
 cn=TPAOMIN.ou=groups.ou=SWQ.o=18M,c=US

 TPCOMPLIANCEANALYST
 cn=TPACMIN.ou=groups.ou=SWQ.o=18M,c=US

 TPCOMPLIANCEANALYST
 cn=TPCONFIGURATIONLIBRARIAN.ou=groups.ou=SWQ.o=18M,c=US

 TPCOMPLOWERTIONLIBRARIAN
 cn=TPCONFIGURATIONLIBRARIAN.ou=groups.ou=SWQ.o=18M,c=US

 TPDEVELOPER
 cn=TPDEVELOPER.ou=groups.ou=SWQ.o=18M,c=US

 WR_VARIANTERCIALIST
 cn=TPDEVELOPER.ou=groups.ou=SWQ.o=18M,c=US

 WR_VARIANTERCIALIST
 cn=TPDEVELOPER.ou=groups.ou=SWQ.o=18M,c=US

 WR_VARIANTERCIALIST
 cn=TPDEVELOPER.ou=groups.ou=SWQ.o=18M,c=US

 WR_R_VARIANTERCIALIST
 cn=WR_AGNIN_PERMISSION

 WR_VARIANTERCIALIST
 cn=WR_SYSADMIN_PERMISSION.ou=groups.ou=SWQ.o=18M,c=US

 WR_VARIANTERCIALIST
 cn=WR_VSASADMIN_PERMISSION.ou=groups.ou=SWQ.o=18M,c=US

 WR_VARIANTERCIALIST
 cn=WR_VSASADMIN_PERMISSION.ou=groups.ou=SWQ.o=18M,c=US
 Unique Name Manage Users
 Manage Groups Monitoring and Tuning ■ Troubleshooting Service integration E UDDI E Settings WR USER cn=WR_USER,ou=groups,ou=SWG,o=IBM,c=US cn=WR_USER_PERMISSION,ou=groups.ou=SWG.o=IBM.c=US 3 **Go** Page 3 of 3 Total: 42

To view the groups previously discussed, from **Users and Groups**, select **Manage Groups** and then click **Search**.

Figure 9-2 List of the Tivoli Provisioning Manager predefined security groups

Next we give you a brief summary of the steps required to add a new user and assign it to the appropriate predefined security group:

- 1. Go to Users and Groups and select Manage Users.
- 2. Click **Create** and enter the appropriate information in all the fields.
- 3. Click Group Membership. See Figure 9-3.

Manage Users	Manage Users
WIM User Management	WIM User Management
Create a User	Group Membership
+ User ID agathac Group Membership	Specify the search criteria that you want to use to find the groups that you want this user to b Search by *Search for *Maximum results Group name * 100
*First name *Last name agatha christie	Search Current groups 42 matching groups. Troncougi supremany ver
E-mail	Add MAXIMOUSERS Add MACFGAUM MACFGAUM MACFGAUM MACFGAUM
* Password * Confirm password	PMCHAIGEADMIN PMCHAIGEADMIN PMCHAIGEADALYST PMCHAIGEAPARYOVER
Create Cancel	Close

Figure 9-3 Adding a new user and assigning it to a security group

- Click Search, from the list in the right box select the group you want to add the user to, and click Add in order to move it to the Current groups box, then click Close to return to the Create a User page.
- 5. Finally, click **Create** and then **Close** to submit.

Note: For more information about the predefined security groups and detailed instructions on controlling user access, refer to the Tivoli Provisioning Manager v7.1.1 documentation available at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp

9.4.3 Scenario implementation

The scenario is implemented by using the following major steps.

Step 1: Run a discovery with TADDM

The first step to be performed consists in running a discovery in TADDM to discover our target computer. The discovery can be run manually (in case there are no scheduled discoveries), and the person in charge of this task is the *Provisioning Administrator*.

Note: For details about discoveries, refer to the Tivoli Application Dependency Discovery Manager v7.1.2 documentation available at:

```
http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/index.jsp?to
pic=/com.ibm.ccmdb.doc_7.1.1/ccmdb_welcome.htm
```

Next we provide a summary of how to run a manual discovery:

- 1. Log in to the TADDM console.
- 2. As prerequisite tasks in order to run a discovery, it is necessary to:
 - a. Define a Windows Gateway on the TADDM server in case you have to discover Windows computers (as in our scenario).
 - b. Define a Scope (the list of machines to be discovered).
 - c. Add the required credentials (userid and password to access the system during the discovery) to the Access List.
 - d. Customize a Profile with the sensor configurations as needed.
- 3. Navigate to **Discovery** \rightarrow **Overview** and click the **Run Discovery** button.
- 4. Select the scope (or the single machine inside the scope) and the proper profile and then click the **OK** button to start the discovery. See Figure 9-4.

Tip: We chose a customized L3 Profile (which is the deepest sensor discovery) that is able to bring in all the details about the *IBM HTTP Server* application and its configuration settings.

Tivoli Application Dependency	Discovery Manager - Version: Curren	t	
	9		
Discovery	Overview		
Overview E	Discovery Information Status: kie Components Found: 0 Sensors Running: 0 Progress:		
Scope	Show only items of status: All status lev	Scope: Selected Scope Elements	
Access List	Sensor	Copes Copes	Description
Custom Servers		9.168.117.175 (ort17175.romelab.likm.com) 9.168.17.1776 (ort17175.romelab.likm.com) 9.168.17.177 (ort17177.romelab.likm.com) 9.168.172.271 (ort17177.romelab.likm.com) 9.468.172.247 (ort171271.romelab.likm.com)	
Topology		9 160 117 210 (no 172 10 domenati 2 domenati 2 domenati 9 168 117 219 (no 125095 romelati 2 domenati	
Analytics	<		<u>></u>
Discovered Components X Application Infrastructure	Information: To view information about the sens		
Comparison Infrastructure Overview	Run Discovery Scope Details Discovery Log		
B-Cal Custom Servers G-Cal Infrastructure Services	Items: Cick Show Details to view data.	Select Al Clear Al	• 2 6
ie- Com Windows File Services(1)		CK Cancel	

Figure 9-4 Running discovery with TADDM

5. While the discovery is running, you can follow the deployment and execution status of the sensors in the **Overview** dialog box as shown in Figure 9-5.

Tivoli Application Dependency Discovery Manager - Version: Current									
File Edit Display Discovery Topology Analytics W	Indows Help	13	V						
Discovery	Overview								
Overview E	Discovery Information Status: Running Components Found: 10 Sensors Running: 1 Propress:			_					
	Trogressi								
Scope	Show only items of status: All status lev								
81	Sensor	Host Name/IP	Date	Status	Description				
	PingSensor(9.168.117.177)	nc117177.romelab.it.ibm.com	7/21/09 19:56:30 CEST	done	Stored - 1 IP addresses in the database				
Access List	PortSensor(9.168.117.177)	nc117177.romelab.it.ibm.com	7/21/09 19:56:40 CEST	done	Stored - [445, 135] in the database				
		nc117177.romelab.it.ibm.com	7/21/09 19:56:31 CEST	done	Stored - nc117177.romelab.it.ibm.com in the database				
Custom Sequere	⊕ SessionSensor(9.168.117.177)	nc117177.romelab.it.ibm.com	7/21/09 19:57:10 CEST	done	Stored - Administrator@9.168.117.177/null (wmi) via Administrator@				
Custom Servers	GenericComputerSystemSensor(9.168.117.177)	nc117177.romelab.it.ibm.com	7/21/09 19:57:11 CEST	done	Stored - Microsoft(R) Windows(R) Server 2003 Enterprise x64 Editi				
	⊕ GenericServerSensor(9.168.117.177)	nc117177.romelab.it.ibm.com	7/21/09 19:57:50 CEST	done	Stored - 11 Server Processes (9 with Windows Services) in the dat				
Topology	WindowsComputerSystemSensor(9.168.117.177)	nc117177.romelab.it.ibm.com	7/21/09 19:58:49 CEST	done	Stored - nc117177.romelab.it.ibm.com/NC117177 in the database				
Analytics	ApacheServerSensor(9.168.117.177:8008)	nc117177.romelab.it.ibm.com	7/21/09 19:57:55 CEST	done	Stored - 1 server bound to 0.0.0.0:8008 in the database				
	⊞ CustomAppServerSensor(9:168:117:177:1631)	nc117177.romelab.it.ibm.com	7/21/09 19:57:42 CEST	done	Stored - JavaServer, 9.168.117.177:1631 in the database				
i uiscovered Components	⊕ ApacheServerSensor(9.168.117.177:80)	nc117177.romelab.it.ibm.com	7/21/09 19:57:43 CEST	in progress	Storing 1 server bound to 0.0.0.0.80 in the database.				
Application Infrastructure									
Application Infrastructure Overview	<	111			>				
Infrastructure Software	Information:								

Figure 9-5 Discovery sensors' log

At the end, you can view the information gathered by TADDM by opening the **Details** dialog box for the discovered system (nc117177 in our scenario) and navigating through the various tabs, as shown in Figure 9-6.



Figure 9-6 Discovery details

Step 2: Import data from TADDM to Tivoli Provisioning Manager

The next step is to populate the Tivoli Provisioning Manager database with the information gathered by TADDM. The data import is performed by running, from the Tivoli Provisioning Manager server, a particular discovery (called TADDM Discovery) that replicates hardware and software data from the TADDM database to the Data Center Model. The person in charge of this task is still the *Provisioning Administrator*.

Here we give a basic summary of the steps in creating, configuring, and running a TADDM Discovery:

1. Log in to the Tivoli process automation engine console as a user with the TPADMIN role:

https://fully_qualified_hostname:9443/maximo

- 2. Select Go To \rightarrow Discovery \rightarrow Provisioning Discovery \rightarrow Discovery Configurations.
- 3. Click the New record icon.
- 4. Enter the name and description for the discovery configuration being created.
- 5. In the *Category* field, select **Hardware Discovery** and in the *Method* field, search for *TADDM Discovery* and then click **OK**. See Figure 9-7.

C Discovery Configurations	Web Replay Butetris: (0) A Go To La Repo	nts 🕈 Start Center 🔺 <u>P</u> rofile 🎽 <u>Sign</u> Out ? <u>H</u> elp <u>TERF</u> .
💉 Find: 🚺 💎 Selec	Action 💌 🗓 🗟 🖉 I 🔅 🔅	
List Discovery	🛡 Add Discovery Configuration 📃 🗄 ? 1 🗵	
Advanced Search 🔻 🍙 Save Query 👻 🖉 Bookmarks		
Discovery Configurations 🕴 🔻 Filter > 🚜 🕴 🛊 + 🍦 🕴 🗢 1 -		E> Download ? =
Discovery Configuration +	Discovery Details	
	Name * My TADDM Discovery	
AIX Acquire Patches	Description taddm discovery	tes 🗞 🗙
	Discovery Configuration	
	Category	
AIX Discover Patches	Aardware Discovery	× ↔
	O Other	
AlX WPAR Discovery		Discovery 🏟 🗙
Cisco Switch Discovery		
	Method TADDM Discovery	
	Description Discovers resources from Tivoli Application Dependency Discovery Manager.	
HP-UX Software Depot: Patch Check Tool	Resources that can be discovered include computers, computer hardware and network resources, operating systems, software components, composite annications such as webSohere standalone.	× ×
	server, ND server, DB2, Oracle, Web Servers (IBM Http Server, Apache Server, MS IIS), Weblogic	
	Server etc. The discovery can be run against a set of selected components. It can also be run against one or more computers based on fully gualified computer names.	
IBM Blade Discovery		* ×
	OK Cancel	

Figure 9-7 Creating a TADDM Discovery configuration

- 6. In the Server Information tab, specify the TADDM server details (Figure 9-8):
 - a. Fully qualified host name or IP address of the TADDM server (nc125095.romelab.it.ibm.com, in this case)
 - b. Port number (9530)
 - c. TADDM server administration user ID (administrator) and password (collation)

Discovery Configurations		C Wel	o Replay 🛛 👂 <u>B</u> ulletins:	(0) 🍖 <u>G</u> o To	<u>I™ R</u> eports	* Start Center	A Profile	X <u>S</u> ign Out ? <u>H</u> e	° IBM.
Find: Select Action	V 🕽 🗟 214 🖗								
Discovery Configuration My TADDM Discovery Method TADDM Discovery	Discovers both hardware and software resou			Category	Hardware	and Software Dis	scovery		
Discovery Parameters Server Information Computer to be Discovered Scope									
Server Information		Dest sumber	9530						
User Id administrator		Password							

Figure 9-8 TADDM Discovery configuration parameter settings

7. In the **Computer to be Discovered** tab, specify the fully qualified host name of the computer that you want to discover (nc117177.romelab.it.ibm.com, in this case).

Note: Only the computers that you specify in this list are replicated from the TADDM server. If you want to discover all the resources, do not specify any hosts in the discovery list. If you leave the list empty, all resources on the server will be replicated.

8. In the **Scope** tab, leave the defaults and click the **Save** icon (Figure 9-9).

C Discovery Configurations		Web Replay 🥊 <u>B</u> ulletins: (0) 🎓 <u>G</u> o To 🕮	Reports * Start Center * Profile * Sign Out ? Help IEM.
Find: Select Action	🗹 📜 🔜 🗶 I 🎄 🔶		
List Discovery			
Discovery Configuration My TADDM Discovery Method TADDM Discovery	Discovers both hardware and software resou	Category	Hardware and Software Discovery
Discovery Parameters			en
Server Information Computer to be Discovered Scope			
Scope			8
Hardware Discovery?			
Software Discovery? 🖌			
	Installed Software Components?	Web Server?	VMWare ESX?
	WebSphere Application Server?	WebLogic Server?	
	Oracle?	DB2?	
Business Applications?			
Computer Collections?			
			Run Discovery

Figure 9-9 TADDM Discovery configuration parameter settings

- 9. The TADDM Discovery configuration is now configured, and you can run it by clicking the Run Discovery button and then the Submit button on the Run Discovery subsequent panel. Monitor the task until it completes. After a successful discovery, the specified computer has been added to the Tivoli Provisioning Manager Data Center Model.
- 10. You can see it displayed in the "Provisioning Computers" list by clicking **Go** To \rightarrow Deployment \rightarrow Provisioning Computers, as shown in Figure 9-10.

Provisioning Computers			🕒 Web Replay Bulletins: (0)		ter 🔺 <u>P</u> rofile 🗡 Sign Out ? <u>F</u>	icip II.	EM.
Find:	💎 Select Action 💌 🚯 🎒 🖃 🧟 1	🎄 🔅 🇀					
List Computer Hardware Soft	ware Compliance Recommendations	Credentials Workflows Variables	Deployment Properties				
🕅 Advanced Search 👻 🎴 Save Query 👻 🔗 B	ookmarks						
Computers 🛩 Filter > 🚯 🗊 🔶 🎍 🔶 1 - 5 of 6	5 ↔				R) <u>Da</u>	wnload	? ==
Computer *	Operating System	Globally Unique Identifier	Agent	Complian	ce Status		
sc117175 romelab it ibm com	Microsoft(R) Windows(R) Server 2003,	F172FF27C9BD3F4564645450459F644CF88	TCA-1420	No como	iance checks configured	×	۵.
	Enterprise Edition		T WY T T T ALL V				
nc117177.romelab.it.ibm.com	Windows Server 2003 R2 Enterprise x64 Edition SP2	2A978E3C949134DE8DB22A7D515D441D		No com	pliance checks configured	×	
nc117217.romelab.it.ibm.com	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	C33948CC0D4537FABE459EF7206BF789	TCA-1.4.2.0	No comp	liance check has been run	×	ۿ

Figure 9-10 Computer list

11. You can also view the related information by clicking the computer entry and navigating through the various tabs. See Figure 9-11.

Provisioning Computers	O Web Replay 🦓 Balanna (I) 🖗 Go To 🔛 Baparis 🕫 Start Canter 🏦 Brollie 🤻 Sign Out. 🤉 Heb	ibm.
🗹 Find: 🛛 🕅 💙 Select Action 🔍 👀 🚺		
List Computer Hardware Software Compliance Recommen	dations Credentials Workflows Variables Deployment Properties	^
Computer # hp117177 romsish it ibm com		-
Globally Unique Identifier 2A978E3C949134DE8DB22A7D515D44		
Configuration Item		
Configuration	Last Known Status	
	Operations	
Management IP Address 9.168.117.177	Framework Deployment engine	
Operating System Windows Server 2003 R	Agent	
Computer Template	Agent Status	
Dotale		
Model Type Vitual Platform	Compliance	Ш
Architecture Intel	Security Configuration required	
Serial Number V/II ware-56 4d da e4 9f	Software Configuration required	
Manufacturer VMware, Inc.	Patches Configuration required	
Static Provisioning Groups > Filter > W 20 + + ++	Download ?	-
Static Provisioning Group	Description Type	
	No rows to display	-
	Assign to Static Group	
Dynamic Group Association		
Discovery	Discovery Type Scan Date	
and they		
My TADDM Discovery	Network Scan 2009-07-21 23:24:43	~

Figure 9-11 Computer details

Step 3: Install the Tivoli Common Agent

Now that the data regarding the target computer has been imported into the Tivoli Provisioning Manager Data Center Model, the installation of the Tivoli Common Agent stack is required to perform security compliance checks and remediation actions. The person in charge of this task is again the *Provisioning Administrator*.

Note: The Tivoli Common Agent is required for security Compliance Management. For other types of compliance, the common agent is only required if you are using the scalable distribution infrastructure (SDI), otherwise adding the Remote Execution and Access (RXA) credentials is enough.

To install the Tivoli Common Agent on the discovered computer:

- 1. Select Go To \rightarrow Deployment \rightarrow Provisioning Computers.
- 2. Filter on the computer (nc117177) and click it.
- 3. From the Select Action menu, select the Install → Common Agent option, as shown in Figure 9-12.

Provisioning Computers		O web Replay 10 guadents (0) 0 go To ≥ Boports + Start Genter + Boote > Son Out ? Heby IIIH.
List Computer Hardware Software Computer Hardware Software Comput Globaly Unique Identifi Configuration te	Instal Software Product Inst Uninstal Patch Software Stack Capture Import Scan Delete Computers	Workfows Variables Deployment Properties
Configuration	Add Credentials > Hardware > Hardware > 177 Storage > Add Resource > Run Reports >	Clustificrown Status Operations Framework Disployment engine Agent Agent Status
Details	Model Type Villware Virtusi Platform Architecture Intel Serial Number Villware-56 4d da e4 917 Manufacturer Villware, Inc.	Compliance Security Configuration required # Software Configuration required # Patches Configuration required #

Figure 9-12 Installing Tivoli Common Agent

4. In the Install Common Agent panel, leave the check on the **Create Credentials** check box and specify the credentials for creating an RXA service access point required for the Tivoli Common Agent installation and then click **Submit**. See Figure 9-13.

Provisioning Computers	C Web I	Replay B Buletins: (0) 🖍 Go To Le Beports 🕈 Start Center 🛓 Profile 🎽 Sign Out ? Help 🌐 👬 🥵
🗸 Find: 🕅 🔻 Select Action 🛛 🖌 🚷 🥥 🔇	2	
List Computer Hardware Software Compliance Recommendations	🛡 Install Common Agent 🛛 🖓 🕴 🛛	
Computer* no117177.romelab 8.bm.com Globaly Unque Kenntifer Configuration tem	Provisioning Task* Install Common Agent 1025	-
Configuration Management P Address Desting System Windows Sarver 2003 R2 Computer Templat Locate Details Model Type Architecture Weare Vriuse Particul Seriel Number Villware-54 ed da set 117 Wandresture Villware, Inc.	Common Agent Stacks [7] [2] [2] [4] [4] [4] [2] [2] [2] [2] [2] [2] [2] [2] [2] [2	Agent Agent ant Statue Security Configuration required Software Configuration required Attaches Configuration required
Static Provisioning Groups	User Name Administrator	Cit powelood ? = Type
Dynamic Group Association	Contin Passwirt Schedulen to change options. Scheduler. Nov Schedule	Assign to Static Group
Recent Discovery Scans + Filter: gb 2 + + + + + 3 of 3 + Decovery	Notification □ Recipients ▶ Filter > ○ [2] ♦ ♦ ♦ 1 + 1 of 1 ♦ Download ?	Scan Date
My TADDM Discovery	MAXADMIN X	2009-07-17 02:06:56
My TADDM Discovery	Add Recipient Add E-mail	2009-07-17 02:08:56
My TADDM Discovery	Sevents # Filter 14, [2] # # ### Provide [1] # [2] Description	2009-07-17 02.20 56

Figure 9-13 Installing Tivoli Common Agent

Note: Because on computers imported from TADDM, credentials are not automatically created, it is necessary to add a Service Access Point (SAP) for root or administrator user ID before running any recommendation (such as installing software or executing provisioning workflows) against them.

5. When you submit the task, the **Provisioning Task Tracking** page is displayed. You can click the task name to see details about the task status and monitor the progress until the task has completed. See Figure 9-14.

Provisioning Task Tr	racking							↑ <u>R</u> eturn IENI.
Find:	曲。	Select Action	💌 🚯 🛃 🧶 🔶 🔶					
List Task								
Provisioning Task	Install Common Agent 10	25				Definition	Install Common Agent 1025	
Type	Common Acent Installatio	10	1			Start Date	2009-07-17 03:05:20	
1990	Max a Direct					End Date		
Created By	MAXADMIN					Status	In Progress	
Changed By						Base Services Task	A	
Provisioning Workflows	▶ Filter > AL (白) ◆ → (⇒ 1 - 1 of 1 ⇒						B) Download 171 =
Provisioning Workflow	v	Status			Start Date	End Date	Concurrency Level Subtask	
 Install_Agent 		In Progress	1		2009-07-17 03:05:21		6 Install Common Agent 63	94
					Details			
Targets Workflow R	Parameters							
Car Filter volto Charles Carl	÷1.10[1.5	_						Browning 1210
Ternel			Statue	Hereage				Provisioning Workflow Lon
nc117177.romelab.it.i	ibm.com		In Progress	in a stand s				10.433
				Landing				
								Detail

Figure 9-14 Installing Tivoli Common Agent

6. Click the **Refresh** icon to see an update on its status, as shown in Figure 9-15.

0	Provisioning Workflow Status			↑ <u>B</u> eturn INM.
List	Find:	🕅 🔻 Select Action 💌 🍬 🔅	9	
	Workflow I S	Name Install_Agent Status Success	;	Deployment Request 10,433
Paran	notors 🔻 Filter > 🐴 🗊 🛊 🤞 🧇	= 1 - 4 of 4 ->		🖏 Download ? =
Param	eters		Input Values Output Values	
Passy	vord		U9IBXdh4zu2FVQA0WewzXw	
Device	1D		6289	
Softw	arrel Ioriula D		S154	
		1		
Execu	ntion Logs ; ♥ Filter>@At ; □ ; + +	i ↓ 1 - 25 of 693 🎐		Download 171 =
	Start Uate	Seconds.Millseconds		
•	2009-07-17 03:05:22	22.879	Start workflow: 'Install_Agent'	debug
+	2009-07-17 03:05:23	23.020	Start workflow: 'Get_DCM_Property'	debug
×.	2009-07-17 03:05:23	23.082	End workflow: 'Get_DCM_Property'	debug
•	2009-07-17 03:05:23	23.192	Start workflow: 'TCA_Check_Platform_Resources'	debug
•	2009-07-17 03:05:23	23.379	Start workflow: 'RXA_Create_RXA_SAP'	debug
•	2009-07-17 03:05:23	23.848	End workflow: 'RXA_Create_RXA_SAP'	debug
•	2009-07-17 03:05:23	23.957	Start logical operation: 'Discovery.OnDevice'	debug
•	2009-07-17 03:05:24	24.035	Start workflow: 'RXA_Discovery_OnDevice'	debug
×.	2009-07-17 03:05:24	24.067	Start workflow: 'Get_Server_Mgmt_P_Address'	debug
•	2009-07-17 03:05:24	24.114	End workflow: 'Get_Server_Mgmt_P_Address'	debug
•	2009-07-17 03:05:24	24.223	Start Java plugin 'com.thinkdynamics.kanaha.de.javaplugin.sap.FindCredentialsPassword'	debug
•	2009-07-17 03:05:24	24.254	End Java plugin 'com thinkdynamics kanaha de javaplugin sap. FindCredentialsPassword'	debug
•	2009-07-17 03:05:27	27.551	Windows,Microsoft Windows 2003,EM64T	debug
•	2009-07-17 03:05:29	29.801	End workflow: 'RXA_Discovery_OnDevice'	debug

Figure 9-15 Tivoli Common Agent installation log

 The Tivoli Common Agent is now installed and running on the computer. In fact, the status (running) is now displayed in the Agent Status field on the Configuration section of the Computer tab, as shown in Figure 9-16.

W Prid W Seed Actor Image: Seed Actor <td< th=""><th>Provisioning Computers</th><th>O Web Replay 3 guidents (0) /* go To Mit Beports /* Start Senter * Potter * Son Out /* Beb INTER</th></td<>	Provisioning Computers	O Web Replay 3 guidents (0) /* go To Mit Beports /* Start Senter * Potter * Son Out /* Beb INTER
Lat Computer Hardware Software Computer Recommendations Creditatia Workfown Vanables Dopkyment Properties Computer International Computer International Creditatian Workfown Vanables Dopkyment Properties Computer International Com	💌 Find: 🛛 👫 🤝 Select Action 🔍 😍 🌅 😡 🖉	
Computer * ACTITITY Transition & Den com Obbally Unique Stentierre 24-77/EEX-D419130/EEX/EEX/E419130/EEX/E6/930/EEX/EFX/E6/930/EEX/E6/930/EEX/E6/930/EEX/E6/930/EEX/EFX/E6/930/EEX/E6/930/EX/E6/9300/EX/E6/9300/EX/E6/9300/EX/E6/9300/EX/E6/9300/EX/E6/9300/EX/E6/9300/EX/E6/9300/EX/E6/93000/EX/E6/930	List Computer Hardware Software Compliance Recommendations	Credentals Workflows Variables Deployment Properties
Configuration Ital at Revenue Status Images (Revenue Status) Naragement P Address (Rel 117:07) Operations Comprision Operations Operations Appendix Status Comprision Computer Template Appendix Status Computer Template Appendix Status Details Montage of the Status Complete Template Appendix Status Complete Template Details Montage of the Status Complete Template Complete Template Complete Template Details Montage of the Status Complete Template Complete Template Complete Template Details Montage of the Status Complete Template Complete Template Complete Template Status Montage of the Status Complete Template Complete Template Complete Template	Computer* Inc117177 romelab & Ibm.com Globally Unique Identifier Configuration item	a a
Maragement P Address B168.117.177 Operations Framework Scalable Datibution Initial Operating System Windows Server 2000.88 Agent CA.14.2.0 Complex Templex	Configuration	Last Known Status
Ottab Model Type Model Type Model Type Model Type Compliance Pic Anotherizer EMAT Compliance Compliance # Source So	Manapement P Address 9.168.117.177 Operating System Windows Server 2003 R/ Computer Template Locae	Operations Framework Solabele Distribution Infra Agent TCA-14.2.0 Agent Status R
Hanvidsterer Wirvers Inc. Patches Configuration required #	Details Hodel Type Vitware Vitual Pattern Acchtecture Estell Stelluter Vituare 50 dd a e 9 fr: Naturfacture Vituare 50 dd a e 9 fr: Naturfacture Vituare 50 dd a e 9 fr:	Longlance Security Configuration required # Schware Configuration required # Petches Configuration required #

Figure 9-16 Computer's details

Step 4: Assign the computer to the compliance group

Compliance checking can be defined for groups of computers as well as for individual computers. Defining compliance groups and assigning targets to the appropriate group are all activities concerning the appliance of compliance policies, so the person in charge of these tasks is the *Compliance Analyst*.

We already defined a provisioning group called *Windows Application Servers* that includes particular computers with the same compliance requirements. Now we assign our target computer nc117177 to that group as follows:

- 1. Log in to the Tivoli Provisioning Manager console as a user with the TPCOMPLIANCEANALYST role.
- 2. Select Go To \rightarrow Deployment \rightarrow Provisioning Computers.
- 3. Filter on the computer (nc117177) and click it.
- 4. On the **Computer** tab click the **Assign to Static Group** button. See Figure 9-17.

Provisioning Computers	C Web Res	lay 🔒 guletins: (0) 📍 Go To 🔝 Beports 🕈 Start Genter 🔺 Profile 👌 Sign Out ? Help 📰 👯 .
🔍 Find: 🎁 🔻 Select Action 🔍 🚯 🎽 🛃 🧶 I 💠 🔅	2	and the second sec
List Computer Hardware Software Compliance Recommendations Creden	tials Workflows Variables Deployment Properties	
Computer * 2517157 etconolibit 8 cm. com Globally Unique Identifier 2A97853049154058082247051504410 Configuration 8cm //		
Configuration	🖙 Last Known Status	
Management P Address (9.188.117.177 Operating System) Windows Server 2003 R2 Computer Temptate // Locate //	Operations Fr Age	anework Scalabe Diatritution Nifre Agent TCA-14.2.0 et Status Running
Details Moder Type Where Virtual Partform Architecture Intelline Intelline Serial Number Virtuar-56 4d as et 977 Manufacture Virtuar-56.	Compliance	Secury Configuration required Activene Configuration required Active Configuration required A
Static Provisioning Groups > Filter > (0 0 + + +>		🕞 gownlosg ? 📼
Static Provisioning Group	Description	Type

Figure 9-17 Assigning the computer to a group

5. From the displayed list, select the desired group and click **OK**. See Figure 9-18.

Provisioning Computers					And a second second		🕑 Web Replay !	Bulletins: (0)	Le Reports A Start Center	Profile	<u>S</u> ign Out ? <u>H</u> elp	IBM.
Y Find:	🔥 🤝 Select Action	💌 🚯 🎽 🖬 🧶	🔷 🔶 🥻	•								
List Computer Hardware	Software Compliance	Recommendations	Credentials	Workflows	Variables	Deployment Properties						
Globe	Computer* nc117177.rom ally Unique Identifier 2A978E3C949 Configuration Item	slab.it.ibm.com 134DE8DB22A7D515D441D										
Configuration						E Last Known Stat	tus					-
Details	Management IP Address Operating System Computer Template Locale	9.168.117.177 Windows Server 2003 R2		무 Assign to Static G	sroup	Operations	Framewor Agen Agent Status	k Scalable Distribution Inf tt TCA-1.4.2.0 s Running	185			
	Model Type Architecture Serial Number Manufacturer	VMware Virtual Platform Intel VMware-56 4d da e4 917 VMware, Inc.		Groups V Filter	> da ⊇ ≱ ¥ +1-	3 of 3 → ^{Eb} <u>Download</u> ? !	Securit Software Patcher	y Configuration required configuration required configuration required	1			
Static Provisioning Groups > Filter	>#\[]]			TPC Servers	puters		-				Ger <u>Downio</u>	👳 ? 📼
Static Provisioning Group				Windows Ap	Add New Gro	P OK Cancel			т	ype	Assign to Static Gr	roup

Figure 9-18 Assigning the computer to a group

Our target computer is now assigned to the desired group.

Step 5: Create a Software Package for installing the ITM agent

Software compliance checks can be defined to require or restrict the installation of software modules. In this scenario, we define a software compliance check for a group of Windows computers, all of which must have the ITM v6.2.1 OS Agent installed. To install this product, we need to create a software package containing all the actions that have to be executed on the target system.

The possible actions can be grouped in different categories as follows:

- The Add Object and Remove Object actions drive the engine to add the specified object to the system or to remove it from the system. Some objects include adding or removing directories, files, registry keys, services, and so on.
- The System actions include checking disk space, restarting the target workstation, adding a signature file to the configuration repository, and so on.
- The Program actions include executing a user-defined program, InstallShield program, Microsoft Setup program, RPM (RPM Package Manager) package, and so on.

Next we summarize the basic steps for defining a Software Package utilizing the Software Package Editor (a Java-based graphical interface for creating and customizing software packages). The person in charge of this task is the *Automation Package Developer*:

- 1. Log in to the Tivoli Provisioning Manager console as a user with the TPDEVELOPER role.
- 2. Select Go To \rightarrow IT Infrastructure \rightarrow Software Catalog \rightarrow Software Products, as shown in Figure 9-19.

Welcome, maxadmin		C Web Replay P Bulletins: (0)	₽ <u>G</u> o	To Let Reports the Start Center Administration	≜ <u>P</u> ro	nfile [™] <u>Sign</u> Out ? <u>H</u> elp <u><u></u>,</u>
Automation Package Developer Compliance Analyst Deployment Spec	cialist Process Management Requester	Provisioning Administrator Provisioning Configuration Librarian	ø	Assets	•	^
Automation doublement and antications	Contras of mu passant available in a contra	🕼 Change Content/Layout 🚇 Display Settings 🖓 C	3	Change Deployment	; T	emplate 🛛 Update Start Center
Automation development applications	Deployment Request ID	Workflow Name	ß	Discovery) U.	/
Provisioning Workflows				Financial	, E	
O Demokratice Washington Clark a	11,317	Discover	9	IT Infrastructure	×	Configuration Items —
Provisioning Workflow Status Provisioning Computers	11,316	Compliance_Validation	0	Integration		Actual Configuration Items
	11,315	Discovery.OnDevice	3	Inventory		Process Requests
Provisioning Computers	11,312	Compliance_Validation	宦	Planning	+	Configuration Processes
	11,310	Discovery.OnDevice		Purchasing		Relationships
Virtualization Management	11,308	Compliance_Validation	ø	Release		CI Lifecycles
<u></u>	11,307	Discovery	-	Security		Collections
Provisioning Task Tracking	11,306	SoftwareInstallation.Uninstall	-	Self Convine		Provisioning Inventory
	11,305	Compliance_Validation		Software Products	N	Software Catalog +
Provisioning Task Definitions	11,303	Compliance_Validation	0	Software Stacks	~	b
	Set Graph Options		4	Set Software Product Im Software Signatures	oort	1 - 10 of 80 <u>Next Page</u> »
Provisioning administration applications	Status of my recent provisioning tasks	🔻 Filter 🛛 🚜 🗄 🕽 🖗	6	Software Validation		/=1
	Provisioning Task	Status	-	Patches		
Other configuration and development applications				Patch Acquisition		

Figure 9-19 Opening Software Products

3. From the Select Action menu, select Start SPE. See Figure 9-20.

Software Products			오 Web Re	eplay 🛛 🥊 <u>B</u> ulletins: (0) 🎤 <u>G</u> o To	[∐] <u>R</u> eports ₱ Start <u>C</u> enter ▲ Profile	× <u>S</u> ign Out ? <u>H</u> elp	IBM.
Find: 🕅 🔻 Sela	ect Action	🕽 🗟 🗶 I 🍳 🍦					
List Software Definition Targets Ta	Install Distribute	Variables					
🛍 Advanced Search 🔻 🗟 Save Query 🔻 🖋 Bookm	Publish						
Software Products 🕴 🔻 Filter > 📸 🛛 🗐 🕴 🗍 🔶 1 - 20	Unpublish					Downlos	<u>ad</u> ? =
Software Definition 🕈	Delete	Version		Vendor			
NETFramework - 1.1.4322.1	Start SPE	1.1.4322.1		Microsoft Corporation		₩	X
<u>AIX 4.3.3</u>	43	4.3.3		IBM		♠	X
AIX 5L Version 5.1		5.1		BM		*	X
AIX 5L Version 5.2		5.2		BM			X

Figure 9-20 Starting Software Package Editor

The Software Package Editor is started, and through this interface you can create the Software Package to be used for installing the ITM agent, as shown in Figure 9-21.



Figure 9-21 Software Package Editor

The Software Package contains a directory (with all its subdirectories), including all the files needed for the installation of the product and an executable program that launches the script to perform the silent installation.

Note: For more details about using the Software Package Editor, refer to the Tivoli Provisioning Manager v7.1.1 documentation available at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp

Step 6: Create compliance checks

Compliance checks define the desired configuration settings on the targets to which they are applied. Let us now describe how to create a set of compliance checks that includes a Software, a Software Configuration, and a Security check, and explain how to apply them to a group of computers. The person in charge of this task is again the *Compliance Analyst*.

Adding a software compliance check

Software compliance checks can be defined to require or restrict software modules or software stacks or to require the installation of one software product from a selected software group. In this case we add a software installation check to ensure that our target has the ITM v6.2.1 OS Agent installed.

Here we summarize the basic steps for adding such a software check:

- 1. Log in to the Tivoli Provisioning Manager console as a user with the TPCOMPLIANCEANALYST role.
- 2. Select Go To \rightarrow Deployment \rightarrow Provisioning Groups.
- 3. Select the group previously created that our target computer nc117177 belongs to, and click the **Compliance** tab. See Figure 9-22.

Provisioning Groups		A DESCRIPTION OF THE OWNER	Web Replay	🖁 gulletins: (0) 🕐 Go To 🛛 🗠 <u>R</u> eports	Start <u>C</u> enter	X Sign Out ? Help TEM.
Find:	Select Action 💌 🚯 🎦 📓 🧶 I	4 4				
List Group Compliance Recomme	ndations Variables					
Compliance Scan						=
Group Windows Application Servers					E	nable Automatic Approval
Status Unknown		Compliance recommendation	ns are not approved automatically			
					Run : 🔻	Schedule : V
				No scheduling o	ptions were specified. Click S	chedule to change these options
All Configured Checks Security Checks	Software Checks Allowed Software	Software Configuration Checks	Notification Setup			
Compliance Checks 🕨 Filter 🔐 😭 🛊 🔶 🧇	•					🕞 <u>Download</u> ? 🚍
Compliance Check		Туре	Last Scan		Compliant	
		No rows to display	Copy Checks	New Checks from Model Compu	ter New C	ompliance Check : 💌 📊

Figure 9-22 Adding a software compliance check

4. Click the New Compliance Check button and select Software Check \rightarrow Software Module Check, as shown in Figure 9-23.

E Provisioning Groups	🕑 Web Replay	₽ <u>B</u> ulletins: (0)	. <u>R</u> eports	▲ <u>P</u> rofile [×] Sign Out ? <u>H</u> elp IE .
🔍 Find: 🕅 🏘 🔻 Select Action 🔍 🚯 🤰 💭 🥥 🕴 🍁				
List Group Compliance Recommendations Variables				
Compliance Scan				
Group Window's Application Servers Status Unknown			Compliance rea	commendations are not approved automatically
		No sc	heduling options were spec	Run : Citick Schedule to change these options
All Configured Checks Security Checks Software Checks Allowed Software Software Configuration Checks	Notification Setup			
Compliance Checks V Filter M [2] + + +				Download ? =
Compliance Check Type	Last Scan		Compliant	
	Copy Checks	New Checks from Hor	lel Computer Software Module Check Software Stack Check Software Patch Check Software Group Check	Patch Check Security Check Software Check > Software Configuration Check

Figure 9-23 Adding a software compliance check

5. On the **Add Software Check** panel search for the ITMv621_agent software module, select it and click **Save**. See Figure 9-24.

Provisioning Groups	Add Software Check		• Go To Mar Reports ♣ Start Center ▲ Profile ★ Sign Out ? Help TTRE.
Find: Select Action			
List Group Compliance Recommendations Variables	Search itm	Search	
Compliance Scan			-
Group Windows Application Servers	Software Checks > Filter > (> 12 + > (+1-1of 1+	Download ? =	Enable Automatic Approval
Status	Software Check Type		Compliance recommendations are not approved automatically
			Run : V Schedule : V
			No scheduling options were specified. Click Schedule to change these options
All Configured Checks Security Checks Software Checks			
Compliance Checks			2 -
Compliance Check			Comoliant
			ks from Model Computer New Compliance Check : 🔻
		Save Cancel	

Figure 9-24 Adding a software compliance check

 A Software check for the selected software module is now added to the Compliance Checks table as shown in Figure 9-25. After clicking the Save button, the software module compliance check is added with the default settings. See Figure 9-25.

B Provisioning Groups		eb Replay 🛛 🖡 <u>B</u> ulletins: (0	i) 🌈 <u>G</u> o To 🔟 <u>R</u> eports	* Start <u>C</u> enter	Profile × Sign Out	? <u>H</u> elp	N.
🗸 Find: 🕅 🕅 🗸 Select Action 🔍 😯 🊺	∄ ∉∣♦ ♦						
List Group Compliance Recommendations Variables							
Compliance Scan Group Windows Application Servers Status Unknown All Configured Checks Security Checks Software Checks Allowed Software	vare Software Configuration Checks Notificat	n Setup	No scheduling o	Compliance recomm Ru ptions were specified	Enable Autome endations are not ap n : • • • • • • • • • • • • • • • • • •	atic Approval oproved automatica Schedule : change these optic	ally
Compliance Checks ▶ Filter > ☆ ② ♦ ♦ ♦ 1 - 1 of 1 ♦					Eł.	Download ? 6	8
Complence Check	Type Softwa Delete Checks Cop	a Module Checks New	Last Sca Checks from Model Compu	n ter	Compliant New New Compliance Ch	X eck : V	

Figure 9-25 Adding a software compliance check

7. You can view and change the default settings by clicking **Detail Menu** (arrow icon) near the entry and selecting **Settings**, as shown in Figure 9-26.

子 Provisioning Groups		C Web Replay 9 Bulletins: ((0) 🎤 <u>G</u> o To 🔟 <u>R</u> eports 🌴 Start <u>C</u> e	nter 🔺 <u>P</u> rofile 🛛 <u>S</u> ign Ou	t ?Hep IEM.
Find: 📕 Velect Action	🛛 🗸 🚯 🚺 🗟 🖉 🛉				
List Group Compliance Recommendations	Variables				
Compliance Scan					8
Group Windows Application Servers				Enable Autor	natic Approval
Status Unknown			Complianc	e recommendations are not a	approved automatically
Status Unknown Compliance recommendations are not approved automatically Run I Schedule to channe these notions No scheduling ontions were seerfied (Thir's Schedule to channe these notions					
			No scheduling options were	specified. Click Schedule to	o change these options
All Configured Checks Security Checks Software Che	cks Allowed Software Software Config	uration Checks Notification Setup			
Compliance Checks 🚺 🕅 🕼 🖓 🛊 🛊 🛊 🕯 🕯 1 - 1 of 1 🗞				G	Download
Compliance Check		Туре	Last Scan	Compliant	
TMv621_agent Set	ings N	Software Module		New	X
Rec	commendations ^W	Delete Checks Copy Checks Nev	v Checks from Model Computer	New Compliance C	heck : 🔻

Figure 9-26 Viewing settings

 The default settings include a Required State option with the value, Software must be installed. This is exactly the state required for the ITM v6.2.1 OS Agent software module, so we keep the defaults. See Figure 9-27.

Provisioning Groups	🕑 Web Replay	<mark>₿ <u>B</u>ulletins: (0)</mark>	₱ <u>G</u> o To <u>IIII R</u> eports	* Start <u>C</u> enter	≜ <u>P</u> rofile × <u>S</u> igr	n Out ? <u>H</u> elp	IBM.
▼ Find: ▶ Select Action ▼ ● □	214 \$						
Compliance Scan Group Windows Application Servers Status Unknown	🖣 Edit Software Product Compliance Checks 🔤 🗄			Compliance reci	Enable A	utomatic Appro	utomatically
All Configured Checks Security Checks Software Checks Allowed Software Compliance Checks #Filter + St + + 1 - 1 of 1 + Compliance Check Thive32_agent	Software TMV621_sgent Version 1.0 Verdor TCM Priority* Software must be installed Description Alert Run Now? Start At Save Cancel	× New C	No scheduling o Last Sca	n ter	Run I Kongeneration Statement	Schedule le to change th	ese options

Figure 9-27 Viewing settings

Adding a security compliance check

The Compliance Management feature includes a set of predefined security compliance checks. In this scenario, we specify a simple security check (that applies to Windows computers only) to ensure that our target has a screen saver active and password protected:

1. Again, click the **New Compliance Check** button and select **Security Check** (Figure 9-28).

Provisioning Groups				D Web Replay	Bulletins: (0) 🏕 Go To 🔟 Reports 🏠	Start <u>C</u> enter 🔺 <u>P</u> rofile 🗡 S	ign Out ? <u>H</u> elp 👔	EM.
Y Find:	🔥 🔻 Select Action	€ 🖞 🗟 🗶 I ᡇ 🔶	an) Varaanaanaan					
List Group Compliance R	ecommendations Variables							
Compliance Scan								6
Group Windows Application Servers						Enabl	e Automatic Approval	
Status Unknown					Co	impliance recommendations a	re not approved automat	tically
						Run : 🔻	Schedule : 🔻	
					No scheduling option	s were specified. Click Sche	dule to change these or	otions
All Can Farrier Charles Connection Charles	Collinear Charles	Hannad Cathuran Cathuran	Can Empetian Chanles	Natification Cation				
All configured checks Security check	is Soltware checks F	alowed Software Software	configuration checks	Notification Setup				
Compliance Checks 🚺 🖗 Filter > 🚳 🗐 🖗	♦ +1-1of1+						Download ?	=
Compliance Check				Туре	Last Scan	Compliant		
TMv621_agent	1			Software Module		New	×	
			Delete Checks	Copy Checks	New Checks from Model Computer	Patch Cher	ck J	
						Security C	heck N	
						Software	Check 4	
						Software	Configuration Check	

Figure 9-28 Adding a security compliance check

2. On the **Add Security Check** panel, select the **Windows Screen Saver** security check and click **Save**, as shown in Figure 9-29.

B Provisioning Groups	🕑 Web Replay 🔒 Bulletins:	(0) P Go To Le Reports A Start Center A Profile X Sign Out ?Help 直面元。
	R Add Security Checks	
🌱 Find: 🕅 🔻 Select Action 👻 🚯	-	
List Compliance Desembandetings Variables		
List Group Compliance Recommendations Valiables		
Compliance Scan	Security Checks i 🖡 Əlter 🖓 i 🗁 i 🗍 🤞 i 🖕 1 - 19 of 19 🔶 📴 Download i ? i 🚍	-
Group Windows Application Servers	Security Check 🗄	Enable Automatic Approval
Status Unknown	AX Activity Auditing	Compliance recommendations are not approved automatically
	AlX Remote Root Login	
	Linux System Logging	Run : V Schedule : V
	Operating System Patches and Updates	No scheduling options were specified. Click Schedule to change these options
	Restrict Other Software	
All Configured Checks Security Checks Software Checks Allowe	Taroet Agent	
Compliance Checks	UNIX File Permissions	Downland 21
	UNIX Services	Last Saca
Diffused agent	User Defined Check	Last Scan Compliant
	Windows Antivirus	Oberlanderen Verdel Communication
	Windows Event Logging	Checks from Model Computer
	Windows File Permissions	
	Windows Firewall	
	Windows Hard Disk Password	
	Windows Power-On Password	
	Windows Screen Saver	
	Windows Services	
	Windows Unauthorized Guest Access	
	Windows User Password	
	Save	

Figure 9-29 Adding a security compliance check

 After clicking the Save button, the selected security check is added with the default settings and it is displayed in the Compliance Check table (Figure 9-30).

Provisioning Groups				🗘 Web Replay	🖁 <u>B</u> uletins: (0) 🖗	<u>G</u> o To <u>In R</u> eports	Start Center	A <u>P</u> rofile	Sign Out ? j	leip IIIM.
Y Find:	Select Action 🛛 🖌 🚺 🔓] @ 🔷 🖗								
List Group Compliance Recommend	lations Variables									
Compliance Scan Group Windows Application Servers								Ena	ible Automatic A	.pproval
Status Unknown							Compliance reco	ommendations	s are not approv	ed automatically
								Run : 🔻	Sche	dule : 🔻
						No scheduling op	tions were speci	fied. Click Sch	hedule to chan	ge these options
All Configured Checks Security Checks	Software Checks Allowed Softwa	re Software Conf	figuration Checks	lotification Setup						
Compliance Checks > Filter > 🚳 🍃 + 🍦 + 1	- 2 of 2 🧇								By Dow	nload ? 🖴
Compliance Check				Туре		Last Scan		Compliant		
ITMv621_agent	1			Software Module				New		X
Windows Screen Saver	4			Security				New		X
	₩ Detail Menu		Delete Checks	Copy Checks	New Chec	ks from Model Compute	er 🗌 🗌	New Com	pliance Check	V

Figure 9-30 Adding a security compliance check

- 4. It is possible to view and change the default settings, as follows:
 - a. Click **Detail Menu** (arrow icon) near the just-created entry and select **Settings**, as shown in Figure 9-31.

Provisioning Groups		🕑 Web Repla	ly ^{II} <u>B</u> ulleti	ns: (0) 🏾 🖗 <u>G</u> o To 🔛 <u>R</u> eports 👘 Start <u>C</u>	center 🎍 <u>P</u> rofile 🗡 <u>S</u> ig	n Out ? Help IBM.
Find: Select Action	3 🗂 🗟 🖉 🖗					
List Group Compliance Recommendations Variables						
Compliance Scan Group Windows Application Servers Status Unknown				Compian	Enable A	Automatic Approval
Al Configured Checks Software Checks All	Settings	1 i	? : 🖂	No scheduing options wer	Run : 💌	Schedule : •
Compliance Checks Piber / A B P 4 (*20/24)	Setting	Enabled	Value	Last Scan	Compliant	UQWNIOBO Y B I
mVv621 agent	Active	V	Yes	Lust ordin	New	X
Windows Screen Saver	Password protected Maximum timeout value (minutes)	V V	Yes 30	New Checks from Model Computer	New New Complian	X nce Check : V
		Save C	ancel			

Figure 9-31 Viewing settings

- b. The following settings are automatically enabled:
 - Active: Yes
 - Password protected: Yes
 - Maximum timeout value: 30

We change just the *Maximum timeout value* parameter from 30 to 10 and keep the first two settings, which means that we want the screen saver activated after a maximum of 10 minutes idle-time, with password protection.

c. Click Save.

Adding a software configuration compliance check

Software Configuration compliance checks are performed by comparing the configuration of an application on the target computer with a standard configuration for that application. In this scenario, we verify that our target computer nc117177 has the application *IBM HTTP Server version 2.0.47.1* installed with a standard configuration. We define the reference configuration by creating a *Software Configuration Template* using the configuration captured on another computer (the nc117218 system), where we assume that the application is correctly configured.

Important: As already reported, to use software configuration checking, it is necessary to store the standard software configuration information into the Tivoli Provisioning Manager Data Center Model. In this case the computer with the standard configuration nc117218 has been previously discovered with TADDM (by using an L3 profile (able to capture the details of the *IBM HTTP Server* application and its configuration) and the discovered data have been imported into the Tivoli Provisioning Manager Data Center Model by running a TADDM Discovery.

Here we summarize the steps for creating the **Software Configuration Template** for the *IBM HTTP Server* application:

1. Select Go To → Deployment → Software Management → Software Configuration Templates. See Figure 9-32.



Figure 9-32 Creating a software configuration template

Software Configuration Templates		O Web Replay
Find: Select Action	V 🕽 🖬 🖉 🕸 🔶	
List Template		
Template Vaster BM-Http-Server configuration tem Date Created 2009-07-20 23:50:53	Master IBM-Http-Server configuration	
Computer	■ Software	E Discovery
Source Computer nc117218 romelabilition.c #	Software Version 2.047.1 Software Version 2.047.1 Software Version BM	Discovery Configuration My TADDM Discovery
Software Configuration Rules Template 🕨 Filter > 🏤 🗊 🔶 🧍 🐡	1 - 10 of 66 🥪	By <u>Download</u> ? =
Parameter	Value	Path E
ihs.credentials	administrator	/IBM-Http-Server/Windows.discovery/lihs. credentials
ihsW selectLocale.lang	?	/BII-Http-Server/Windows.discovery/hs. -W selectLocale.lang
ihsP ihs.install.ocation	C:/Program Files/IBM/HTTPServer	/IBII-http:Server/Windows.discovery/lhs. -P hs.install.ocation
ihsP ihsService.active	true	/IBM-http-Server/Windows.discovery/ihs. -P hsService.active
ihsP admin.Service.active	true	//BII-http-Server/Windows.discovery/lhs. -P admin.Service.active
ihsW I/TService.user	?	/BM-http-Server/Windows.discovery/hs. -W NTService.user
ihsW NTService.password	?	/IBM-http-Server/Windows.discovery/ihs. -W NTService.password
		/IRM.Http.Server/Windows discovery/ibs

2. Click the New record icon. See Figure 9-33.

Figure 9-33 Creating a software configuration template

- 3. In the **Template** field, enter a name for the software configuration template.
- 4. In the **Source Computer** field, click **Detail Menu** (arrow icon) near the field and from the list of computers displayed, select the computer where the *IBM HTTP Server* is configured with the settings that you want to use as reference (nc117218 in this case).
- 5. In the *Software Name* field, click **Detail Menu** (arrow icon) near the field and from the list displayed, select the application **IBM HTTP Server**.

The *Discovery Configuration* field is automatically filled in with the name of the TADDM Discovery configuration used to discover the application.

All the details regarding the configuration settings for the application on the source computer are displayed in the *Software Configuration Rules Template* section.

6. Click the Save (shown as diskette picture) icon.

After the template has been created, it is possible to add a Software Configuration check to the provisioning group for which we already created the Security and Software checks. The tasks to create the software configuration compliance check based on that template just created are shown here:

- 1. Select Go To \rightarrow Provisioning \rightarrow Provisioning Groups.
- 2. Select the same group and click the **Compliance** tab, as shown in Figure 9-34.

Provisioning G	roups		🕟 Web Replay	₽ <u>B</u> ulletins: (0) 🖗 <u>G</u> o To 🗽 <u>R</u> eports	* Start <u>C</u> enter * Profile * Sign Out ? Help III .
•	Find: Select Action	🛩 🚯 🎽 🗟 🧶 🏟 🔹			
List Group	Compliance Recommendations Variable	is			
Compliance Scan Group Windo Status Unknor	vs Application Servers	Alowed Software Software C	onfiguration Checks Notification Setup	No scheduling of	Enable Automatic Approval Compliance recommendations are not approved automatically Run Schedule Schedule to change these options
Compliance Check	s ≱ Filter > () [1] ≱ ↓ ↔ 1 - 2 of 2 →				By Download ? =
Complian	e Check		Туре	Last Scan	Compliant
□ ITM_621	agent 🧪		Software Module		New X
Windows	Screen Saver		Security		New X
			Delete Checks Copy Checks	New Checks from Model Comput	er New Compliance Check :

Figure 9-34 Adding a software configuration compliance check

3. Click the New Compliance Check button and select Software Configuration Check. See Figure 9-35.

₿ Pr	rovisioning Groups				🕑 Web Replay 🛛 🖡	Buletins: (0) 🏾 🖗 Go To 🛛 🕮 <u>R</u> eports	* Start <u>C</u> enter ⁴ <u>P</u> rofile X	Sign Out ? Help
	Find:	Select Action	3 🕽 📓 🖉 🔶					
List	Group Compliance Reco	mmendations Variables						
Complia	ance Scan							8
G	roup Windows Application Servers						Enal	ble Automatic Approval
St	tatus Unknown						Compliance recommendations	are not approved automatically
All Co	onfigured Checks Security Checks	Software Checks Al	lowed Software Software C	Configuration Checks	Notification Setup	No scheduling oj	Run : V	Schedule : V
Comp	liance Checks 🕨 Filter 🕅 👌 🛊 🔶							Download ?
	Compliance Check				Туре	Last Scan	Compliant	
	ITTM_621_agent	1			Software Module		New	×
	Windows Screen Saver	1			Security		New	×
				Delete Checks	Copy Checks	New Checks from Model Comput	er Patch Ch Security Software Software	eck Check • Check • Configuration Check

Figure 9-35 Adding a software configuration compliance check

4. In the Add Software Configuration Check panel, select the desired software configuration template and click **Save**. See Figure 9-36.

Provisioning Groups	O Web Replay 🤚 Bulletins: (0) 🕈 Go To 🔤 Beports	* Start Center * Profile * Sign Out ? Help 1977
🖌 Find: 🕅 🕅 🔻 Selec	IAction 💌 🚯 🖏 🧟 I 🏟 🎐	
List Group Compliance Recommendation	Variables	
Compliance Scan		8
Group Windows Application Servers		Enable Automatic Approval
Status Unknown		Compliance recommendations are not approved automatically
		Run : V Schedule : V
	No scheduling	ptions were specified. Click Schedule to change these options
All Configured Checks Security Checks Softw	투 Add Software Configuration Checks 🛛 🗄 🕴 ? 🗆 🛛	
Compliance Checks 1 Stress M 121 4 1 1 2 of		By numbers 1 2 1
Compliance Check		Compliant
ITTM_621_agent	Software Configuration Checks 🚺 Filter M 🖾 🛊 🔶 🖛 1 - 1 of 1 🔶 📴 Download 1 ? 📼	New X
Windows Screen Saver	Template Description Golden computer Module	New X
	Master IBM-Http-Server configuration Master IBM-Http-Server configuration nc117218.romelab.it.ibm.com IBM-Http-Server template	ter New Compliance Check
	Stre Carcel	

Figure 9-36 Adding a software configuration compliance check

A Software Configuration check related to that configuration template is now added to the **Compliance Checks** table, as shown in Figure 9-37.

H Provisioning Groups				C Web Replay	♥ <u>B</u> ulletins: (0) 🔗 .	<u>G</u> o To Un <u>R</u> eports	* Start <u>C</u> enter	* <u>P</u> rofile	× Sign Out ?	Help IBM.
🚩 Find:	Select Action 📉 🔽 🚯 🚺 🖟	3 2 4 4								
List Group Compliance Recommend	lations Variables									
Compliance Scan										
Group Windows Application Servers								En	able Automatic	Approval
Status Unknown							Compliance rec	ommendation	ns are not appro	oved automatically
								Run : 🔻	Sch	edule : 🔻
						No scheduling or	tions were spec	ified. Click Sc	chedule to cha	nge these options
All Configured Checks Security Checks S	Software Checks Allowed Softw	are Software	Configuration Checks	Notification Setup						
Compliance Checks > Filmr > 📣 🗊 🛊 🐠 🗢 1 -	- 3 of 3 🗇								Dov	wnload 🕴 ? 🕴 📼
Compliance Check			1	уре		Last Sc	an	Complia	ant	
ITM_621_agent	1		:	ioftware Module				New		×
Windows Screen Saver	1		5	ecurity				New		×
Master BM-Http	Settings N		5	oftware Configuration				New		×
	Recommendations		Delete Checks	Copy Checks	New Check	s from Model Comput	er 🛛	New Cor	mpliance Check	(i 🔻

Figure 9-37 Viewing settings

5. Click **Detail Menu** (arrow icon) near the entry and select **Settings** to see the details about the software configuration check. The **Software Configuration Check Details** panel is displayed and all the parameter settings from that template are listed as reported in Figure 9-38.

Provisioning Groups		🕑 Web Replay 🕴	Bulletins: (0) 🎓 Go To 🕅 Reports 🦸	Start Center & Profile X Sign Out ? Help
	🗟 Software Configuration Check Details			
✓ Find: db				
List Group Compliance Recon				
	Tomplete Dotaile Million - M. I.M. A. J. - 4. 44	11 1 m	Re	
Compliance Scan	Medula Version Source compute	ar Discovery	Download of the	Eashie Automatic Assessed
Status Unknown	IBM-Http-Server 2.0.47.1 nc117218.rom	elab.it.ibm.com My TADDM Discovery-762	4 cloned from 5832	Enable Automatic Approval
	Parameters is Filter 144 in the 4 is 31 : 40 of 5	8 🛧		
	Parameter	Description Path	Value	Run : V Schedule : V
All Configured Checks Security Checks	IhsP doc.active	/IBM-Http-Server/Windows.discovery/serv er/ihsP doc.active	true X	re specified. Click Schedule to change these options
Compliance Checks 🌶 Filiar - 🖧 🚍 🐥 🗼) ihsP security.active	/IBM-Http-Server/Windows.discovery/serv er/ihsP security.active	true 🗙	C* Download ? =
Compliance Check		ADM UMa CastarAM/adatus disastart/sast		Compliant
Windows Screep Saver	ServerRoot	er/config-parameters/ServerRoot	"C:/Program Files/IBM/HTTPServer"	New A
Master IBM-Http	🕨 PidFile 🥒	//BM-Http-Server/Windows.discovery/serv	logs/httpd.pid	New X
	▶ Timeout	/IBM-Http-Server/Windows.discovery/serv er/config-parameters/Timeout	300 ×	New Compliance Check : V
	KeepAlive	/IBM-Http-Server/Windows.discovery/serv er/config-parameters/KeepAlive	On ×	
	MaxKeepAliveRequests	/IBM-Http-Server/Windows.discovery/serv er/config-parameters/MaxKeepAliveRequest s	100	
	KeepAiveTimeout	/IBM-Http-Server/Windows.discovery/serv er/config-parameters/KeepAliveTimeout	10	
	▶ ExtendedStatus	//BM-Http-Server/Windows.discovery/serv er/config-parameters/ExtendedStatus	On X	V

Figure 9-38 Viewing settings

6. If necessary, it is possible to make any changes before saving.

Tip: In this case we deleted the parameter *ServerName* (containing the hostname of the source machine).

Our set of compliance checks is now created and ready to be run.

Step 7: Run compliance checks

Compliance checking can also include a scan of the target computers to ensure that the information against which the checks are made is completely up-to-date. In our case, target computer information was just brought into DCM running the TADDM Discovery, so we could skip the scan and run a compliance check only (this is done for software and software configuration compliance checks). Nevertheless, because our set also includes a security check, we need to perform a scan on the target computer to collect the relevant information required for that check and compare the results to the required state. The person in charge of this task is the *Provisioning Configuration Librarian*.

The tasks to run the compliance checks previously defined are as follows:

- 1. Log in to the Tivoli Provisioning Manager console as a user with the TPCONFIGURATIONLIBRARIAN role.
- 2. Select Go To \rightarrow Provisioning \rightarrow Provisioning Groups.
- 3. Select the group for which the set of compliance checks has been created and click the **Compliance** tab, as shown in Figure 9-39.

Provisioning Groups			🕞 Web Rep	lay 🤨 <u>B</u> ulletins: (0) 🎓 <u>G</u> o To 🔤 Beports 🌴	Start <u>C</u> enter ¹ <u>P</u> rofile [×] Sig	n Out ? <u>H</u> elp IEM.
Find:	🎝 🔝 Select Action 🕑 🄇	🔶 🐥 🛃 뎞 🛃 🧕				
List Group Compliance Rec	ommendations Variables					
Compliance Scan						-
Group Windows Application Servers Status Unknown All Configured Checks Security Checks	Software Checks Allo	ved Software Software	Configuration Checks Notification Setup	C No scheduling optio	Enable A ompliance recommendations are Run : The second se	Automatic Approval not approved automatically Schedule : lie to change these options
Compliance Checks > Filter > 🕅 🗦 🛊 🧍	∳ + 1 - 3 of 3 +					Download ?
Compliance Check			Туре	Last Scan	Compliant	
MWv621_agent	1		Software Module		New	×
Windows Screen Saver	1		Security		New	×
Master IBM-Http	1		Software Configuratio	New Checks from Model Computer	New Complian	ce Check : 🔻

Figure 9-39 Running compliance checks

4. Click $\mathbf{Run} \rightarrow \mathbf{Scan}$ and \mathbf{Check} . See Figure 9-40.

ال Pro	wisioning Groups			🕑 Web Replay	₽ <u>B</u> uletins: (0) ♠ <u>G</u> o To Lat <u>R</u> eports ♣	Start <u>C</u> enter 🏼 <u>P</u> rofile 🎽 <u>S</u> ign	Out ? Help IIM.		
	Y Find:	Select Action 🛛 🖌 🚯 🎒 🔒	<u>@</u> \$\$						
List	Group Compliance Recomme	ndations Variables							
Complian	nce Scan								
Gro	Windows Application Servers					Enable A	utomatic Approval		
Stat	Status Unknown Compliance recommendations are not approved automatically								
	E. and Charles Consult Charles	Colour Charles Time Manual Colours	Coliman Coliman	- Oberland University Outer	No scheduling option	check s were sp Scan and Che	chedule : V		
All Cor	rigured checks Security checks	Software checks Allowed Software	Sontware Configuratio	n checks Notification Setup					
Complia	ance Checks 🚺 Filter 🕅 💷 🛉 🐓 🗇	1 - 3 of 3 🔶					^B ∕ <u>Download</u> ? =		
	Compliance Check			Туре	Last Scan	Compliant			
V	ITMv621_agent	< 1 · · · · · · · · · · · · · · · · · ·		Software Module		New	×		
V	Windows Screen Saver	1		Security		New	×		
V	Master IBM-Http	1	De	Software Configuration ete Checks Copy Checks	New Checks from Model Computer	New New Compliance	e Check : 🔻		

Figure 9-40 Running compliance scan and check

5. Then click **Yes** to display the **Provisioning Task Tracking** page and monitor the task, as shown in Figure 9-41.

Provisioning Groups			🕑 Web Replay 🛛 👂	<u>B</u> ulletins: (0) 🏾 A Go To 🛛 🖾 <u>R</u> eports	nter denter denter denter denter denter denter denter de la constante de la co	<u>P</u> rofile XSign Out	?Help IIM.			
Find:	V Select Action	🔁 🕽 🗟 🖉 🖗 🖗			ananananananana					
List Group Compliance Recom	mendations Variables									
Compliance Scan							=			
Group Windows Application Servers						Enable Automa	atic Approval			
Status Unknown Compliance recommendations are not approved automatically										
Run I Y Schedule I Y										
				No scheduling op	tions were specifie	d. Click Schedule to	change these options			
All Configured Checks	Coffware Checks	Mawad Caffuara Caffuara Canfauratian Chaola	Intification Cotus							
All configured checks Security checks	SUILWAIR CITEURS	Allowed Software Software computation checks	vouncation Setup							
Compliance Checks 🎽 Filter > 🎋 🗇 🛊 🖕	⇔ 1 - 3 of 3 ⇒	System Message	[X		El/	Download			
Compliance Check				Last Sc	an	Compliant				
TIMv621_agent	1					New	×			
Vindows Screen Saver	1					New	×			
Master IBM-Http	1	COPTSK162I - The provisioning task has started.	Do you want to go to the			New	X			
		Provisioning Task Tracking application to monitor t	he task?	New Checks from Model Comput-	er 📄 🗌	New Compliance Ch	eck : 🔻			
			Yes No							

Figure 9-41 Running compliance scan and check

When running the scan, depending on the types of compliance checks requested, a series of discoveries are performed to collect all the relevant information. See Figure 9-42.

Provisioning Task Tracking			◆Beturn IEM.
Find: Select Action	💌 🚯 🗟 🧶 🗍 🔶		
List Task			
Provisioning Task Compliance Scan and Check Type Compliance Scan and Check Created By MAXADMN Changed By	Compliance Scan and Check		Definition Compliance Scan and Check Start Date 2009-07-22 01:42:06 End Date Status In Progress
Provisioning Workflows 🌶 Filter > 🚓 🗊 🛊 👙 🔶 1 - 4 of 4 🧇			^{®}} <u>Download</u> [? ■
Provisioning Workflow Status		Start Date	End Date Concurrency Level Subtask
Discovery.OnDevice In Progress	1	2009-07-22 01:42:08	5 Discovery.OnDevice
Discovery.OnDevice In Progress	1	2009-07-22 01:42:09	5 Discovery.OnDevice
Discovery.OnDevice In Progress	×	2009-07-22 01:42:09	5 Discovery.OnDevice
Compliance_Validation Scheduled	1		5 Compliance_Validation

Figure 9-42 Running compliance scan and check

For software and security checks, the system performs a Tivoli Provisioning Manager inventory discovery. This is based on the Common Inventory Technology scan (CIT) used to collect hardware and software information and the Security Compliance Manager collectors technology (SCM) utilized to discover security configurations, as shown in the portions of the provisioning workflow logs reported in Figure 9-43 and Figure 9-44.

•	2009-08-14 22:38:08	08.327	Start workflow: 'Cit_SDI_OnDevice'
•	2009-08-14 22:38:08	08.359	Starting CIT Discovery over SDL
•	2009-08-14 22:38:08	08.374	Discovery-Technology CitScannerAgent is associated with Device ID 8857
•	2009-08-14 22:38:09	09.905	Associated discovery and resolved discovery properties.
•	2009-08-14 22:39:25	25.046	CIT Discovery over SDI Submitted.
•	2009-08-14 22:39:25	25.062	End workflow: 'Ctt_SDL_OnDevice'

Figure 9-43 Compliance scan log

2009-08-14 21:32:24	24.155	Start workflow: 'SCM_S0I_OnServers'
2009-08-14 21:32:24	24.249	Associate discovery and with target computers start
2009-08-14 21:32:25	25.171	Discovery-Technology SCMColectorAgent is associated with Device D 8857
2009-08-14 21:32:25	25.171	Associated discovery and resolved discovery properties.
2009-08-14 21:32:25	25.202	Associate discovery and with target computers end
2009-08-14 21:32:25	25.546	Resolved ScanScopeD: 6464
2009-08-14 21:32:25	25.718	Start workflow: 'CdsPublishSCMinputFile'
2009-08-14 21:32:26	26.499	SCMFlePathinTIO: CVProgram Flex/BMt/vol/tpm/SCMCollectorAgent
2009-08-14 21:32:29	29.468	Start workflow: 'GenerateSCMInpuFile'

Figure 9-44 Compliance scan log

In the case of software configuration checks, the product launches a TADDM Discovery to synchronize data from TADDM to the Tivoli Provisioning Manager Data Center Model before checking the configuration details, as you can see in the portion of the provisioning workflow log reported in Figure 9-45.

•	2009-08-14 22:38:08	08.452	Start logical operation: 'Discovery.OnDevice'
•	2009-08-14 22:38:08	08.577	Start workflow: 'TADDM_Discovery_On_Device'
•	2009-08-14 22:38:08	08.624	Starting TADDM discovery with discovery technology: 7811 on device: 8857
•	2009-08-14 22:38:08	08.702	Loading TADDDM resource mapping
•	2009-08-14 22:38:08	08.765	Loading TADDM Application Registry XML plugin file
•	2009-08-14 22:38:26	26.390	TADDM-Network discovery time: 813 (ms)
•	2009-08-14 22:38:28	28.546	Computer: 8857 already exists in the DCM. Updating.
•	2009-08-14 22:38:29	29.265	Nic: 8858 already exists in the DCM. Updating.
•	2009-08-14 22:38:30	30.437	Network interface: 8859 already exists in the DCM. Updating.
•	2009-08-14 22:38:30	30.640	removed 0 unknown ip devices
•	2009-08-14 22:38:30	30.687	Total TADDM-Network discovery time: 5(s) (including DCM updates)
•	2009-08-14 22:38:30	30.702	Processing Computer nc117177.romelab.it.ibm.com
•	2009-08-14 22:39:03	03.327	Completed the TADDM Discovery.
•	2009-08-14 22:39:03	03.343	Total 1 computers are processed.

Figure 9-45 Compliance scan log

6. After the Compliance Scan and Check has been performed, it is possible to check on the **Recommendations** tab to see whether there are any noncompliance issues to resolve. See Figure 9-46.

Step 8: Review and approve recommendations

Recommendations identify the actions required to resolve noncompliance issues. The compliance checking process generates a recommendation for each noncompliance issue. The person in charge of this task is again the *Compliance Analyst*.

To review the recommendations generated for our noncompliance issues:

- 1. Select Go To \rightarrow Provisioning \rightarrow Provisioning Groups.
- 2. Select the desired group and click the **Recommendations** tab.

Provisioning Groups	G Web Replay	Bulletins: (0) 🎓 go To 💷 Reports 🏶 Start Genter 🌲 Profi	ile × Sign Out ? Help IEH.
🔽 Find: 🕅 🗣 Select Action 🔍 😍 🎒 🍙 🧶	4 4		
List Group Compliance Recommendations Variables			
Group Windows Application Servers View by Computer View by Recommendation			
Compliance Recommendations > Filter > 66 20 + 4 + 1 - 5 of 8 +			Download ?
Recommendation ID Computer	Recommendation	Recommendation Time	Status
9,297 nc117177.romelab.it.ibm.com	Install the required software "ITMv621 agent".	2009-07-22 01:46:16	Opened
9,336 nc117177.romelab.#.bm.com	Change the value of the "IBU-thic-ServerVirideova, discovervirier vertication-barrandeers/keep-layer sating to "On" of software installation TBU-third Server 6. 10.23 Apacher 2.4.7" to match the complemi value.	2009-07-22 01:46:23	Opened =
9,339 nc117177.romelab.it.bm.com	Change the value of the VBU-Htbc-ServerWindows.discovervier verconfice-arameters/advices/advices/advices/advices/ tsi'setting to 100° of adviare instalation "EMI ITTP Server_ 6.1.0.23 Appendix2.0 aT to match the combinit value.	2009-07-22 01:46:23	Opened
9,384 nc117177.romelab.it.bm.com	Change the value for the "Active" setting for the user "Administrator" to match the compliant value.	2009-07-22 01:46:33	Opened
9,366 nc117177.romelab.it.bm.com	Set or remove the Windows screen saver password for the user "Administrator" in order to match the compliant value.	2009-07-22 01:46:33	Opened
Toggle Select All		Approve Open Run Schedule	Ignore Close

Figure 9-46 Viewing recommendations

As shown in Figure 9-46, a list of recommendations for our target computer (nc117177) is displayed reporting all the actions to be taken to resolve the noncompliance issues:

- Install the ITM v6.2.1 OS Agent.
- Change the value of two parameters regarding the configuration of the *IBM HTTP Server* application (set *KeepAlive* to "**0n**" and *MaxKeepAliveRequests* to "**100**").
- Activate the screen saver for the Administrator account (this is the only account defined on the system) and set a password according to the defined compliant settings.

In fact, our target computer does not have the ITM v6.2.1 OS Agent installed and the screen saver activated, and it does not have a standard configuration for the *IBM HTTP Server*. We can see that the current values (*KeepAlive* and *MaxKeepAliveRequests* parameters are set to "**0ff**" and "**50**" respectively) for that computer in the Software Resource details panel are populated with the data imported from TADDM. To open the Software Resource details panel:

- 3. Select Go To \rightarrow Provisioning \rightarrow Provisioning Computers.
- 4. Click the target computer **nc117177** and select the **Software** tab.
- 5. Filter for the IBM HTTP Server entry and click it. See Figure 9-47.

Provisioning Computers		🕑 Web Replay	🦉 <u>B</u> uletins: (0) 🛛 🧖 Go To	LLL <u>R</u> eports 🎁 Start <u>C</u> enter 🕯	Profile Sign Out ? <u>H</u> e	^{ap} IBM.
Find: Select Action	0 🖞 🗟 🖉 🏟					
List Computer Hardware Software Compliance	Recommendations C	redentials Workflows Variables De	ployment Properties			^
Computer nct17177.romelab.it.lbm.com	Operating System Agent	Windows Server 2003 Enterprise x64 Edition S	Statistics	82 Products Installed / 0 Patche	es Installed	
 ⊙ All ⊙ Software ○ Patches 						
Software Installations 🛛 🛪 Filter 🖓 🔞 😓 🖓 🤞 🖓 11 - 20 of 82 🥪 💦					By Downlos	ad ? =
Software Installation	Version	Software Definition	Installa	ble Status		
HBM Tiveli Monitoring - Windows OS Agent (Version 6.2)	6.2	IBM Tivoli Monitoring - Windows OS Agent 6.2				Û
BM HTTP Server - 6.1.0.23 Apache/2.0.47	2.0.47.1	IBM-Http-Server				Û
Activemovie	10.0.0.3997	activemovie - 10.0.0.3997				Û

Figure 9-47 Verifying results

6. In the *Software Resources* box, expand the *server* entry, and click **configResource**. See Figure 9-48.

Software Resources				↑ <u>R</u> eturn IBI€.
Find: Select Action				
List Software Resource				^
Software Resources				-
C = IDM_HTTF_Server+0.10.23 Apadte/2.0.47	Details Workflows Variables			
🖬 📕 Web Module WebSphere Plugin				
Web Module access_module	Software Resource Details			-
Web Module actions_module	Computer Name	nc117177.romelab.it.ibm.com	1	
Web Module suits module	Software Medule	IRM. Http. Server		
Web Module autoindex module	Software Module	iom-mup-derver		
Web Module ogi_module	Software Installable			
Web Module dir_module	Status	Unknown		
Web Module env_module	Requirements > Filter > 40 12 4 4 4	-1 of 1 ->		Download 12
Web Module indude_module				Dominoad
Web Module log_config_module	Requirement Type		Requirement	
Web Module mime_module) US		os.tamily	
Web Module sective_module				New Requirement
🖬 📰 configResource 😽	Capabilities 🕨 Filter > 🖓 🔁 🔶 🔶 🔶			Le <u>Download</u> ?
	Capability Type	Capability	Capability Value	
		No rows	to display	
				New Capability
	Configuration Template:			config-parameters
	Template Parameters 🌶 Filter 🤌 🗊 🛊	👙 🐟 1 - 10 of 29 🧼		😫 <u>Download</u> ? 📼
	Parameter	Description V	alue	
	ServerRoot		C:/Program Files/IBM/HTTPServer"	×
	PidFile	lo	qs/httpd.pid	×
	Timeout	3	0	×
	Keenálive		"	
	HawKasa AlivaBaawaata			
	Maxicephaiverequests	5		<u>0</u>
	KeepAliveTimeout	1		<u>`</u>
	ExtendedStatus	0	n	X
	ServerAdmin	y	pu@your.address	×
	ServerName	n	c117177.romelab.it.ibm.com:80	×
	UseCanonicalName	0	ff	×
				New Parameter

Figure 9-48 Verifying results

The settings of the two parameters mentioned for the reference configuration are actually "0n" and "100", as shown in Figure 9-38 on page 253.

By default, recommendations are created in the **Open** state. It is possible to take the following actions to change the state:

- Approve: Before an automated remediation can be applied for a recommendation, you must approve it.
- Close: Closing a recommendation changes its state to Implemented. You can use this action for issues that must be resolved manually.
- **Ignore**: Use this action if you do not want to apply a recommendation.
- Open: Use this action to reopen a recommendation that is in any of the other states.

We want to approve the recommended actions.

7. In order to approve the actions, we select the check box for each recommendation and click **Approve**. See Figure 9-49.

Provisioning Groups - Microsoft Internet Explorer			
File Edit View Favorites Tools Help			At
🌀 Back 🝷 🕥 🔄 📓 💰 🔎 Search 👷 Favorites 🤣 🎯 🤹	🔒 🖃 🥃		
Address 🗃 https://nc117218.romelab.it.ibm.com:9443/maximo/ui/login			🛩 🋃 Go
Google 🚽 🐫 Search 🚥 🍏 ד 😭 ד 🏠	Bookmarks* 🏾 🤣 Check • 🧏 AutoFill • 🌛		Links *
Provisioning Groups		⊃ Web Replay 🤒 Bulletins: (0) 🎓 go To 💷 Beports 🕈 Start Center 🔺 Pro	ofile X Sign Out ? Help IEM.
💌 Find: 🔥 🔻 Select Action 💌 😍 门 🔒 🧶	🏟 🔅		
List Group Compliance Recommendations Variables			^
Group Windows Application Servers			
View by Computer View by Recommendation			
Compliance Recommendations > Filter > (A) 2 + + + 1 - 5 of 5 ->			Download ? =
<u>Recommendation ID</u> Computer	Recommendation	Recommendation Time	Status
9,297 nc117177.romelab.it.ibm.com	Install the required software "ITMv621 agent".	2009-07-22 01:46:16	Opened
9,336 nc117177.romelab.il.bm.com	Change the value of the "IBU-Hto-Server/Vindows.discover/view vericonte-astranetres/KesseAive" setting to "On of software installation "IBU-HTD" Server-6.10.23 Asache/2.0.47* to match the compliant value.	2009-07-22 01 48 23	Opened
9,339 nc117177 romelab. #.Dm.com	Change the value of the 7/80 - Http:Server/Window s discover/view verticedia-parameters MaxKeepAlveReques is* setting to 100° of settivary instalation "BM HTTP Server - 6.1.0.23 Apasche2.0.47" to match the company value of the setting of the setting of the company value of the setting of the setting of the setting company value of the setting of the setting of the setting of the company value of the setting of the setting of the setting of the company value of the setting	2009-07-22 01 48 23	Opened
9,364 nc117177.romelab.II.bm.com	Change the value for the "Active" setting for the user "Administrator" to match the compliant value.	2009-07-22 01:46:33	Opened
v 9,366 nc117177.romelab.it.ibm.com	Set or remove the Windows screen saver password for the user "Administrator" in order to match the compliant value.	2009-07-22 01:46:33	Opened
Toggle Select All		Approve Open Run Scheduk	e Ignore Close
Done			Sucal intranet

Figure 9-49 Approving recommendations

All the recommended actions are now in the **Approved** status as shown in Figure 9-50.

Provisioning Groups	C Web Replay	Bulletins: (0) 🎤 Go To 💷 Reports 希 Start Çenter 🌲 Profile	×Sign Out ?Help III₩.
🔽 📕 Find: 🔤 🛱 🔝 Select Action 🔤 🚯 🗍 🗔 🧶 I 🎄 🛊			
List Group Compliance Recommendations Variables			^
Group Windows Application Servers View by Computer View by Recommendation			
Compliance Recommendations > Filter > (A 2 4 + 4 1 - 5 of 5 +			🖄 Download 🔅 📼
Recommendation ID Computer	Recommendation	Recommendation Time	Status
9,297 nc117177.romelab.it.ibm.com	Install the required software "ITMv621_agent".	2009-07-22 01:46:16	Approved
9,336 nc117177.rometab.t.bm.com	Change the value of the "IBH-ITL-ServerWindows discoverwiser vertices for anothers Medica-Alve" setting to "Con" of a chiver a shalladion TBH ITTL Server a 51,022 Apactor 2,047 to match the compliant value.	2009-07-22 01:46:23	Approved
9,339 nc117177.romelab.ll.bm.com	Change the value of the 'IBI-Http://www.discovern/iker ver/confo-acametera/ika/Keps/kveReuse ts' astimato T00° of software mstalistion TBI HTTP Server: 5.1.023 Apacteg 0.471 to match the completer value.	2009-07-22 01:46:23	Approved
9,384 nc11717.romelab.it.bm.com	Change the value for the "Active" setting for the user "Administrator" to match the compliant value.	2009-07-22 01:48:33	Approved
9,366 nc117177.romelab.it.bm.com	Set or remove the Windows screen saver password for the user "Administrator" in order to match the compliant value.	2009-07-22 01:46:33	Approved
Toggle Select All		Approve Open Run Schedule	Ignore Close

Figure 9-50 Approving recommendations

Step 9: Implement recommendations

After being approved, each recommended action can be performed by running a workflow or by scheduling it to run at a convenient time. In this scenario, all the workflows that automate the remediation actions required to resolve the noncompliance issues reported are provided out of the box by Tivoli Provisioning Manager. We run all the recommendations immediately.

The person in charge of this task is the *Deployment Specialist*.

The tasks to run the remediation actions are as follows:

- 1. Log in to the Tivoli Provisioning Manager console as a user with the TPDEPLOYMENTSPECIALIST role.
- 2. Select Go To \rightarrow Deployment \rightarrow Provisioning Groups.
- 3. Select the provisioning group for which the compliance checks were run, then click the **Recommendations** tab.
- 4. Check all the recommendations and click Run. See Figure 9-51.

Provisioning Groups	🕑 Web Replay 👎 Bulet	tins: (0) 🔌 <u>G</u> o To 💷 <u>R</u> eports 🏚 Start <u>C</u> enter 🔺 <u>P</u> rofile	X Sign Out ? Help TEM.
🌱 Find: 🛛 🧑 🔫 Select Action 🔍 🚯 🎽 🛃 🧶 🕴 🌳			
List Group Compliance Recommendations Variables			~
Group Windows Application Servers Vew by Computer Vew by Recommendation			
Compliance Recommendations 👂 Filter 🤉 🏟 😂 🛊 🐐 🗢 1 - 5 of 5 🧇			🕒 Download ? 🖶
<u>Recommendation ID</u> Computer	Recommendation	Recommendation Time	Status
9,297 nc117177.romelab.it.ibm.com	Install the required software "ITMv621 agent".	2009-07-22 01:46:16	Approved
9,336 nc117177.romelabili.bm.com	Change the value of the "IBL-Main-ServerWindows discoverviser ver/confo-parameters/KeepAlve" setting to "On" of software mahalarian "IBL HTTP Server - 6.10.23 Apache/2.0.47" to match the compliant value.	2009-07-22 01:46:23	Approved
9,339 nc117177.romelab.l.bm.com	Change the value of the TBH-THD-ServerVivindows discoverviser vectorofics are understandarderstandard statistication to the off of the state of the statistication that the server- 6.10.23. Asachec 2.0.47. to match the company value.	2009-07-22 01:46 23	Approved
9,364 nc117177.romelab.il.bm.com	Change the value for the "Active" setting for the user "Administrator" to match the compliant value.	2009-07-22 01:46:33	Approved
9,366 nc117177.romelab.it.bm.com	Set or remove the Windows screen saver password for the user "Administrator" in order to match the compliant value.	2009-07-22 01:46:33	Approved
Toggie Select All		Approve Open Run Schedule	Ignore Close

Figure 9-51 Implementing recommendations

A provisioning task will be created to run the workflows that perform the remediation actions to bring the computer into a compliant state. A panel, as shown in Figure 9-52, will give you the option to view the task details.

Provisioning Groups	🕑 Web Replay 🕌	<u>B</u> ulletins: (0) 🌈 Go To 🔟 <u>R</u> eports 🏚 Start <u>C</u> enter 🚢 <u>P</u> rofile	e [×] Sign Out ? <u>H</u> elp <u>III</u> ,
Image: Select Action List Group Compliance Recommendations Variables)		A
Group Windows Application Servers View by Computer View by Recommendation			
Compliance Recommendations : Pritter > 0 : 2 : 4 . 4 . 5 of 5	Decomposedation	Decommodation Time	Status
Precommendation Output Output	Install the required software	2009-07-22 01:46:16	Approved
⊙ 9,336 nc117177.romelab.l.bm.com	System Message OPTSK1621 - The provisioning task has started. Do you want to go to the Provisioning Task Tracking application to monitor the task?	2009-07-22 01:48-23	Approved
	Yes No		

Figure 9-52 Implementing recommendations

5. By clicking **Yes**, the *Provisioning Task Tracking* panel opens, and it is possible to view the progress of the task and, if needed, open the task log. See Figure 9-53.

Provisioning Task Tracking			CUTION DESCRIPTION			≜ <u>R</u> eturn IIII
Find: Find: Select Action	💌 🚯 🗟 🧶 🔶 🔶					
List Task						
Provisioning Task Compliance Remediation (7/22/09 1:49 AM) Type Compliance Remediation Created By MAXADMN Changed By	Compliance Remediation (7/22/09 1:49 A	ν.M]		Definition Start Date End Date Status Base Services Task	Compliance Remediation [7/2209 1:49 AM] # 2009-07-22 01:49 54 in Progress #	
Provisioning Workflows 🌶 Filter > 💥 😂 🛊 🖕 😞 1 - 4 of 4 🧄 🖉						Download 1 2
Provisioning Workflow	Status	Start I	Date End Date	e Concurrency	Level Subtask	
ComplianceRecommendation.Remediate	In Progress 🥖	2009-	07-22 01:49:55		5 ComplianceRecommendation.Remedia	e
ComplianceRecommendation.Remediate	In Progress	2009-	07-22 01:49:55		5 ComplianceRecommendation.Remediate	
ComplianceRecommendation.Remediate	In Progress 🥒	2009-	07-22 01:49:56		5 ComplianceRecommendation.Remediate	
ComplianceRecommendationGroup.Remediate	In Progress 🧪	2009-	07-22 01:49:56		5 ComplianceRecommendationGroup.Remediat	e
Notification						

Figure 9-53 Implementing recommendations

The launched workflows will perform the installation of the ITM v6.2.1 OS Agent and the activation of the screen saver for the Administrator account, enabling password protection after a maximum of 10 minutes idle-time.

Another workflow will modify the configuration file (httpd.conf) on the target computer to change the two noncompliant parameter settings for the *IBM HTTP Server* application, as shown in the portion of the recommendation workflows log depicted in Figure 9-54.
Þ	2009-08-14 22:18:10	10.312	Performing software configuration remediation on IBM-Http-Server
Þ	2009-08-14 22:18:11	11.499	IBM-Http-Server is installed at C:/Program Files/IBM/HTTPServer
۲	2009-08-14 22:18:16	16.343	Files for recommendation group: 1
۲	2009-08-14 22:18:16	16.499	Delimiter for httpd.conf: ''
۲	2009-08-14 22:18:16	16.874	File location: C:/Program Files/IBM/HTTPServer/conf
Þ	2009-08-14 22:18:17	17.374	Number of recommendations in recommendation group:11122 is 2
Þ	2009-08-14 22:18:18	18.327	Found srt rule for software configuration recommendaiton 11080: 10763
►	2009-08-14 22:18:19	19.249	Found paramPath: //BM-Http-Server/Windows.discovery/server/config-parameters/MaxKeepAliveRequests
Þ	2009-08-14 22:18:20	20.046	Found file: httpd.conf
Þ	2009-08-14 22:18:20	20.202	Found srt rule for software configuration recommendation 11077: 10762
Þ	2009-08-14 22:18:20	20.249	Found paramPath: //BM-Http-Server/Windows.discovery/server/config-parameters/KeepAlive
Þ	2009-08-14 22:18:20	20.515	Found file: httpd.conf
Þ	2009-08-14 22:18:20	20.671	Recommendations for httpd.conf: 2
Þ	2009-08-14 22:18:24	24.343	Parameter/Desired Value: MaxKeepAliveReguests/100
	2009-08-14 22:18:28	28.968	Parameter/Desired Value: KeepAlive/On

Figure 9-54 Recommendation workflows log

The workflow will then will restart the *IBM HTTP Server* application in order for the applied changes to take effect. Finally it will instruct TADDM to run an L3 sensor discovery to bring in the new configuration settings for the target computer into TADDM, as reported in the portion of the recommendation workflows log depicted in Figure 9-55.

> 2009-08-14 22:19:48	48.015	End logical operation: 'Device.ExecuteCommand'
2009-08-14 22:19:48	48.093	The IBM HTTP Server 6.1 service is starting. The IBM HTTP Server 6.1 service was started successfully.
2009-08-14 22:19:48	48.140	End workflow: IBMHttp_Start
2009-08-14 22:19:48	48.171	End workflow; 'BIIHttp_SoftwareInstance_Start'
> 2009-08-14 22:19:48	48.265	End logical operation: 'SoftwareInstance.Start'
> 2009-08-14 22:19:48	48.437	The discovery D for the recommendation group matches TADDM Discovery.
2009-08-14 22:19:48	48.546	Management IP for server is 9.168.117.177
> 2009-08-14 22:19:49	49.827	Profile found for IBM-Http-Server. Run TADDM Sensor Discovery using Level 3 Discovery.
> 2009-08-14 22:19:49	49.984	Start workflow: TADDM_Sensor_Discovery_with_Profile
> 2009-08-14 22:19:52	52.577	TADDM Scope created with 1 IP addresses.
> 2009-08-14 22:19:52	52.765	TADDM Run Definition created.
2009-08-14 22:20:23	23.718	The discovery has started.
2009-08-14 22:20:24	24.671	A TADDM sensor discovery has been started using the profile Level 3 Discovery. Manual refresh of the Product Console is required to view changes once discovery is complete.
> 2009-08-14 22:20:24	24.687	End workflow: "TADDM_Sensor_Discovery_with_Profile"
> 2009-08-14 22:20:24	24.749	Deleting recommendation group with id 11122
> 2009-08-14 22:20:28	28.827	End workflow: 'Software_Config_Group_Remediate_TextFile'
> 2009-08-14 22:20:28	28.905	End logical operation: 'ComplianceRecommendationGroup.Remediate'

Figure 9-55 Recommendation workflows log

Important: With the next scan and check that will be run, a TADDM Discovery from Tivoli Provisioning Manager will be launched and the new configuration data will be updated also in the Tivoli Provisioning Manager Data Center Model.

After the remediation workflows have been successfully completed, the recommended actions will move to the **Implemented** status, as shown in Figure 9-56.

肖 Provisioning Groups	O Web Repla	y 🨫 <u>B</u> ulletins: (0) 🎢 <u>G</u> o To 🔛 <u>R</u> eports 👫 Start <u>C</u> enter	Profile X Sign Out ? Help TEM.
💌 Find: 🕅 🔻 Select Action 🔍 🚯 】 詞	2 4 4		
List Group Compliance Recommendations Variables			^
Group Windows Application Servers			
Compliance Recommendations ♦ Filter > ఈ □ ♦ ♦ ♦ 1 - 5 of 5 ↔			🖄 <u>Download</u> 📪 📼
Recommendation ID Computer	Recommendation	Recommendation Time	Status
9,297 nc117177.romelab.it.ibm.com	Install the required software "ITMv621 agent".	2009-07-22 01:46:16	Implemented
9,336 nc117177.romelab.il.bm.com	Chance the value of the <u>VBU-HIII-Server/Windows discoverviser</u> vertconfbe_arameters/KeepAhe* setting to "to" of software residention <u>"BII_HITP_Server-8.10.23</u> <u>Acaehe20.47" to match the compliant</u> value.	2009-07-22 01.46.23	Implemented
9,339 nc117177.romelab.il.bm.com	Channe the value of the "(BiLHttm-Saren eVintows a discoverwher "reflocing-arranger and MacKspaAlvefeeues Is setting to "10" of software instation (BM HTTP Sarener: 6.10.23 Appender 20 47 to match the comparison value.	2009-07-22 01 46 23	Implemented
9,364 nc117177 romelab it.lbm.com	Change the value for the "Active" setting for the user "Administrator" to match the compliant value.	2009-07-22 01:46:33	Implemented
9,366 nc117177 romelab it.bm.com	Set or remove the Windows screen saver password for the user "Administrator" in order to match the compliant value.	2009-07-22 01:46:33	Implemented
Toggle Select AI		Approve Open Run S	chedule Ignore Close

Figure 9-56 Implementing recommendations

6. The compliance status will still show "Not Compliant", as you can see in Figure 9-57.

All Co	onfigured Checks Security Checks	Software Checks	Allowed Software Software Configuration Checks Notification Setup			1
Comp	liance Checks 🕨 Filler > M 🗊 🔄 🐳 🗧	1 - 3 of 3 🧇			R	Download ?
	Compliance Check		Туре	Last Scan	Compliant	
	ITMv621_agent	1	Software Module	2009-07-22 01:45:12	0/1	×
	Windows Screen Saver	1	Security	2009-07-22 01:44:26	0/1	×
	Master IBM-Http	1	Software Configuration	2009-07-22 01:42:25	0/1	×
			Delete Chaster Casu Chaster	New Checks from Medal Computer	New Cemelanas C	haak : 💌

Figure 9-57 Compliance status

Step 10: Verify compliance

It is necessary to run a new compliance check to ensure that all recommended actions have been successful applied. Refer to "Step 7: Run compliance checks" on page 253.

Note: A simple check would be sufficient to verify software and software configuration compliance after running the remediation actions (just by querying the database). Because we have also a security compliance check, it is needed to run a Tivoli Provisioning Manager inventory scan as well on the target computer to verify that the security settings have been applied. So we run both scans and check again as shown in Figure 9-58.

Provisioning Groups	• Web Replay	₱ <u>B</u> uletins: (0) ₱ <u>G</u> o To <u>I</u> <u>M</u> <u>R</u> eports ₱ State	irt <u>C</u> enter ▲ <u>P</u> rofile × Sign Out	^{2 Lep} IIM.
Find: 🕅 🔻 Select Action 💌 😢	1 🖬 🖉 🛊 🔅			
List Group Compliance Recommendations Variables				
Compliance Scan				=
Group Windows Application Servers		Com	Enable Automa	tic Approval
Al Configured Checks Security Checks Software Checks Allow	ed Software Software Configuration Checks Notification Setup	No scheduling options v	were sp Check Scan and Check	chedule : V
Compliance Checks > Filter > 🔅 🗊 + 🔰 + 1 - 3 of 3 ->			E)	Download 🕴 📟
Compliance Check	Туре	Last Scan	Compliant	
TMv621_agent	Software Module	2009-07-22 01:45:12	0/1	X
🗌 Windows Screen Saver 🧳	Security	2009-07-22 01:44:26	0/1	×
🗌 Master IBM-Http 🍡	Software Configuration	2009-07-22 01:42:25	0/1	×
	Delete Checks Copy Checks	New Checks from Model Computer	New Compliance Che	ick : 🔻

Figure 9-58 Running compliance check

Continue by using the following steps:

1. When the Compliance Scan and Check is completed, click **Return** to return to the list of the compliance checks and then click the **Refresh** icon.

Our target computer nc117177 is now compliant for each of the compliance checks defined, as shown in Figure 9-59.

Provisioning Groups		🕑 Web F	teplay 🥊 Bulletins: (0) 🎤 Go To 🛄 Reports 👫 Start (Center ⁴ Profile ^X Sign Out ? Help III.
Find:	Select Action 💌 🚯 门 🔒 🧶 🎄 💠			
List Group Compliance Recomment	dations Variables			
Compliance Scan				8
Group Windows Application Servers				Enable Automatic Approval
Status Compliant			Complian	ice recommendations are not approved automatically
				Run : V Schedule : V
			No scheduling options were	e specified. Click Schedule to change these options
All Configured Checks Security Checks	Software Checks Allowed Software Software Con	figuration Checks Notification Setup		
		inger allow on one of the interest of the p		
Compliance Checks 🕨 Filler > 👫 [🗇 🗍 💠 1	- 3 of 3 🧇			Download ?
Compliance Check		Туре	Last Scan	Compliant
TMv621_agent]/	Software Module	2009-07-22 02:06:09	(1/1) X
Windows Screen Saver	1	Security	2009-07-22 02:05:25	1/1 🗙
Master IBM-Http	1	Software Configuration	2009-07-22 02:01:34	1/1 ×
		Delete Checks Copy Cher	ks New Checks from Model Computer	New Compliance Check : 🔻

Figure 9-59 Verifying compliance

 You can also find the compliance status of our target computer by clicking Go To → Deployment → Provisioning Computers, as shown in Figure 9-60.

Provisioning Computers			C Web Replay P Bulletins: (0)	Go To I ^M Reports A Start Center A Profile X Sign Out ? Help Help Sign Out Y Sign Out Y Help Help Sign Out Y Help Help Help Sign Out Y Help Hel	IBM.
Y Find:	🔻 Select Action 🛛 🖌 🚷 🎾 🔒 🖉 I	4 \$ P			
List Computer Hardware Softw	vare Compliance Recommendations	Credentials Workflows Variables	Deployment Properties		
🕅 Advanced Search 🔻 🗟 Save Query 🔻 🔗 Bo	okmarks				
Computers 🕴 🛛 Filter > 🃸 🛛 💱 🛊 🛊 🛊 4 - 5 of 5	+			E/ Down!	oad 🕴 🖻
Computer 🕈	Operating System	<u>Globally Unique Identifier</u>	Agent	Compliance Status	
nc117175.romelab.it.ibm.com	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	E172FE27C9BD3F45AA5450459EA4CF88	TCA-1.4.2.0	No compliance checks configured	X 🏘
nc117177.romelab.it.lbm.com	Microsoft Windows Operating System 2003 server x64 Enterprise Edition SP2 [Version SP2]	2A978E3C949134DE8DB22A7D515D441D	TCA-1.4.2.0	Compliant	¥ &

Figure 9-60 Verifying compliance

9.4.4 Scenario conclusion

At the end of our scenario, our target computer meets the desired setup:

► The ITM v6.2.1 OS Agent is installed, as shown in Figure 9-61.



Figure 9-61 Verifying compliance on target computer

The screen saver for the Administrator account is activated to start after 10 minutes of idle-time, with password protection. See Figure 9-62.



Figure 9-62 Verifying compliance on target computer

The configuration file (C:\Program Files\IBM\HTTPServer\conf\httpd.conf) for the IBM HTTP Server application has been changed, modifying the settings of the two parameters to the compliant values. (This has been automatically performed by the remediation workflow.) See Example 9-1.

Example 9-1 httpd.conf file

```
# KeepAlive: Whether or not to allow persistent connections (more than
# one request per connection). Set to "Off" to deactivate.
#
KeepAlive On
#
# MaxKeepAliveRequests: The maximum number of requests to allow
# during a persistent connection. Set to 0 to allow an unlimited
amount.
# We recommend you leave this number high, for maximum performance.
#
MaxKeepAliveRequests 100
```

- After the last scan, check that it launched a TADDM Discovery on the Provisioning server to synchronize data between TADDM and Tivoli Provisioning Manager database. Also, the Software Resources details panel shows the updated compliant values for the two previous parameter settings on our target computer. To see the new values:
 - a. Select Go To \rightarrow Provisioning \rightarrow Provisioning Computers.
 - b. Click the target computer nc117177 and select the Software tab.
 - c. Filter for the *IBM HTTP Server* entry and click it (Figure 9-63).

Provis	sioning Computers			🕑 Web Rep	olay 🎴 <u>B</u> ulletins: (0) /	^ф <u>G</u> o To Ш⊔ <u>R</u> e	eports 🏾 🏛 Start <u>C</u> enter	Profile X Si	gn Out ? <u>H</u> elp	IBM.
	Y Find:	🚯 🔝 Select Action	🛛 🚯 🏷 🗟 🧶 🖣 🗉	e e						
List	Computer Hardware	Software Compliance	Recommendations Cre	dentials Workflows Variables	Deployment Properties					
Compute	nc117177.romelab.it.ibm.com		Operating System	Windows Server 2003 Enterprise x64 Edition S 🎤		o	Desidential installed (0 D	tobas lostellad		
Last Sca	n		Agent	TCA-1.4.2.0		Statistics o	5 Products Installed 7 0 Pr	atches installed		
								_		
O Callura										
O Detebes	5									
Patches										
Software In:	stallations 🛛 🔻 Filter >🐴 🗇 🔶	🍦 👍 11 - 20 of 83 🥪							E/ Downlos	ad ? 📼
	Software Installation		Version	Software Definition		Installable S	Status			
	IBM Tivoli Monitoring		621	IBM Tivoli Monitoring - 621						Û
	IBM Tivoli Monitoring - Windows O	<u>)S</u>	6.2	IBM Tivoli Monitoring - Windows OS						Û
I	Agent Iversion 6.21			Agent 6.2						-
	IBM HTTP Server - 6.1.0.23 Apac	che/2.0.47	2.0.47.1	IBM-Http-Server						
	activemovie		10.0.03997	activemovie - 10.0.0.3997						
	Windows Marketplace Link		1.0.0.0	Windows Marketplace Link - 1.0.00						
	Symantec Antivirus Win64		10.1.7000.7	Symantec Antivirus Win64 - 10.1.7000.7						
	Ineme Component		1.1.1.7	Ineme Component - 1.1.1.7						
	BRANDING CAR		0.0.0.1	Genoeup - 5.0.0.1						
	USD10		0.0.3790.1630	UED10 4 207 2406 4						
	05-10		1.357.2400.1	03610 - 1.307.2400.1						
							Add Soft	ware	Uninstall Softv	vare

Figure 9-63 Verifying compliance of target computer

d. In the *Software Resources* box, expand the *server* entry, then click **configResource**, as shown in Figure 9-64.

Software Resources	the second secon	↑ _{Beturn} IBM.
🖌 Find: 🕅 🤝 Select Action 🖌 🛃		
Liet Software Deenurce		
Software Resources		-
E BIDIT_HTTF_Server+0.1.0.23 Apadie/2.0.47	Details Workflows Variables	
Web Module WebSphere Plugin		
Web Module access_module	Software Resource Details	-
Web Module actions_module	Computer Name nc117177 romejab 8 ibm com	
Web Module allas_module		
Web Module subindex module	Software Module	
Web Module coi module	Software Installable	
Web Module dir module	Status Unknown	
Web Module env module		Pt
Web Module include_module	Requirements Filter > 1 2 4 + 1 - 1 of 1 +	Download 7
Web Module log_config_module	Requirement Type Requirement	
Web Module mime_module	OS os.family	Û
Web Module setenvif_module		New Requirement
Web Module userdir_module		
E server	Conshilting 1 - Eliter W 1711 - Alfred	G#
ConfigResource	coponince :	pomiopol = =
	Capability Type Capability Capability Capability Value	
	No rows to display	New Capability
Software Resources Image: Software Resource Software Resource Software Resource Image: Software Resource		
	Configuration Template:	config-parameters
	Template Parameters 🔺 Filter > 👯 🗊 🔶 🍦 🗢 1 - 10 of 29 🚕	Download ? =
	Parameter Description Value	
	ServerRoot "C:/Program Files/IBM/HTTPServer"	×
	PidFile logs/httpd.pid	×
	▶ Timeout 300	×
	KeepAlive On	×
	MaxKeepAlveRequests 100	×
	KeepAliveTimeout 10	×
	ExtendedStatus On	×
	ServerAdmin vou@vour.address	×
	ServerName nc117177.romelab.it.ibm.com:80	×
	UseCanonicalName Off	×
		New Parameter
Provisioning Computers > Software Resources		

Figure 9-64 Verifying compliance of target computer

The *KeepAlive* and *MaxKeepAliveRequests* parameters report the "**0n**" and "**100**" values respectively, as expected.

270 IBM Tivoli Provisioning Manager V7.1.1: Deployment and IBM Service Management Integration Guide

10

IBM Service Management integration scenarios: Incident Management integration with Tivoli Service Request Manager and ITIL

In this chapter we describe how the powerful integration capabilities of IBM Tivoli Provisioning Manager and IBM Tivoli Service Request Manager allow you to fulfil a typical Incident Management scenario.

We cover the following topics:

- An overview of the Incident Management process as part of ITIL
- An overview of Tivoli Service Request Manager and Service Desk functionality
- A description of the lab environment used to implement the integration scenario
- A description of the prerequisite steps to set up the integration scenario
- ► A description of the Incident Management integration scenario

10.1 Information Technology Infrastructure Library (ITIL) and Incident Management

In order to provide the basis for the Incident Management integration scenario, in this section we briefly introduce the Information Technology Infrastructure Library (ITIL). ITIL provides a non-proprietary framework for implementing service management best practices aligned with overall business objectives. Creating IT processes for ITIL guidelines enables organizations to more effectively manage IT changes, assets, personnel, and service levels.

10.1.1 Service considerations

The latest ITIL release, ITIL Version 3, focuses on best practices throughout the service life cycle. It addresses service and solution life cycle management by including the following five core volumes that we briefly describe next, Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement.

Service Strategy

This volume provides a view to align business and IT so that each brings out the best in the other. It ensures that every element of the Service life cycle is focused on customer outcomes and relates to all the companion process elements that follow. It includes the following processes:

- Strategy Generation
- Market Intelligence
- ► IT Financial Management
- Service Portfolio Management
- Demand Management
- Risk Management

Service Design

This volume provides guidance for the design of a new or changed service to introduce into the live environment, ensuring that there is a holistic approach to all aspects of design. It encompasses the following processes:

- Service Portfolio Management
- Service Catalog Management
- Service Level Management
- Capacity Management
- Availability Management
- Service Continuity Management
- Information Security Management
- Supplier and Contract Management

Service Transition

This volume provides guidance for the development and improvement of the capabilities for transitioning new and changed services into the production environment. It. includes the following processes:

- ► Change Management
- Service Asset and Configuration Management
- Knowledge Management and Service Knowledge System
- Service Release and Deployment Planning
- Performance and Risk Evaluation
- Testing
- Acquire, Build, Test Release
- ► Service Release, Acceptance, and Test and Pilot
- Deployment, Decommission, and Transfer

Service Operation

This volume introduces and explains delivery and control activities to achieve operational excellence on a day-to-day basis. It encompasses the following processes:

- Monitoring and Event Management
- Incident Management (actually the subject of this chapter)
- Request Fulfillment
- Problem Management
- Access Management

Continual Service Improvement

This volume provides guidance for continual alignment of the IT Services portfolio with the current and future business needs, growth, and maturity. It encompasses the following processes:

- Measurement and Control
- Service Measurement
- Service Assessment and Analysis
- Process Assessment and Analysis
- Service Level Management
- Improvement Planning

10.1.2 Incident Management process

As part of the Service Operation core module, Incident Management is the process of restoring normal service operation as quickly as possible to minimize an incident's adverse impact on business operations. In ITIL terms, an incident is any deviation from the expected standard operation of a system or a service. Best practice incident management involves immediate service restoration utilizing standard processes of investigation, diagnosis, resolution, and recovery.

10.2 Tivoli Service Request Manager

In this section we discuss the Tivoli Service Request Manager capabilities, including Service Desk functionality,

10.2.1 Overview of Tivoli Service Request Manager

Tivoli Service Request Manager is a solution that closely aligns IT operations and the business, improving IT service support and delivery performance. In other words, it is used to manage any type of critical enterprise asset, and to lower the cost of ownership. It is an integrated platform that improves the efficiency of service delivery and offers opportunities to drive down operating costs by consolidating your service desk and systems.

Built from the ground up on the ITIL framework, Tivoli Service Request Manager provides a comprehensive and modular approach to integrated *Service Desk* and *Service Catalog* management. In addition, this product enables you to establish and efficiently operate a corporate service desk for Service Requests around enterprise assets.

The scenarios described in this Redbooks publication focus on the Service Desk functionality.

10.2.2 Service Desk functionality

According to ITIL, organizations invest in a Service Desk to:

- Provide a single point of contact for users
- Deliver the high quality support critical for achieving business goals
- Help identify and lower cost of ownership for IT services as a whole
- Support changes across business, technology, and process boundaries
- Aid user retention and satisfaction
- Assist identification of business opportunities

The Service Desk component inside Tivoli Service Request Manager includes seven applications, described in Table 10-1, that help you improve the service level, keep costs down, improve agent productivity, quickly resolve incidents, and measure the satisfaction of end users.

Service Desk Application	Description
Global Search	Global Search allows searching across applications for records that contain specified text.
Incidents	Incident records capture information about an event that deviates from standard service or that might disrupt the service quality, The Incidents Application allows creating and modifying incident records.
Priority Matrix	A priority matrix defines, in advance, internal priorities for Service Desk tickets that specify given combinations of impact and urgency.
Process Requests	This application is used to create, view, and modify IT process requests for the various process managers.
Problems	A problem record allows capturing an unknown, underlying cause of one or more incidents.
Service Requests	A Service Request can be opened to resolve an issue, obtain new service, obtain information, or change a current service.
Solutions	The Solutions application allows creating and managing solutions records, containing predefined responses to commonly asked questions or problems.
Activities and Tasks	The Activities and Tasks application allows planning, reviewing, and managing activities and tasks.
Ticket Templates	The Ticket Templates application allows creating and managing generic ticket templates that Service Desk environments can leverage to standardize common or high-volume Service Requests, incidents, or problems.

Table 10-1 - Service Desk applications available in Tivoli Service Request Manager

In the remainder of this chapter we exploit most of the above components to describe an Incident Management integration scenario. In particular, as far as Incident Management is concerned, Tivoli Service Request Manager documents incidents from users, service technicians, and network systems management applications. Streamlining the process further, it leverages ticket types and classifications with powerful visual workflow escalation and e-mail notifications for quicker resolution, helping to meet customer expectations and improve service desk efficiency.

Consolidation of user communication across channels, including phone, e-mail, Web, and fax, captures each incident, creating a searchable knowledge base that can vastly reduce staff response time to anomalies or outages if similar incidents reoccur. Incidents can be linked with appropriate problems or changes, and are associated with their related CIs in the CMDB.

10.3 Lab environment

Figure 10-1 (also shown in Chapter 10, *IBM Service Management Integration Scenarios: TADDM Discovery and compliance check and remediation with TADDM*) represents the lab environment used for the integration scenarios described in this Redbooks publication.



Figure 10-1 Lab environment used for the integration scenarios

The following systems are involved in the Incident Management scenario:

► NC117218:

This system hosts Tivoli Change and Configuration Management Database, Tivoli Provisioning Manager and Tivoli Service Request Manager together with the *Configuration Management DataBase* (*CMDB*), storing all *Configuration Items* (*CIs*) defined in the lab environment, and the Tivoli Provisioning Manager *data center model* (*DCM*), storing the computers that will be the target of the provisioning activities. NC125095:

This system hosts Tivoli Application Dependency Discovery Manager, responsible for discovering all Configuration Items defined in the lab environment and for populating the CMDB, through the IBM Tivoli Integration Composer installed on NC117175, and the Data Center Model, through the "TADDM Discovery" mechanism available in Tivoli Provisioning Manager.

Important: As we show in the remainder of this chapter, a computer discovered by TADDM will be identified by the same Globally Unique Identifier (GUID) in both CMDB and Data Center Model, which will allow the Incident Management scenario to address the same computer both as a Configuration Item in Tivoli Service Request Manager and as a Computer in Tivoli Provisioning Manager.

► NC117175:

This system is responsible, through IBM Tivoli Integration Composer, for populating CMDB with data discovered by Tivoli Application Dependency Discovery Manager.

▶ NC117217:

This system hosts a Windows Gateway used by Tivoli Application Dependency Discovery Manager to discovery Windows targets. In fact, because Tivoli Application Dependency Discovery Manager discovery is based on SSH communication, the Windows Gateway works as a proxy to communicate with Windows systems by connecting through SSH with Tivoli Application Dependency Discovery Manager server and through WMI with the Windows targets. No Windows Gateway is needed to discover UNIX or Linux targets.

NC117177:

This is a Windows system that will be used as target of the Incident Management integration scenario.

10.4 Prerequisites steps for integration

In order for the Incident Management integration scenario to be run, the following preparation steps have been executed after the installation of the involved components:

1. Post-installation tasks for Tivoli Change and Configuration Management database

- 2. Import of Configuration Items from Tivoli Application Dependency Discovery Manager to CMDB as *actual Configuration Items* and promotion to *authorized Configuration Items*
- 3. Import of Computers from Tivoli Application Dependency Discovery Manager to Tivoli Provisioning Manager Data Center Model

Although the detailed description of the above tasks goes beyond the scope of this book, in this section we identify the basic steps that are needed to set up the integration scenario environment. Further detailed information is provided in the official documentation for the involved IBM Tivoli products.

10.4.1 Posts-installation tasks for Tivoli Change and Configuration Management Database

Details about the post-installation task to be run after the installation of Tivoli Change and Configuration Management Database are provided in the publication, *IBM Tivoli Change and Configuration Management Database -Version 7 Release 1.1 - Planning and Installing Guide*, which can be found at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/topic/com.ibm.c cmdb.doc_7.1.1/reference/ccmdb_plan_install.pdf.

In this section we briefly describe the tasks that are needed for the execution of the Incident Management integration scenario.

In order to run the Incident Management integration scenario, you need to create at least one *Organization* and associate a *Site* to it. Creating an organization requires the previous definition of *currency code*, *item*, and *company sets*. Moreover, in order to activate an organization (which is needed to be used in the integration scenario), you need to create a *general ledger account*, which requires the creation of at least one *general ledger account component*. Furthermore, the execution of the Incident Management integration scenario requires the creation of a *default insert site*.

Create currency codes

To define a currency code, complete the following steps:

- 1. Open the Currency Code application by selecting Go To \rightarrow Financial \rightarrow Currency Code.
- 2. Click New Row.
- 3. Enter a currency name; for example, EURO.
- 4. Click the Save icon.

Figure 10-2 shows the result of such steps in the integration scenario environment.

⇔\$ (€⇔	Currency Codes	🕑 Web Replay	Bulletins: (0)	🖗 <u>G</u> o To	IIII <u>R</u> eports	* Start Center	^A <u>P</u> rofile	Sign Out	? <u>H</u> elp	IBM.
Select A	ction 💌 🗟 🖉									
Currer	icy Codes ♥ Filter > 🚜 🚍 ♦ 🐳 ♦ 1 - 1 of 1 ↔				_			E	Downloa	<u>d</u> ? =
	Currency Description						Activ	2		
								₽		
-	EURO						V			î
			Details							
	Currency EURO								Active?	

Figure 10-2 Currency codes definition

Create item and company sets

To define item and company sets, complete the following steps:

- 1. Open the Sets application by selecting Go To \rightarrow Administration \rightarrow Sets.
- 2. Click New Row.
- 3. Enter an item name; for example, IT_ITEMS.
- 4. Enter ITEM in the *Type* field.
- 5. Click New Row.
- 6. Enter a company set name; for example, IT_COMPS.
- 7. Enter COMPANY in the Type field.
- 8. Click the Save icon.

Create an organization

To define an organization, complete the following steps:

- 1. Open the Organizations application by selecting Go To \rightarrow Administration \rightarrow Organizations.
- 2. Click the New Organization icon in the toolbar.
- 3. Enter an organization name in the Organization field, for example, TIVOLI.
- 4. Enter the previously defined base currency in the Base Currency 1 field; for example, EUR0.
- 5. Enter the previously defined item set the *Item Set* field, for example, IT_ITEMS.
- 6. Enter the previously defined company set in the *Company Set* field; for example, IT_COMPS.
- 7. Click the Sites tab.
- 8. Click New Row.
- 9. Enter a site name in the *Site* field; for example, Roma.
- 10. Click the Save icon.

Create a general ledger account component

To create a general ledger account component, complete the following steps:

- 1. Open the Database Configuration application by selecting Go To → System Configuration → Platform Configuration → Database Configuration.
- 2. Select GL Account Configuration from the Select Action drop-down menu.
- 3. Click New Row.
- 4. Enter a component name in the *Component* field; for example, MYCOMPONENT.
- 5. Enter a numeric length for the component; for example, 5.
- 6. Enter a type for the component; for example, ALN.
- 7. Click OK.

Create a general ledger account

To create a general ledger account, complete the following steps:

- 1. Open the Chart of Accounts application by selecting Go To \rightarrow Financial \rightarrow Chart of Accounts.
- 2. Click the name of your organization to select it; for example, click TIVOLI.
- 3. Select **GL Component Maintenance** from the *Select Action* drop-down menu.
- 4. Click New Row.
- 5. Add a *GL Component* value and a description, and then click **OK**; for example, 1234.
- 6. Click New Row.
- 7. Select your General Ledger Account.
- 8. Click Save.

Figure 10-3 shows the result of these steps for the general ledger account.

Chart of Accounts		Web Replay	P <u>B</u> ulletins: (0)	🖗 <u>G</u> o To	IIII <u>R</u> eports	Start Center	¹ Profile	X Sign Out	? <u>H</u> elp	IB.
Select Action	21									
Organizations	2 4 + + 1 - 2 of 2 +							C	Downloa	d ?
Organization	Description								Active	
PMSCIBM	PMSCIBM Inc. North America									
TIVOLI									V	
GL Accounts for TIVOLI	Filter > 🙉 📋 🔶 🐳 🔶 1 - 1 of 1 🌩							0	Downloa	<u>d</u> ?
GL Account =	Description					Type			Active	
🗕 1234 🔎	GL Comp Value								V	ť
			Details							
GL Account 1234	GL Comp Value	1					Туре		1	
Active?									_	
									New	/ Row

Figure 10-3 General Ledger Account

Activate the previously created organization

To activate the previously created organization, complete the following steps:

- 1. Open the Organizations application by selecting Go To \rightarrow Administration \rightarrow Organizations.
- 2. Click the organization name you created, for example, TIVOLI.
- 3. From the *Clearing Account* field, select the General Ledger Account that you just created.
- 4. Select Active.
- 5. Click the Save icon.

Figure 10-4 shows the Organization after its activation. The *Active*? field is flagged.

Crganizations ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐			C Wet	Replay	₽ <u>B</u> ulletins:	(0) 🍖 <u>G</u> o To
Find:		Select Ac	tion 🗸	7	214	🔶 ا 🔿 ا 🔜
List Organization Address	ses Sites					
Organization	TIVOLI					
Base Currency 1	EURO					
Base Currency 2						
ltem Set	IT_ITEMS	и П	tems			
Company Set	IT_COMPS	🖉 П (Comps			
Default Item Status *	PENDING	2				
Clearing Account	1234	9				
Active?						

Figure 10-4 Organization after its activation

Create default insert site

To create a default insert site, complete the following steps:

- 1. Open the Users application by selecting **Go To** \rightarrow **Security** \rightarrow **Users**.
- 2. Search for maxadmin and select it to open the record for user maxadmin.
- 3. Enter the previously created site in the *Default Insert Site* field; for example, Roma.
- 4. Enter the previously created site in the *Storeroom Site for Self-Service Requisitions* field; for example, Roma.
- 5. Click Save.

Figure 10-5 shows the result of the steps for the creation of the Default Insert Site.

ି⇔ୁ Users		C Web Replay	P <u>B</u> ulletins: (0)	🖻 Go To 🔟 Report	is 📫 Start <u>C</u> enter	▲ <u>P</u> rofile × <u>S</u> ign (Dut ? <u>H</u> elp
Find:	Select Action	💌 🚺 🖬	@ 💠 💠		•		
List User Groups Security F	Profile						
User MAXADMIN		Status ACTIVE			Туре 🏾	TYPE 1	
Login Information							
User Name* maxadmin						Set Password	
Personal							
Person * MAXADMIN	Display	Name maxadmin			Address		
Status ACTIVE	Primary P	Phone	\$		City		
First Name	Primary	E-mail			State/Province		
Last Name maxadmin	Workflow Del	legate	1		ZIP/Postal Code		
Supervisor		Memo			Country		
User Settings							
Default Insert Site	ROMA			Us	e Default Insert Site	as a Display Filter?	✓
Storeroom Site for Self-Service Requisitions	ROMA					System Account?	✓
Default Storeroom for Self-Service Requisitions					Can Ac	cess Inactive Sites?	✓
Language	R				Passv	vord Expiration Date	
Locale					U	Ise Screen Reader?	
Time Zone							
Search Language	P						

Figure 10-5 Default Insert Site

Applying changes to the database

When you create organizations, item and company sets, and so on, these configuration changes must be applied to the Maximo database.

Attention: A database backup is highly recommended before applying changes to the Maximo database in order to quickly restore a stable environment in case of failure.

Note: In order to apply changes to the Maximo database, the System Properties *mail.smtp.host* and *mxe.adminEmail* have to be defined, which allows Tivoli Change and Configuration Management database to notify the e-mail address specified in mxe.adminEmail through the SMTP server specified in mail.smtp.host about the results of this step. If the definition of such properties have been skipped during the installation phase, the **Apply Configuration Changes** step will fail with the following error message:

BMXAA4092E - The SMTP Host does not have a property value.

In order to avoid this problem:

- 1. Select Go To \rightarrow System Configuration \rightarrow Platform Configuration \rightarrow System Properties.
- 2. In the **Global Properties** list, find the *mail.smtp.host* and *mxe.adminEmail* properties and provide the IP address or the host name of the SMTP server for the first of them, and the e-mail address of a user to notify of task results for the second of them, as depicted in Figure 10-6 and Figure 10-7. Even fake values can be provided if you do not want to exploit the notification feature; but in any case, you cannot skip this step.

System Properties	🕑 Web Replay Bulletins: (0) 🔗 <u>G</u> o Tr	o 💷 <u>R</u> eports 🌴 S	itart <u>C</u> enter 🔺 <u>P</u> rofile 🗡	Sign Out ? H	eb IBJ
Select Action 💌 🔒 🖉 1 🧐 🦦 🍐					
Global Properties 🗸 Filter 🖓 🚼 🛊 🐳 🔦	1 - 1 of 1 -			E) Dov	wnload 2
Property Name +	Description		Current Value		
smtp					
mail.smtp.host	The name of the SMTP mail server		nc117218.romelab.i	t.ibm.com	Û
	Global Properties Details				
Property Name mail.smtp.host		File Override?	Security Level	SECURE	_ ₽
Description * The name of the SMTP mail	server	Global Only?	User Defined?		
Global Value nc117218.romelab.it.ibm.com	m	Instance Only?	Nulls Allowed?		
Current Value nc117218.romelab.it.ibm.com	m Online Cha	anges Allowed? 🗹	Data Type	ALN	P
Maximo Default		Live Refresh?	Domain		P
		Encrypted?	Masked?		
				6	New Row

Figure 10-6 Definition of mail.smtp.host property

Ð	System Proper	ties	🕞 Web Replay 🛛 🔒 <u>B</u> ulletins: (()) 🎓 <u>G</u> o To 🔟 <u>R</u> eports	Start Center	r 🏝 <u>P</u> rofile 🗙	<u>S</u> ign Out	? <u>H</u> elp	IBM
Select	Action 🗸) 🗟 🖉 🔯 🦦 🍐							
Glob	al Properties 🛛 🔻	Filter > 🚜 📳 💠 🐳 🔤 4-1 - 1 of 1 👳					Dł/	Download	<u>1</u> ? [
	Property Na	ime 🗢	Description			Current Valu	e		
	mxe.admin	mai							-
	- mxe.admint	mail	Clobal Properties De	Maximo system admir		localhost@	it.ibm.com)	
	Description Name	anna adapiaEanail	Global Properties De	The Owner idea		0	escupe	0	
	Property Name		-	File Override?	-	Security Level	SECORE	~	
	Description *	I ne email address of the Maximo system adm	<u> </u>	Global Only?		User Defined?			
	Global Value	localhost@it.ibm.com		Instance Only?		Nulls Allowed?			
	Current Value	localhost@it.ibm.com		Online Changes Allowed?	 Image: A set of the set of the	Data Type	ALN	۹ 🗌	
	Maximo Default			Live Refresh?		Domain		۹ 🗌	
				Encrypted?		Masked?			
								C 1	
								New	ROW

Figure 10-7 Definition of mxe.adminEmail property

To apply configuration changes to the Maximo database, complete the following steps:

- 1. Log in to the Base Service GUI as maxadmin.
- 2. Navigate to Go To \rightarrow System Configuration \rightarrow Platform Configuration \rightarrow Database Configuration.
- 3. On the Select Action drop-down list, select Manage Admin Mode.
- 4. Click **Turn Admin Mode ON**, and then click **OK** when prompted. This task will take several minutes to complete. You can use the **Refresh Status** button to view progress.
- After Admin Mode has been successfully enabled, select Apply Configuration Changes, which will apply the changes to the Maximo database.

Note: When running the Apply Configuration Changes step in our lab environment, we received the following error message showing that the default database heap size for the Maximo database was not large enough to run the commands needed to update the database:

Not enough storage is available in the database heap to process the statement. SQLCODE=-956, SQLSTATE=57011, DRIVER=3.51.90

Because all environments have unique characteristics, such a problem is not necessarily going to occur in other Tivoli Change and Configuration Management Database installations. However, if you do get this message, Figure 10-8 shows you the steps that we ran in order to address the problem.

📾 DB2 CLP - DB2COPY1	
C:\Program Files\IBM\SQLLIB\BIN>set DB2INSTANC	E=CTGINST1
C:\Program Files\IBM\SQLLIB\BIN>db2 connect to Enter current password for db2admin:	maxdb71 user db2admin
Database Connection Information	
Database server = DB2/NT64 9.5.1 SQL authorization ID = DB2ADMIN Local database alias = MAXDB71	
C:\Program Files\IBM\SQLLIB\BIN> db2 get datab Sort heap threes for shared sorts (4KB) (SHEAF Sort list heap (4KB) Database heap (4KB) Utilities heap size (4KB) (UTI SQL statement heap (4KB) Default application heap (4KB) (AB) Statistics heap size (4KB) (STA	ase configuration grep HEAP THRES_SHR> = AUTOMATIC (SORTHEAP) = AUTOMATIC (DBHEAP) = AU906 L_HEAP_SZ) = 10000 (STMTHEAP) = 4096 PPLHEAPSZ) = 8192 T_HEAP_SZ) = 8196
C:\Program Files\IBM\SQLLIB\BIN>db2 update dat 8192 DB200001 The UPDATE DATABASE CONFIGURATION co	abase configuration for MAXDB71 using DBHEAP mmand completed successfully.
C:\Program Files\IBM\SQLLIB\BIN> db2 get datab Sort heap threes for shared sorts (4KB) (SHEAF Sort list heap (4KB) Database heap (4KB) Utilities heap size (4KB) (UTI SQL statement heap (4KB) (A Default application heap (4KB) (A Statistics heap size (4KB) (STA	ase configuration grep HEAP THRES_SHR> = AUTOMATIC (SORTHEAP) = AUTOMATIC (DBHEAP) = AUTOMATIC L.HEAP SZ) = 10000 (STMTHEAP) = 4096 PPLHEAPSZ) = 8192 L.HEAP_SZ) = 8196

Figure 10-8 Changing database heap size in order to run database update

- 6. Log out of the Base Service GUI.
- 7. Open a command prompt on the administrative system and issue the following commands:
 - a. cd c:\IBM\maximo\tools\maximo
 - b. dropbackup.bat
- 8. Restart the MXServer application within WebSphere Application Server.
- 9. Select Go To \rightarrow System Configuration \rightarrow Platform Configuration \rightarrow Database Configuration.
- 10. From the *Select Action* drop-down list, select Manage Admin Mode.
- 11. Click Turn Admin Mode OFF, and then click OK when prompted.

10.4.2 Import of Configuration Items from Tivoli Application Dependency Discovery Manager to CMDB

In order for the Incident Management scenario to be run, at least one Configuration Item has to be defined in the Configuration Management Database. In fact, the Incident Management scenario implies opening an incident associated to a specific Configuration Item, in order to be able to automatically identify it as the target of a resolution action. In particular, in order to open and associate an incident to a Configuration Item in Tivoli Service Request Manager, such a Configuration Item has to be defined as an authorized Configuration Item. In fact, two kinds of Configuration Items are available in CMDB:

- Actual Configuration Items, representing the actual state of a Configuration Item according to the results of its configuration discovery performed by Tivoli Application Dependency Discovery Manager or other discovery tools.
- Authorized Configuration Items, also referred as Configuration Items, representing the authorized or desired state for a specific Configuration Item. In IBM Tivoli Change and Configuration Management Database, a reconciliation process between actual and authorized Configuration Items allows identifying the ones whose actual state does not comply with the desired state. Authorized Configuration Items can be defined a priori (manually in the Base Services GUI or through integration with external tools) or by promotion of actual Configuration Items, if their actual state is identified as the desired one and any future change to it has to be detected.

Important: Even if authorized Configuration Items can be defined manually, the Incident Management scenario described in this chapter will exploit a Configuration Item discovered in TADDM, imported in CMDB as an actual Configuration Item, and finally promoted to an authorized Configuration Item. Such a choice (together with the import of the same Configuration Item as a Computer from Tivoli Application Dependency Discovery Manager to Tivoli Provisioning Manager) will allow automatically identifying the Configuration Item asgociated to the incident in Tivoli Service Request Manager and the target of the resolution action in Tivoli Provisioning Manager as the same computer, by means of its GUID.

In the remainder of this section we describe the import of actual Configuration Items into CMDB and their promotion to authorized Configuration Items.

Import of actual Configuration Items into CMDB

In this section we briefly describe the steps that we performed to import actual Configuration Items from Tivoli Application Dependency Discovery Manager to CMDB by IBM Tivoli Integration Composer. Detailed information about such tasks is provided in *Tivoli Change and Configuration Management Database -Version 7 Release 1.1 - Integration Adapter for Tivoli Application Dependency Discovery Manager Implementation Guide*, which can be located at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/index.jsp?topic =/com.ibm.ccmdb.doc_7.1.1/ccmdb_welcome.htm The steps described next assume that:

- IBM Tivoli Integration Composer, including files for Tivoli Application Dependency Discovery Manager, has been installed on the IBM Tivoli Integration Composer server (this is done by extracting ITIC71WithTADDMAdapters-Win32.zip and running setup.exe).
- The Configuration Management DataBase is based on DB2.
- Configuration Items have been discovered and are available in Tivoli Application Dependency Discovery Manager database.

Here we describe the steps to import actual Configuration Items (also referred to as CIs in remainder of this section) from Tivoli Application Dependency Discovery Manager to CMDB:

1. Create a top level actual Configuration Items class.

In Base Services GUI, select **Go To** \rightarrow **Administration** \rightarrow **Classifications**. In the **Classification** application, create a new classification called *TOPCICLASS*. This will be the root classification for all the Configuration Item classes imported from Tivoli Application Dependency Discovery Manager.

On the Tivoli Change and Configuration Management Database server, open a DB2 command window and execute the following commands:

- a. set DB2INSTANCE=ctginst1
- b. db2 connect to maxdb71 user maximo using <maximo password>
- c. db2 update maxvars set varvalue=(select classstructureid from classstructure where classificationid='TOPCICLASS') where varname='CICLASS'
- d. db2 commit

Figure 10-9 shows the resulting TOPCICLASS in Base Services GUI.

Classifications			Web Replay	P <u>B</u> ulletins: (0)	🖗 <u>G</u> o To 🔟 <u>R</u>	eports 🌴 Start <u>C</u> ent	ter 🌲 <u>P</u> rofile 🎽 <u>S</u> ig	n Out ? <u>H</u>elp	IBM.
Fir	nd: 🚺 🔻	Select Action	V 🐌 🔒) 🧶 💠 🇅		3			
List Classifications									
Classification Classification Path Parent Classification Generate Description?	TOPCICLASS TOPCICLASS	₽	Top class fo Top class fo	r Actual Cis r Actual Cis			Organization Site Owner Group Service Group Indicated Priority Use Classification?		2 2 2 2
Use With > Filter > (%)	⊒ ∳ ∳ ⇔1 - 1 of 1 ↔	Description					Top Level	Download	? =
- ACTCI	P	Use with Actual (Configuration	Items				ĺ	Û
Use With Top	Object ACTCI	Use with Actual Cor	figuration Items	5				New Rot	~
Children > Filter > M	🗀 🔶 🍦 🛶 1 - 5 of 468 🥧							Download	2 =
Classification APP.J2EE.JBOSS.JBOS	SSERVER	Classification Desc		Ger	nerate Description	Use Classification	Organization	<u>Site</u>	
APP.SOFTWAREIMAGE	1							£	
APP.PACKAGEDAPP.M	YSAP.BASIS.MYSAPJ2 🍠						<u></u>	ş	
SYS.HPC.CM.CONFIGU	RATIONMANAGEMENTN 🎤						P	۶	
APP.DB.MSSQL.SQLSE	RVER 🏓						Q.	New Roy	
Attributes : > Filter > #								Dewnload	? : =
Attribute	Description	Section	Dom	nain	Data Type	Unit c	of Measure	223111222	
			No rov	ws to display				New Roy	w •

Figure 10-9 Top level actual Configuration Items class

- 2. Copy the needed files into the proper directories.
 - a. On the IBM Tivoli Integration Composer server, copy *.schm files (from extracted zip) to C:\Integration Composer\data\dataschema and *.fsn files to C:\IntegrationComposer\data\mappings.
 - b. Copy *.db2 files from the IBM Tivoli Integration Composer server to a temporary directory on the Tivoli Change and Configuration Management Database server.
 - c. Copy *db2 files from the IBM Tivoli Integration Composer server to a temporary directory on the Tivoli Change and Configuration Management Database server.
- 3. Create the CI type data schema for the TADDM data source.

On the Tivoli Change and Configuration Management Database server, in the same DB2 command window, that was used in step #1, enter:

- a. db2 -tvf createTADDM71CITypeDataSchema.db2
- b. db2 commit

- 4. Create a data source connection for TADDM CI type data.
 - a. Sign in to the Integration Composer application using a valid user ID and password.
 - b. Select Define New Data Source.
 - c. Select the TADDM CI Type data schema and click Next.
 - d. In the *Data Source* field, type a name for the data source, for instance, TADDM-71x-CI-Types, and click **Next**.
 - e. In the *Connection Method* drop-down list select the **IBM Configuration Discovery and Tracking API** method.
 - f. Type in the connection parameters required for the API connection to Tivoli Application Dependency Discovery Manager. The values that were provided for the integration scenario environment are:
 - Connection Method: IBM Configuration Discovery and Tracking API
 - Host Name: nc125095.romelab.it.ibm.com
 - Host Port: 9530
 - User Name: administrator
 - Password: collation
 - g. Select **Test Connection** and click **Finish** if the test is successful. Otherwise, check your connection parameters.
- 5. Create a data schema for CCMDB CI type data.
 - a. Sign in to the Integration Composer application using a valid user ID and password.
 - b. Select Define New Data Schema.
 - c. In the *Data Schema* field, type CCMDB71Classification as the name of the new data schema (you can choose a different name, but in this case, you have to change it in qualifierCCMDB71Classification.db2). Click **Next**.
 - d. In the *Data Source* field, type the name that you want to use to identify the data source, for example, CCMDB71x-Classification, and click **Next**.
 - e. In the *Connection Method* drop-down list, select **IBM DB2 JDBC Driver**.
 - f. Type in the connection parameters required for the JDBC[™] connection to the CMDB. The values that were provided for the integration scenario environment are:
 - Hostname: nc117218.romelab.it.ibm.com (Maximo database server)
 - Host Port: 50005
 - Database: maxdb71
 - Username: maximo
 - Password: password (maximo user's password in the lab environment)
 - Table owner: maximo

- g. Select **Test Connection** and click **Finish** if the test is successful. Otherwise check your connection parameters.
- h. From the *Select Action* menu in the title bar of the Data Schema window, select **Import Data Schema**.
- i. Select: CCMDB71Classification.schm and click Open.
- j. Select **Synchronize** and then click **OK.** Select **Save** from the *Select Action* menu.

Note: Although official documentation refers to the **Synchronize** button as **Fix Errors**, its name has been changed to **Synchronize** in Tivoli Base Services 7.1.1 fix pack 4.

6. Load the class qualifiers into the target CI type data schema.

On the Tivoli Change and Configuration Management Database server, in the same DB2 command window, that was used in step #1, enter:

```
a. db2 -tvf qualifierCCMDB71Classification.db2
```

- b. db2 commit
- 7. Create a mapping for CI type data.
 - a. Sign in to the Integration Composer application using a valid user ID and password.
 - b. Select Create new mapping.
 - c. From the *Source* drop-down list, select the TADDM data source.
 - d. From the *Target* drop-down list, select the CCMDB data source.
 - e. In the *Mapping Name* field, type a new mapping name, for instance, taddm-2-ccmdb-citypes.
 - f. Click **OK**. The Integration Composer opens the Mapping window.
- 8. Import mapping file CI type data.
 - a. From the *Select Action* menu in the Integration Composer Mapping window, select **Import**.
 - b. Select the mapping file, **TADDM71CITypeToCCMDB71Classification.fsn**, and click **Open** to import the mapping file.
 - c. Select **Save** from the *Select Action* menu.
- 9. Execute mapping for CI type data.
 - a. Close Integration Composer, if running.
 - b. Go to the bin subdirectory in your Integration Composer installation directory.

c. Enter the following command:

commandLine <mappingName> <repositoryUser> <repositoryPwd>
<sourceUser> <sourcePwd> <targetUser> <targetPwd>

In the lab environment case, this became:

commandLine taddm-2-ccmdb-citypes maximo password administrator
collation maximo password

- 10. Activate CI Types.
 - a. Log into Base Services GUI.
 - b. Select Go To \rightarrow Administration \rightarrow Cl Types.
 - c. Find SYS.COMPUTERSYSTEM.
 - d. Change status to active, using the change status icon.
- 11.Create a data source connection for TADDM Actual CI data.
 - a. Sign in to the Integration Composer application using a valid user ID and password.
 - b. Select Define New Data Source.
 - c. Select the TADDM Actual CI data schema and click Next.
 - d. In the *Data Source* field, type a name for the data source, for instance, TADDMActualCI, and click **Next**.
 - e. In the *Connection Method* drop-down list, select the **IBM Configuration Discovery and Tracking API** method.
 - f. Type in the connection parameters required for the API connection to Tivoli Application Dependency Discovery Manager. The values that were provided for the integration scenario environment are:
 - Connection Method: IBM Configuration Discovery and Tracking API
 - Host Name: nc125095.romelab.it.ibm.com
 - Host Port: 9530
 - User Name: administrator
 - Password: collation
 - g. Select **Test Connection** and click **Finish** if the test is successful. Otherwise, check your connection parameters.

12. Create a data schema for CCMDB Actual CI data.

- a. Sign in to the Integration Composer application using a valid user ID and password.
- b. Select Define New Data Schema.
- c. In the *Data Schema* field, type CCMDB71ActualCI as the name of the new data schema (you can choose a different name, but in this case, you have to change it in qualifierCCMDB71ActualCI.db2) and click **Next**.
- d. In the *Data Source* field, type the name that you want to use to identify the data source, for example, CCMDB71x-ActualCI, and click **Next**.
- e. In the Connection Method drop-down list, select IBM DB2 JDBC Driver.
- f. Type in the connection parameters required for the JDBC connection to the CMDB. The values that were provided for the integration scenario environment are:
 - Hostname: nc117218.romelab.it.ibm.com (Maximo database server)
 - Host Port: 50005
 - Database: maxdb71
 - Username: maximo
 - Password: password (maximo user's password in the lab environment)
 - Table owner: maximo
- g. Select **Test Connection** and click **Finish** if the test is successful. Otherwise, check your connection parameters.
- h. From the *Select Action* menu in the title bar of the Data Schema window, select **Import Data Schema**.
- i. Select: CCMDB71ActualCl.schm and click Open.
- j. Select **Synchronize** and then click **OK**. Select **Save** from the *Select Action* menu.

Note: Although official documentation refers to the **Synchronize** button as **Fix Errors**, its name has been changed to **Synchronize** in Tivoli Base Services 7.1.1 fix pack 4.

13. Load the class qualifiers into the target Actual CI data schema.

On the Tivoli Change and Configuration Management Database server, in the same DB2 command window that was used in step #1, enter:

db2 -tvf qualifierCCMDB71ActualCI.db2

db2 commit

14. Create a mapping for CI type data.

- a. Sign in to the Integration Composer application using a valid user ID and password.
- b. Select Create new mapping.
- c. From the *Source* drop-down list, select the TADDM data source.
- d. From the *Target* drop-down list, select the CCMDB data source.
- e. In the *Mapping Name* field, type a new mapping name, for instance, taddm-2-ccmdb-actualci.
- f. Click OK. The Integration Composer opens the Mapping window.

15.Import mapping file CI type data.

- a. From the *Select Action* menu in the Integration Composer Mapping window, select **Import**.
- b. Select the mapping file, **TADDM71CITypeToCCMDB71ActualCI.fsn**, and click **Open** to import the mapping file.
- c. Select Save from the Select Action menu.

16. Execute mapping for CI type data.

- a. Close Integration Composer, if running.
- b. Go to the bin subdirectory in your Integration Composer installation directory.
- c. Enter the following command:

commandLine <mappingName> <repositoryUser> <repositoryPwd>
<sourceUser> <sourcePwd> <targetUser> <targetPwd>

In our lab environment, we entered:

commandLine taddm-2-ccmdb-actualci maximo password administrator
collation maximo password

Actual Configuration Items should now be displayed in the Base Services GUI and can be accessed by selecting Go To \rightarrow IT infrastructure \rightarrow Actual Configuration Items.

Figure 10-10 shows the integration scenario's Configuration Items in Tivoli Application Dependency Discovery Manager console before their import in CMDB.

Figure 10-11 shows the same Configuration Items after their import as actual Configuration Items.

ETivoli Application Dependency Discovery Manager	- Version: Current			
File Edit Display Discovery Topology Analytics Wi	ndows <u>H</u> elp			
< > 🗈 🖿 🔚 🔛 🗞 🜒 🍇	₽= ♀=			
Discovery	Overview			
A	Discovery Information			
	Status:	Idle		
Overview	Components Found:	0		
	Sensors Running:	0		
¥3	Progress:			
Scope	Show only items of status:	All status lev 💌		
Topology		Sensor	Host Name/IP	
Analytics				
Discovered Components				
List/Search				
Keyword:				
Component: Windows Computer System	•			
nc117175.romelab.it.ibm.com	Information:	To view information about the se	nsor, select a row.	<u> </u>
nc117177.romelab.it.ibm.com				-
nc117217.romelab.it.ibm.com				
nc117218.romelab.it.ibm.com	Run Discovery S	cope Details Discovery Lo	g	
nc125095.romelab.it.ibm.com	Details			7 7 ×
		Username: a	dministrator Server: nc1	25095:9433

Figure 10-10 Computer Configuration Items in TADDM console

Actual Configuration Items	C Web Replay	Bulletins: (0)	☆ <u>G</u> o To <u>Int</u> <u>R</u> eports	Start Center	A Profile	<mark>≭ S</mark> ign Out	? <u>H</u> elp	IBM.
Find:	Select Action		🔶 🔶 🛃 🔗					
List Actual Configuration Item	Related Actual Cls Operati	onal Management I	Products					
🕅 Advanced Search 🔻 🗟 Save Query 🔻	A Bookmarks							
Actual Configuration Items 🕴 🔻 Filter > 🏟	👔 🛊 🐳 🖕 1 - 5 of 5 🐟					E4	Download	? =
Actual CI	Description		Cl	assification				
			c	mputer				
NC117175.ROMELAB.IT.IBM.COM~2			SY	S.WINDOWS.WIN	DOWSCON	IPUTERSYSTE	EM	↔
NC117218.ROMELAB.IT.IBM.COM~117			SI	S.WINDOWS.WIN	DOWSCOM	PUTERSYSTE	М	A
NC125095.ROMELAB.IT.IBM.COM~230			SI	S.WINDOWS.WIN	DOWSCOM	PUTERSYSTE	М	
NC117217.ROMELAB.IT.IBM.COM~341			SI	S.WINDOWS.WIN	DOWSCOM	PUTERSYSTE	М	<
NC117177.ROMELAB.IT.IBM.COM~457			SI	S.WINDOWS.WIN	DOWSCOM	PUTERSYSTE	M	
Select Records								

Figure 10-11 Actual Configuration Items in Base Services GUI

Promotion of actual Configuration Items

In order for the Incident Management process to manage an incident related to a specific Configuration Item, the Configuration Item has to be defined in CMDB as an authorized Configuration Item. Moreover, in order for the Incident Management integration scenario to work, the Authorized Configuration Item (that could be also defined manually) has to be created by promoting the corresponding actual Configuration Item, which will allow Tivoli Provisioning Manager to automatically identify the target of the resolution activity.

In order to promote an actual Configuration Item, select **Create Authorized Configuration Item** from the *Select Action* drop-down menu as shown in Figure 10-12.

Actual Configuration Items		🕑 Web Replay 🔰	Bulletins: (0) 🍖 Go To 🛄 Reports	✿ Start <u>C</u> enter ▲ <u>P</u> rofik	e [×] <u>S</u> ign Out ? ∣	Help IEM,
Find. Find.	Solect Action Image: Constraint of the solect		GUD Last Scan Date	2A978E3C949134DE8D 2009-07-28 04:36:02	B22A7D515D441D	
Configuration Item NC117177.ROMELAB.IT.IBM.0	COM~ Run Reports		Last Modified Date	2009-07-28 04:36:02		
Specifications > Filter > 24 10 1 4 4 4 1 - 10	0 of 19 🦗				^B / <u>D</u>	ownload 🦙 😑
Attribute	Description	Data Type	Alphanumeric Value	Numeric Value	Unit of Measure	Table Value
COMPUTERSYSTEM_MEMORYSIZE	COMPUTERSYSTEM_MEMORYSIZE	NUMERIC		8,320,450,560.0		
COMPUTERSYSTEM_TYPE	COMPUTERSYSTEM_TYPE	ALN	ComputerSystem	0.000000000		
COMPUTERSYSTEM_FQDN	COMPUTERSYSTEM_FQDN	ALN	nc117177.romelab.it.ibm.com	0.000000000		
COMPUTERSYSTEM_MANUFACTURER	COMPUTERSYSTEM_MANUFACTURER	ALN	VMware, Inc.	0.000000000		
COMPUTERSYSTEM_SIGNATURE	COMPUTERSYSTEM_SIGNATURE	ALN	9.168.117.177(000C295A0C0A)	0.000000000		
COMPUTERSYSTEM_ARCHITECTURE	COMPUTERSYSTEM_ARCHITECTURE	ALN	Intel	0.000000000		
MODELOBJECT_CONTEXTIP	MODELOBJECT_CONTEXTIP	ALN	9.168.117.177	0.000000000		
COMPUTERSYSTEM_MODEL	COMPUTERSYSTEM_MODEL	ALN	VMware Virtual Platform	0.000000000		
MODELOBJECT_CREATEDBY	MODELOBJECT_CREATEDBY	ALN	system	0.000000000		
MODELOBJECT_DISPLAYNAME	MODELOBJECT_DISPLAYNAME	ALN	nc117177.romelab.it.ibm.com	0.0000000000		

Figure 10-12 Promotion of a Configuration Item from Actual to Authorized

By defining the TOPCICLASS as in Figure 10-9 on page 288, actual CIs are created in a hierarchy that follows the Tivoli Common Data Model. One might have chosen to import only some types of CIs or to limit the number of levels of child CIs that are imported. Similarly, it is possible to limit the CIs and the attributes that are included in authorized CIs.

In order to control which CI types and attributes are included in authorized CIs, one can build a hierarchy of authorized CI classifications that mirrors the hierarchy of actual CIs, but contains only those CIs and attributes that one wants to manage. The description of the steps to create an authorized Configuration Items hierarchy goes beyond the scope of this book. Detailed information about such steps is provided in *IBM Tivoli Change and Configuration Management Database - Version 7 Release 1.1* official documentation, which can be accessed at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/index.jsp?topic =/com.ibm.ccmdb.doc 7.1.1/ccmdb welcome.htm

As shown in Figure 10-13, a simple hierarchy has been created in the lab environment; the authorized Configuration Item Top Class CI.TOPCICLASS has been assigned three children in order to be able to represent Windows computers in terms of computer attributes, operating system attributes, and software components attributes. For the purposes of the Incident Management scenario, the class CI.SYS.WINDOWS.WINDOWSCOMPUTERSYSTEM (mapping the actual Configuration Items class SYS.WINDOWS.WINDOWSCOMPUTERSYSTEM), which allows representing Windows computers as authorized Configuration Items and associating them to Tivoli Service Request Manager Incidents, is enough.

Classifications		C Web Replay	P <u>B</u> ulletins: (0) 🌈 <u>G</u> o To 🕮 <u>R</u> eș	oorts 📫 Start <u>C</u> ente	r 🌲 <u>P</u> rofile 🎽 <u>S</u> ign (Out ? <u>H</u> elp	IBM.
Fir	nd: 🕅 🧖	Select Action 💌 谢 🔒	🧶 🔶 🕴	🖌 i 🖳 i 🛃 i 🤗				
List Classifications								
	-							
Classification	CI.TOPCICLASS	<u>م</u>				Organization		P
Classification Path	CI.TOPCICLASS					Site		P
Parent Classification		1				Owner Group		₽
Generate Description?	\checkmark					Service Group		P
						Indicated Priority		
						Use Classification?		
Use With ↓ 🌢 Filter > 🖧 🕴	🗐 🔶 🐳 🔶 1 - 1 of 1 🔶						Download	? =
Use With Object		Description				Top Level		
CI	2	Use with Configuration	Items					Û
			Details					
Use With Top	h Object Cl P D Level?	Use with Configuration Items						
							New	Row
Children 🕨 Filter > 🙌 🚦	🗐 🔺 🍦 🐳 1 - 3 of 3 🐳						Download	? =
Classification		Classification Desc	<u>(</u>	Generate Description	Use Classification	Organization	Site	
CI.SYS.SOFTWARECOM	MPONENT 🎤	SYS.SOFTWARECOMPONENT		3		P		۵ 🔎
CLSYS.WINDOWS.WIND	DOWSOPERATINGSYS1 🎤	SYS.WINDOWS.WINDOWSOPERATI	NGSYSTEI [٩		Р 🗊
CLSYS.WINDOWS.WIND	DOWSCOMPUTERSYST 🎤	SYS.WINDOWS.WINDOWSCOMPUTE	ERSYSTEN [P		Р 🗊
							New	Row
Attributes > Filter > 👸	12 4 4 44						Download	2 =
Attribute	Description	Section Do	omain	Data Type	Unit	of Measure		
		No n	ows to display					
							New	Row

Figure 10-13 Top level authorized Configuration Items class

After promotion, authorized Configuration Items can be accessed by selecting Go To \rightarrow IT infrastructure \rightarrow Configuration Items.

Figure 10-14 shows the result of promoting to authorized Configuration Items, the actual Configuration Items represented in Figure 10-11.

Configuration Items	🕞 Web R	eplay 🤑 <u>B</u> ulletins: (0)	<u> <u> </u></u>	* Start <u>C</u> enter ² Pr	ofile XSign Out ? <u>H</u> elp]	IBN
Find:	🔥 🔝 Select Actio	n 🔽 🚺 🔒	⊘ ♦ ♦ ∰	1 🔮 🔋	1122	
List Configuration Item	Related Cls					
🕅 Advanced Search 🔻 🗟 Save	Query 🔻 🛷 Bookmarks					
Configuration Items 🕴 🔻 Filter 🧃	🌇 🎦 🛧 🤞 🔶 1 -5 of 5 🔿				E ¹ Download	?
Configuration Item	Description		Status	Classification		
	P			computer		
C117175.ROMELAB.IT.IBM.COM~	2		NOT READY	CI.SYS.WINDOWS.	WINDOWSCOMPUTERSYSTEM	1 4
NC117218.ROMELAB.IT.IBM.COM~11	7		NOT READY	CLSYS.WINDOWS.	WINDOWSCOMPUTERSYSTEM	Ş
NC125095.ROMELAB.IT.IBM.COM~23	0		NOT READY	CLSYS.WINDOWS.	WINDOWSCOMPUTERSYSTEM	4
NC117217.ROMELAB.IT.IBM.COM~34	1		NOT READY	CLSYS.WINDOWS.	WINDOWSCOMPUTERSYSTEM	4
NC117177.ROMELAB.IT.IBM.COM~45	7		NOT READY	CLSYS.WINDOWS.	WINDOWSCOMPUTERSYSTEM	é
Select Records						

Figure 10-14 Authorized Configuration Items in Base Services GUI

10.4.3 Import of Computers from Tivoli Application Dependency Discovery Manager to Tivoli Provisioning Manager Data Center Model

The import into Tivoli Provisioning Manager Data Center Model of computers discovered in Tivoli Application Dependency Discovery Manager can be performed by running the TADDM Discovery method in Tivoli Provisioning Manager console. The detailed steps to configure and run such tasks are described in *Chapter 8, "IBM Service Management integration scenarios: TADDM Discovery" on page 195.*

Figure 10-15 shows the TADDM Discovery method panel in Tivoli Provisioning Manager console.

Contraction Contraction Contraction	nfigurations					🕞 Web Replay	♥ <u>B</u> ulletins: (0)	<i>е</i> <u>G</u> o To	🔟 <u>R</u> eports	Start Center	* Profile	X Sign Out	? Help	IBM.
	Y Find: Sele	ect Action 🛛 🔽 🎦	🗟 🧶 ا 🌲	~										
List Discover	У													
Disco	very Configuration My TADDM Discovery Method TADDM Discovery	M	Discovers be	oth hardware and software	e resou		Category	Hardware	and Software D	liscovery				
Discovery Paramete	ors													
Server Information	Computer to be Discovered	Scope												
Server Informatio	n													-
Name	nc125095.romelab.it.ibm.com				Port number	9530								
User Id	administrator				Password	•••••								
												R	un Discov	very

Figure 10-15 TADDM Discovery in Tivoli Provisioning Manager console

After importing computers in the Tivoli Provisioning Manager Data Center Model, you can access them by selecting **Go To** \rightarrow **Deployment** \rightarrow **Provisioning Computers**.

Figure 10-16, Figure 10-17, and Figure 10-18 show the representation of computer nc117177 respectively in actual Configuration Items, authorized Configuration Items, and Provisioning Computers. The red circles highlight the fact that the GUID in Figure 10-16, the Provisioning Object in Figure 10-17, and the Globally Unique Identifier in Figure 10-18 are all the same, which allows Tivoli Service Request Manager and Tivoli Provisioning Manager to recognize the Configuration Item associated to an incident as the same computer defined in Tivoli Provisioning Manager.

	Actual Configuration Items		Web Replay	■ <u>B</u> ulletins: (0)	🕈 Start <u>C</u> enter 🏾 🔺 <u>P</u> rofi	le 🔺 <u>S</u> ign Out	
	Find:	💌 Select Action 💌 🖃 🧶 💠 💠	🛃 🚔				
List Actual Configuration tem Related Actual Cls Operational Management Products							
	Actual CI NC117177.ROMELAB.IT.IBM.C Classification TOPCICLASS \ SYS.WINDOW Configuration Item NC117177.ROMELAB.IT.IBM.C	COM~457 S.WINDOWSCOM COM~457		GUID Last Scan Date Last Modified Date	2A978E3C949134DE80 2009-07-28 04:36:02 2009-07-28 04:36:02	DB22A7D515D441	
Sp	ecifications ≽ Filter > 🖄 🗊 🛧 🔌 🔶 1 - 10) of 19 🧄				Dł/	Download ? 🚍
Þ	Attribute COMPUTERSYSTEM_MEMORYSIZE	Description COMPUTERSYSTEM_MEMORYSIZE	Data Type NUMERIC	Alphanumeric Value	Numeric Value 8,320,450,560.0	Unit of Measure	Table Value
•	COMPUTERSYSTEM_TYPE	COMPUTERSYSTEM_TYPE	ALN	ComputerSystem	0.000000000		
•	COMPUTERSYSTEM_FQDN	COMPUTERSYSTEM_FQDN	ALN	nc117177.romelab.it.ibm.com	0.000000000		
•	COMPUTERSYSTEM_MANUFACTURER	COMPUTERSYSTEM_MANUFACTURER	ALN	VMware, Inc.	0.000000000		
•	COMPUTERSYSTEM_SIGNATURE	COMPUTERSYSTEM_SIGNATURE	ALN	9.168.117.177(000C295A0C0A)	0.000000000		
•	COMPUTERSYSTEM_ARCHITECTURE	COMPUTERSYSTEM_ARCHITECTURE	ALN	Intel	0.000000000		
•	MODELOBJECT_CONTEXTIP	MODELOBJECT_CONTEXTIP	ALN	9.168.117.177	0.000000000		
•	COMPUTERSYSTEM_MODEL	COMPUTERSYSTEM_MODEL	ALN	VMware Virtual Platform	0.000000000		
•	MODELOBJECT_CREATEDBY	MODELOBJECT_CREATEDBY	ALN	system	0.000000000		
		HODELOBIEST DISPLANNAME			0.000000000		

Figure 10-16 Target computer represented as actual Configuration Item
Configuration Items			•	Web Replay 🦊 Bulletins: (0) 🌈 🤆	o To 🔟 <u>R</u> eports 🗚	Start <u>C</u> enter ⁴ Profile	<mark>≭ <u>S</u>ign Out</mark>	^{? Help} IRM.
✓ Find	i: di t	🗸 🗢 Select Action 🛛 🖌 🛃 🥒 I	💠 🔶 🛟	I 🛃 I 🔗 🕕				
List Configuration Ite	m Related Cls							
Configuration Item	NC117177.ROMELAB.	T.IBM.COM~457				Attachment	s @	
Classification	CLTOPCICLASS \ CLS	YS.WINDOWS.WINDOWS				Statu	NOT REA	DY
Class Description	SYS.WINDOWS.WIND	OWSCOMPUTERSYSTEM P				CI Locatio	n	-
Asset						Sit	e .	
Location	1					Organizatio	n	
Item	1					Item Se	et	P
Service	P					Calenda	ır 🗌	
Service Group	1					Shi	ft	P
Actual CI	NC117177.ROMELAB.	T.IBM.COM~457				CI Owne	er 🗌	1
Provisioning Object	2A978E3C949134DE8	DB22A7D515D441D / nc117177.romelab.	it.ibm.com			Change Window	v	2
						Change Numbe	er 🗌	1
					_			
Specifications > Filter > #	1 [2] 수 🔶 🧇 1 - 1	0 of 35 🦀					Lø	Download ? =
Attribute		Description	Data Type	Alphanumeric Value		Numeric Value Unit of M	easure	Section
MODELOBJECT_DISPLAY	(NAME	P MODELOBJECT_DISPLAYNAME	ALN	nc117177.romelab.it.ibm.com	₽ _	P	P	
MODELOBJECT_DESCRIP	TION 🥻	MODELOBJECT_DESCRIPTION	ALN		2	2	2	
MODELOBJECT_CONTEXT	TIP 🧳	MODELOBJECT_CONTEXTIP	ALN	9.168.117.177	<i>P</i>	2	P	Û
MODELOBJECT_LABEL	1	MODELOBJECT_LABEL	ALN		2	2	₽	Û
COMPUTERSYSTEM_BOO	OTORDER 🖌	COMPUTERSYSTEM_BOOTORDER	ALN		P	2	₽	Û
COMPUTERSYSTEM_NAM	AE 🏅	COMPUTERSYSTEM_NAME	ALN	NC117177	₽	2	2	Û
COMPUTERSYSTEM_TYP	e j	COMPUTERSYSTEM_TYPE	ALN	ComputerSystem	2	2	2	Û
COMPUTERSYSTEM_SYS	STEMID 🥻	COMPUTERSYSTEM_SYSTEMID	ALN	NC117177.00:0C:29:5A:0C:0A	9	2	2	Û
COMPUTERSYSTEM_SYS	STEMBOARDUUID 🔰	COMPUTERSYSTEM_SYSTEMBOARDUUD	ALN		P	<u>_</u>	۶	Û
COMPUTERSYSTEM_PRIN	MARYMACADDRESS	COMPUTERSYSTEM_PRIMARYMACADDRESS	ALN		2	<u>_</u>	،	Û
								New Row

Figure 10-17 Target computer represented as authorized Configuration Item



Figure 10-18 Target computer represented as Provisioning Computer

10.5 Incident Management integration scenario

In this section we describe a very simple Incident Management scenario that exploits the integration capabilities of Tivoli Service Request Manager and Tivoli Provisioning Manager. Depending on the Incident Management process in place in your organization, more complex scenarios can be envisaged.

In particular, this section describes the following actions:

- The process flow of the Incident Management scenario
- The steps needed to create and configure the users that have been used to run the different stages of the scenario
- The steps needed to create and configure the Tivoli Services Request Manager and Tivoli Provisioning Manager components used to run the scenario
- The detailed scenario's implementation steps

10.5.1 Process flow

Figure 10-19 shows the process flow for the Incident Management integration scenario.



Figure 10-19 Incident Management scenario's process flow

The scenario includes the following steps:

- 1. An end user opens a *Service Request* through the Tivoli Service Request Manager Self Service console in order to highlight a performance degradation that they are experiencing with the intranet Web site.
- 2. A Help Desk operator opens an *Incident* to address the Service Request and takes ownership of it. Then the operator contacts the end user to collect further information. Finally the operator understands that they are not able to address the issue and forwards the incident to an Incident Analyst.
- 3. The Incident Analyst applies an *Incident Template* that is suitable for the issue. As a consequence of the template application, incident fields are updated with further information and an *Activity* that should be executed to address the issue (emergency restart of the HTTP server) is automatically associated to the incident. Moreover the incident is forwarded to a Deployment Specialist that is responsible to run the resolution activity.
- 4. The Deployment Specialist uses the *Start Assisted Workflow* option to run a *Provisioning Task* that restarts the HTTP server. After the successful execution of the provisioning task, they route the incident back to the Help Desk operator.
- 5. The Help Desk operator verifies that the original issue has been addressed and finally closes the incident.

10.5.2 Creation and configuration of users needed to run the Incident Management integration scenario

The previously described scenario implies the availability of a different user profile for each step.

The following users have been involved:

► SRMSELFSERVICEUSR:

This is the default self service user in Tivoli Service Request Manager, member of the SRMSELFSERVICE group. It maps the end user in the incident management scenario.

PMINCOWNUSR:

This is the default incident owner user in Tivoli Service Request Manager, member of the PMINCOWN group. It maps the help desk user in the incident management scenario. ► PMINCANALUSR:

This is the default incident analyst user in Tivoli Service Request Manager, member of the PMINCANAL group. It maps the incident analyst user in the incident management scenario.

► GIOVANNIB:

This is a custom user (defined for this scenario), member of the TPDEPLOYMENTSPECIALIST group. It maps the deployment specialist user in the incident management scenario.

As depicted in Figure 10-20, these users (highlighted by red circles) are defined in WebSphere console by selecting **Users and Group** \rightarrow **Manage Users**. Assigning them to specific security groups allows defining their authorizations in terms of the actions that they can perform and the data that they can access. The configuration of the security groups can be accessed in the Base Services GUI by selecting **Go To** \rightarrow **Security** \rightarrow **Security Groups.** As an example, Figure 10-21 shows the configuration of group TPDEPLOYMENTSPECIALIST. Every tab in the picture allows defining access to specific resources.

Eile Edit View Favorites Tools Help						1
🔇 Back 🔹 🕥 👻 😰 🏠 🔎 Search 🛭 👷 Favori	tes 🔗	🝰 - 🚴 🗖				
Address 🕘 https://nc117218.romelab.it.ibm.com:9043/ibm	/console/l	ogin.do?action=secure				🗾 🔁 Go 🛛 Links 🏾
Integrated Solutions Console Welcome wasadmin	n					Help Logout
View: All tasks						Select Action 💌
Welcome My Startup Pages	User I		100			
Guided Activities	Sear	ch				
E Servers						
Applications	26 user	s matched the search	criteria.			
Resources	Cm	eate Delete	Select an action.		7	
E Security	Select	User ID	First name	Last name	E-mail	
Environment	Г	wasadmin	wasadmin	wasadmin		cn=wasadmin.ou=users.ou=SWG.o=IBM.c=US
E System administration		myintadm	myintadm	mvintadm		uid=myintadm.ou=users.ou=SWG.o=IBM.c=US
Users and Groups		managan				
Administrative Oser Roles Administrative Group Roles		maxieg		maxieg		
Manage Users		maxadmin	maxadmin	maxadmin		uld=maxadmin,ou=users,ou=swd,o=16m,c=05
- Manage Groups		SRMSELFSERVICEUSR	Self	Service		uid=SRMSELFSERVICEUSR,ou=users,ou=SWG,o=IBM,c=US
El Monitoring and Tuning		PMUSRMGRUSR	PMUSRMGRUSR	PMUSRMGRUSR		uid=PMUSRMGRUSR,ou=users,ou=SWG,o=IBM,c=US
E froubleshooting		PMUSRANALUSR	PMUSRANALUSR	PMUSRANALUSR		uid=PMUSRANALUSR,ou=users,ou=SWG,o=IBM,c=US
		PMUSRADMUSR	PMUSRADMUSR	PMUSRADMUSR		uid=PMUSRADMUSR,ou=users,ou=SWG,o=IBM,c=US
E Settings		PMINCANALUSR	PMINCANALUSR	PMINCANALUSR		uid=PMINCANALUSR,ou=users,ou=SWG,o=IBM,c=US
		PMSCSRUUSR	ServiceRequisition	User		uid=PMSCSRUUSR,ou=users,ou=SWG,o=IBM,c=US
		PMSCSRUMUSR	ServiceRequisition	User		uid=PMSCSRUMUSR,ou=users,ou=SWG,o=IBM,c=US
		PMINCOWNUSR	PMINCOWNUSR	PMINCOWNUSR		uid=PMINCOWNUSR,ou=users,ou=SWG,o=IBM,c=US
		PMSCSDMUSR	Service	Delivery		uid=PMSCSDMUSR,ou=users,ou=SWG,o=IBM,c=US
		PMSCSDGNUSR	Service	Designer		uid=PMSCSDGNUSR,ou=users,ou=SWG,o=IBM,c=US
		GIOVANNIB	Giovanni	Bianchi		uid=GIOVANNIB,ou=users,ou=SWG,o=IBM,c=US
					Go	Tataly 26

Figure 10-20 Incident Management scenario users

ဂုံးဂို Security Groups	• Web Repl	y <mark>₱ B</mark> ulletins: (0) 🏕 <u>G</u> o To 💷 <u>R</u> eports 🌴 Sta	rt <u>C</u> enter [▲] Profile [×] Sign Out ? Help III师。
Find:	🗢 Select Action 📉 🎽 属 🧶 ᡇ 💠 🔍 🍇		
List Group Sites Applications	Storerooms Labor GL Components Limits and Toleran	ces Data Restrictions Users Pro	visioning Permissions
Group TPDEPLOYMEN			
Applications > Filter > 🙈 🗇 + 😝 + 1 - 10 of	199 🥪		🕒 <u>Download</u> ? 📼
		Grant Listed Applications : 🔻	Revoke Listed Applications : 🔻
Description 🗢	Main Object/Table	Original Application (if copied)
Access Control Lists	TPM View Acl		
Actions	Table to hold actions.		
Activities and Tasks	The WOACTIVITY view.		
Actual Configuration Items	Actual CI Table		
Adapter Conversion	Deployed Assets Adapter Conversion Targets		
Application Designer	The MAXAPPS Table		
Application Tiers	TPM View Cluster		
Asset Link Results	Asset Link Result view.		
Asset Reconciliation Results	Asset Result of Link and/or Comparison		
Assets	The ASSET Table		
Options for Access Control Lists > Filter > #	🗇 🛧 🦆 🐟 1 - 4 of 4 🐟		🖾 Download ? 📼
			Grant Listed Options for This Application
Description 🗢	Grant Access	Condition	
Delete ACL		1	
New ACL			
Read Access to TPACL		1	
Save ACL		8	

Figure 10-21 TPDEPLOYMENTSPECIALIST security group

10.5.3 Creation of components needed for the execution of the Incident Management integration scenario

In order for the scenario described to be run, the following objects have to be created in advance:

An incident template:

An *incident template* contains predefined data that you can insert in common, high-volume incident records. An applied template can specify information such as internal priority, classification, owner, service, vendor, and activities. Applying templates can significantly reduce the amount of time needed to create incident records, because you can insert information simply by applying the correct template. In this integration scenario, applying a template allows associating to the incident an activity to quickly address the performance issue. ► A job plan:

Job plans provide structured lists of tasks for processing a request. In order for an activity to be associated to the incident, a job plan has been created before the creation of the incident template.

A provisioning workflow:

Provisioning workflows exploit a powerful scripting technology to automate the execution of configuration tasks that usually are performed manually. In order to address the performance problem highlighted by the end user, a provisioning workflow to restart the HTTP server serving the intranet Web site has been created.

In the remainder of this section we describe the creation of such objects. All the steps described next have been executed by logging into the Base Services GUI with the maxadmin user.

Job plan creation

The following steps have been run in order to create the job plan:

1. Select **Go To** \rightarrow **Planning** \rightarrow **Job Plans**. The *Job Plans* panel in Figure 10-22 will be displayed.

Job Plans	
v	Find:
List Job Plan	Work Assets Specifications
M Advanced Search 👻	🗟 Save Query 🔻 🔗 Bookmarks
Job Plans 🕴 💙 Filter 🤉 🍘	8 12 14 + 1 ++
Job Plan	Description

Figure 10-22 Selecting option to create a new Job Plan

2. In the *Job Plans* panel in Figure 10-22, select the red-circled **New Job Plan** icon in order to create a new Job Plan.

∫ Job Plans		🗘 Web Replay 🧧 <u>B</u> ulletins: (C	i)	: X Sign Out ? Help IEM.
💌 Find: 🕅 🔻 Select Action 💌 🎒 🔒	। 🖉 । 🔶 । 🛟 । 🖓 📑 📑 📑			
List Job Plan Work Assets Specifications				<u>, 1</u>
Job Plan × HTTP_RES Job Plan to restart HTTP Servers		Organization TIVOLI	Site ROMA	Attachments 🖉
Details		📼 Responsibility		-
Status DRAFT	Default WO Class	S		
Template Type * Activity	W0 Priority	Supervisor	Work Group	1
Duration * 0:30	Interruptible?	Crew	P Owner	
Classification	Flow Controlled?	Lead	Owner Group	1
Class Description	Suspend Flow Control?			
Launch Entry Name data	Flow Action	P		
	Flow Action Assist?			
Job Plan Tasks ≱ Filter > 👯 🔄 🔶 🐳 🔶 1 - 1 of 1 →				Download 1 ? 1 =
Sequence Task Description		Nested Job Plan	Duration Meter	
✓ 10 Restart HTTP Server		R.	0:00	/ 🛈
	Details			
Organization TIVOLI		Duration * 0:00		Attachmente R
Site ROMA		Meter A		Attacimenta
Task* 10 Restart HTTP Server	a	Owner GIOVANNIB		
Sequence		Owner Group 🎤		
Nested Job Plan		Flow Controlled?		
Classification TPTASK \ TPTASKDEFINITION		Suspend Flow Control?		
Class Description Provisioning Task Definition		Flow Action		
Launch Entry Name		Flow Action Assist?		
Implementation Task?		Assisted Workflow TPCREATASK A		
		Predecessors	1	
				New Row

Figure 10-23 Job Plan creation

- 3. In the New Job Plan panel in Figure 10-23, execute the following steps:
 - a. Specify a Job Plan name (HTTP_RES in this figure).
 - b. In the *Site* field, specify the site that can use the information about the plan. If you do not specify this information, the job plan can be used in any site of any organization. For the integration scenario, the previously created site, **Rome**, was selected, which automatically populated the *Organization* field with the previously created organization Tivoli.
 - c. In the Template Type field, select Activity.
 - d. In the *Duration* field, select 0:30, because we assume that the resolution activity will last 30 minutes (the default value is 0:00).
 - e. In the *Owner* field, specify the user that is expected to manage the Job Plan, which in this case is the deployment specialist GIOVANNIB.
 - f. In order to define a task associated to the considered job plan, select **New Row** in the *Job Plan Tasks* table. The *Organization* and *Site* fields are populated automatically.
 - g. Select the task **Owner** (GIOVANNIB in this case).
 - h. In the *Assisted Workflow* field, specify TPCREATASK, which will allow you (during the execution of the scenario) to associate a Tivoli Provisioning Manager Task to the job plan and to pass it the required information for its execution.

i. In the *Classification* field, specify TPSTASK-TPSTASKDEFINITION. Figure 10-24 shows the panel that allows you to specify this value. In order for this value to be associated to the *Classification* field, the corresponding blue square in Figure 10-24 has to be selected.

🗟 Classify		?	1	\boxtimes
PMAPPR:Approval PMCHG:Change PMSCCMDB:DB Install and Config PMSCCMMI:Middleware Install and Config PMSCCNSM:Build New Server with Middleware PMSCFWRQ:Firewall Request TPTASK:Provisioning Task Classification TPAGINSTALL:Common Agent Install TPPATCHINSTALL:Patch Installation TPSVINSTALL:Software Installation TPTASKDEFINITION:Provisioning Task Definition				
	C	anc	el	J

Figure 10-24 Job plan classification

- j. Add a description for the Job Plan Task (*Restart HTTP Server* in the figure).
- 4. Select **Change Status** from the *Select Action* drop-down menu in order to activate the Job Plan as shown in Figure 10-25.
- 5. Save the Job Plan.

🛡 Change	e Status				1	?	1	\boxtimes
Job Plan	HTTP_RES	Job Plan to restart HT	TP Servers				7	3
Status	DRAFT	Draft						
	New Status*	~						_
		Active						
		Inactive	OK	1	-		-1	
			UK	J	6	anc	e	

Figure 10-25 Job Plan activation

Incident template creation

The following steps have been run in order to create the incident template:

- 1. Select Go To \rightarrow Service Desk \rightarrow Ticket Templates.
- 2. In the *Incident Templates* panel in Figure 10-26, select the red-circled **New Ticket Template** icon in order to create a new Template.

C Ticket Templates	-		C Web Replay	Pulletins: (0)	^{ер} <u>G</u> o To <u>№</u> <u>н</u>	eports 🏛 Start	<u>C</u> enter ¹ Profile	¥ <u>S</u> ign Out ? <u>H</u> ei	· IEM.
Y Find:	n 🙀 🤝 Select Action 🛛 🖌 👸)⊒ @ ♦ 🕼 🔿							
List Template Specification	18								
🏟 Advanced Search 👻 📓 Save Query	👻 🔗 Bookmarks								
Templates 🛩 Filter > 🙀 😂 🛊 🔶 🕫	+ 1 - 2 of 2 →							E/ Down	load ? =
Template	Description		Class			Status			
				₽			₽		
1002	HTTP Performance issue		INCIDENT			ACTIVE			÷
1005			INCIDENT			DRAFT			♣
Select Records									

Figure 10-26 Selecting option to create a new template

- 3. In the *New Ticket Template* panel in Figure 10-27, execute the following steps, which will allow you to define the default value that will automatically fill an incident's fields when a template will be associated to it.
 - a. Add a description (for example, "Web Server Issue"").
 - b. Select **INCIDENT** in the *Class* field.
 - c. Select **GIOVANNIB** in the *Owner* field (as a consequence of this selection, applying this template to an incident will automatically set GIOVANNIB as the incident owner).
 - d. Select **HIGH** in the *Internal priority* field (as a consequence of this selection, applying this template to an incident will automatically set hits priority to HIGH).
 - e. Select **INPROGR** in the *Ticket Status* field (as a consequence of this selection, applying this template to an incident will automatically set its status to INPROGR).
 - f. Select a **Classification** (the *Class Description* field will be automatically populated as a consequence of such selection), which will allow you to automatically classify the incident as soon as the template will be applied to it.
 - g. Select TIVOLI in the Organization field.
 - h. Select **New row** in order to associate the previously defined Job Plan to this Template.
 - i. Select HTTP_RES in the *Job Plan* field. The *Organization* and *Site* fields will be automatically populated.

Note: Associating a Job Plan to a Ticket Template is not possible if the Job Plan has not been previously activated, as described in Figure 10-25.

(?) _∰ Ticket Templates		🗘 Web Replay 👎	Bulletins: (0) 🏾 🖗 Go To 👘	<u>let R</u> eports	rt <u>C</u> enter 🏼 🖡	Profile 🔻 Sign C	lut ? <u>H</u> elp	IBM.
🖌 Find: 🕅 🖓 🤝 Select Action] 🗓 🗟 🖉 । 🔅 । 🛟 । 🖓							
List Template Specifications								
Template 1008 Web Server Issue		Class			Status	RAFT		
Details		ſ						=
Owner Group	Service Group	Classification	21\2102\210210					
Owner GIOVANNIB	Service	Class Description	Thissue (Software (Perform	ance issue	2			
Internal Priority 2	Vendor	Organization						
Ticket Status INPROG								
Activities ▶ Filter > 🛞 😂 ♦ . ♦ ♦ 1 - 1 of 1 ♦							Downlos	ad ? =
Sequence Job Plan Description		Owner	Owner Group		Priority	Vendor		
✓ HTTP_RES Job Plan to res	tart HTTP Servers	1	1				1	Û
	Details							
Job Plan to restart HTTP Servers		Owne	er 🖉 🥕					
Job Plan HTTP_RES A		Owner Grou	ip 🥒					
Site ROMA		Priorit	ty 🔄					
Organization TIVOLI		Vendo	or 🖉 🧖					
		Classificatio	in		1			
		Class Descriptio	in 🗌					
							Nev	v Row

Figure 10-27 Incident Template creation

- 4. Select **Change Status** from the *Select Action* drop-down menu in order to activate the Template as shown in Figure 10-28.
- 5. Save the Template.

Status DRAFT DRAFT	

Figure 10-28 Incident Template activation

Workflow creation

The following steps have been executed in order to create a Tivoli Provisioning Manager workflow to restart the HTTP server:

1. Select **Provisioning Workflows** from the maxadmin Start Center to access the Provisioning Workflows application.

Note: Provisioning Workflows leverage a powerful scripting technology to perform automation activities on target systems.

2. Define a Provisioning Workflow to be run to address the incident issue. Figure 10-29 shows the simple Provisioning Workflow that has been created in order to restart the HTTP server.

Provisioning Workflows	
Find:	🛗 🔻 Select Action 🕑 🎦 🧶 🎄 🔅 🗩
Automation Package	default_automation_package
Source Code	workflow HTTP_Restart_Redbook(in DeviceID, out returnCode, out returnResult) Localeinsensitive var returnErrorString var TimeOut=300 var WorkDir=Jython("%stemo%")
	var Command = Jython("net stop IBMHTTPServer8.1 & net start IBMHTTPServer8.1") Device.ExecuteCommand(DeviceID, Command, WorkDir, "default", TimeOut, "error", returnCode, returnErrorString, returnResult) If Jython(returnCode != "0") then log error Jython("returnErrorString: >" + returnErrorString + "<,") endif

Figure 10-29 Workflow to restart HTTP server

10.5.4 Implementation steps

This section provides a detailed description of the Incident Management integration scenario summarized in Figure 10-19.

Step 1: End user opens a Service Request

An end user is experiencing a degradation of intranet performance and decides to open a Service Request to address this issue:

- 1. The end user logs in to Base Services GUI as SRMSELFSERVICEUSR in order to access to the Self Service console shown in Figure 10-30.
- The end user selects Go To → Self Service → Service Requests → Create Service Request.

Welcome, Service			<u>B</u> ulletins: (0) 🛛 🧖 Go To	Int <u>R</u> eports ♥ Start <u>C</u> enter	<u>Profile Sign Out</u> ?	Help IBM
			다.	nange Content/Layout 🔹 Dis	play Settings 划 🛙 Upda	te Start Center
Favorite Applications	🤋 📋 🧧 Bulletin Board i 🔻	Filter 🛛 🏟 🙄				Û
ਪ੍ ^L L Offering Catalog	Subject	Message	Post Date	Expiration Date	Viewed?	
View Service Requests		There	e are currently no bulletin	board messages to view.		
Create Service Request	Inbox / Assignments					2 - i
I	Description		Due Date		Route	Refresh
Help Desk 🥒 🖉			No Accimento fo	und for Coming		
View Service Requests			No Assignments to	and for service		
	My Catalog Requests	s 👽 Filter > 🚜 🗊 🔗 👘				/ = :
Create Service Request	Requisition	Description	Status	Requested By	Requested For	
Catalog Requests	No	Data Found.				
Offering Catalog	My Soprice Request	S I - Ciltor & A I to I 🖄				
••	Service Request	Summary	Status	Reported By	Affected User	<i>•</i> – u
View Catalog Requests			NEW			
····	1008	Problem on Payroll System	NEW	SRMSELFSERVICEUSR	SRMSELFSERVICE	USR
View Shopping Carts	Set Graph Options					1 - 1 of 1
Search 🥒						
Service Request Manager Search						

Figure 10-30 SRMSELFSERVICEUSR console

- 3. In the Create Service Request panel in Figure 10-31, the end user:
 - a. Specifies a phone number and an e-mail address in order to be contacted from the help desk.
 - b. Selects the authorized Configuration Item representing the intranet Web Server that is experiencing bad performance in the *Affected Configuration Item* field (NC117177.ROMELAB.IT.IBM.COM-457 in Figure 10-31).
 - c. Selects a priority for the issue in the *Reported Priority* field.
 - d. Adds a summary and a detailed description of the issue in the *Summary* and *Details* fields.
 - e. Specifies a classification for the issue in the *Classification* field.
 - f. Selects Submit in order to submit the Service Request.

Crea	ate Service Request			₽ <u>B</u> ulletins: (0)	🖗 <u>G</u> o To 🛛 💷 <u>R</u> eports	✤ Start <u>C</u> enter	[▲] <u>P</u> rofile × Sign O	ut ? Help IIM.
AD View S	ervice Requests							
Create Use this for located next	Service Request m to fill out a new request for s t to a field may be used to assis	t ervice. When you are done, selec st in choosing/selecting an approp	t the Submit button below to create iate value for a field.	the record. For additional det	ails about a field descripti	on, place the curs	or in the field and pres	ss Alt + F1. The icons
	Reported By	SRMSELFSERVICEUSR	🔎 Affe	cted Asset	1			
	Phone	0659665511	Affected Ass	et Location	1			
	E-mail	c.white@uk.ibm.com	Affected Config	uration Item NC117177.RON	IELAB.IT.IBM.COM~457	/		
	Affected User	SRMSELFSERVICEUSR	P Repo	rted Priority 2 🔎				
Prownk	ad Remote Diagnostics Agent		Re	orted Date 2009-08-08 05:	:49:33 🗈			
Request D Please ente	escription r a summary and a more detaile	d description of your Service Reg	Classify	tion to choose the best class	ification or grouping for th	nie request You of	an do it filling the Class	eification or the Class
Summary	Experiencing Intrantet bad per	formance	Description	fields.	meaner or grouping for a	na request. Tou er	in do it hing the clast	sincedon of the class
Details	Since 12pm today I am experie	encing bad performance when acc	essing the	Classification 2112	103 \ 210304 \ 21030401	1		
	intranet web site.			Class Description IT Issu	ue \ Networks \ Internet \	Performance 🖉 🔎		
				the second s		_		Ch
			Attachmer	its 🔸 Filter > 🗥 📋 🛧 🧃	*			Download ? 📼
			Document		Desc No rowa to	ription		
						Attach File	Attach We	eh Address Link
								in Address Link
Attributes	Eller S.M. Phile & J. P.							
Attribu	te Description	Data Type	Alphanumeric Value		Numeric Value	Init of Measure	Та	ble Value
	<u>to</u> bosciption	Data type	No rov	vs to display	ingine ine value		1.0	ale thing
							S	ubmit Cancel

Figure 10-31 Service request creation

g. Takes note of the Service Request ID in Figure 10-32.

Service Request Submitted							: ?	: 🖂
	Service Req Record your Ser	uest 1012 has rvice Request f	been subr for future r	nitted. eference.				
View Details	Return to Start	Center	 c	reate Anoth	er Service Re	ques	st)

Figure 10-32 Service Request ID available after submission

h. Logs out from the Self Service console.

Step 2: Help Desk operator creates an Incident

A Help Desk operator opens an incident to address the Service Request and contacts the end user to collect further information. Finally the Help Desk operator forwards the incident to an Incident Analyst:

- 1. The Help Desk operator logs in to Base Services GUI as PMINCOWNUSR (Incident Owner).
- 2. The Help Desk operator notices, as shown in their console depicted in Figure 10-33, that a new Service Request, highlighting bad intranet performance, has been opened with ID 1012 (red-circled in the figure).

Note: The *All Open Service Requests* table, showing the new Service Request opened by the end user in Figure 10-31 on page 311, was not included in the default console for PMINCOWNUSR and has been added by using the **Change Content/Layout** option.

Welcome, PMINCOWNUSR					P <u>B</u> ulletins:	(0) 🔗 <u>G</u> o T	o <u>I R</u> eports	Start Center	[≜] <u>P</u> rofile × <u>S</u> ign	Out ? Help	m	
							Change Conte	ent/Layout 🕮 Di	isplay Settings 🕻	입음 Update Start Cer	nter	
Quick Insert	/ = :	Bulletin Board	🔻 Filter 🛛 🏟	2		- Constant					in l	
A New Incident		Subject	Messa	ige	Post Date	8	Expiratio	on Date	Vie	wed?		
New Service Request									N			
Vew Solution			There are currently no bulletin board messages to view.									
		Inbox / Assignme	ents							/ = 1		
Favorite Applications	2 = 1	State And State								Refre	sh	
Incidents		Description		Due Date		Priorit	y	Start Date		Route		
					No Assign	ments found	for PMINCOW	NUSR				
Problems												
		My Late incident	S 💗 Filter⇒d¥0a	12 10						2 = 1	1	
Service Requests		Ticket ID	Description	Internal Priority	Status		vner	Owner Group	Target Start	Target Finish		
· Solutions		No Data	Found.									
		My Open Inciden	ts 💗 Filter⇒d#b	15 0						/ = i		
Open Incidents	1 = 1	Ticket ID	Description	Internal Priority	<u>Status</u>	<u>0\</u>	vner	Owner Group	Target Start	Target Finish		
Last Run:	Update											
Incidents that are currently o	pen	No Data	Found.									
8 10 12		All Open Service	Requests V	Filter > 🕅 👔 🕴	<u>ې</u>					/ = 1	5	
6	14	Internal Priority	<u>Owner</u> <u>Ow</u>	ner Group Se	vice Request	Status	Summary		Tarq	et Finish Target Sta	<u>rt</u>	
4	16					NEW						
2	.10			10	08	NEW	Problem on P	ayroll System				
-	10			(10	12	NEW	Experiencing	Intrantet bad perfo	ormance			
0	20	Set Graph Options								1 - 2 c	of 2	

Figure 10-33 Help Desk user console highlighting new Service Request

 The Help Desk operator opens the new Service Request (ID 1012) for reading its content and selects Create → Incident from the Select Action drop-down menu (as in Figure 10-34) in order to open an Incident from it.

	Y Find:	Select	Action 💌 🔠 🔒 🧶	4	🔶 I 🛟 I 🎇 📓 👔
List Service	Request Related Records	4	Change Status View History	fication	IS
Service Request	1012 Owner Source		View Costs Edit History Service Request		Owner Creat
			Create +		Service Request
User Information			Apply Service Request Template		Incident
Reported By Name	SRMSELFSERV		Select Owner Take Ownership		Problem Change
Phone E-mail	c.white@uk.ibm.com		Modify/Delete Work Log Show Similar Tickets		Release Work Order
Service Request De	etails		View Catalog Order Infomation		Communication
Summary	Experiencing Intrantet bad performan		Apply SLA		Process Request
Details	Since 12pm today I am experiencing		View SLAs		Catalog Requisition

Figure 10-34 Opening an incident from a Service Request

- 4. The Help Desk operator then takes ownership of the new incident by selecting **Take Ownership** from the *Select Action* drop-down menu.
- 5. The Help Desk operator contacts the end user who opened the original Service Request in order to collect further information about the issue and consequently updates the fields, *Impact, Urgency, Global Issue* (because the issue is impacting not only the end user) and *Site* as in Figure 10-35.

Attention: Defining the proper site is particularly important if the incident has to be later applied to an incident template. In fact when you apply a template to an incident, the system searches for active templates for incident records. Because templates can contain and apply job plans (as in the integration scenario we are considering), the set of templates from which you choose depends on the organization and site associated with the incident record:

- If there is no value in the *Site* field of the incident, the system displays all incident templates for all organizations.
- If there is a value in the *Site* field of the incident, the system displays both incident templates where the site specified on the incident is within the organization specified on the template and incident templates that have no organization specified.

Incidents		e guletins: (0) /* Go To Le Reports /* Start Center /* Profile /* Sign Out ? Help I	N.
	Find: Select Action 💌 👸 🥃	ଌାବ ବାହାଞ୍ଜ ଛି ଛାଓ ଓ ଡାରାସି≣ା ଅଥାନେ "	
List Incident	Activities Related Records Solution Details Log	Failure Reporting Specifications	^
Incident 1007	Owner PMINCANALUS Source	Owner Group Status QUEUED Attachments Ø P Created By PMINCOWNUSR Filler Fil	
User Information			
Reported By	SRMSELFSERV #	Affected Person SRMSELFSERV	
Name	Service A	Name Service	
Phone	0659665511	Phone Phone	
E-mai	c.white@uk.ibm.com	E-mail	
Incident Details			
Summary	Experiencing Intrantet bad performance	Classification	-
Details	Since 12pm today I am experiencing bad performance when accessing the	Classification Path	
	intranet web site.	Class Description	
		Indicated Priority	
		Reported Priority 2	
Asset	× 🗉	Impact 1 P Critical	
Location	A	Urgency 2 P High	
Configuration Item	NC117177.ROMELAB.IT.IBM.COM~457	Internal Priority 1 Urgent	
Target Description		Service Group	
GL Account	P	Service 🥂	
Asset Site	P	Vendor	
		Site ROMA	
		SLA Applied?	
		Create WO Options MULTI	

Figure 10-35 Incident updated after collecting further information from end user

 The Help Desk operator realizes that they will not be able to address the issue and therefore forwards the incident to the Incident Analyst (PMINCANALUSR) by selecting Select Owner from the Select Action drop-down menu and finally saving the modified incident.

Step 3: Incident Analyst applies an Incident template

The Incident Analyst whom the incident has been assigned to applies an Incident Template that is suitable for the issue. Consequently, incident fields are updated with information defined in the template. Moreover an emergency activity that should be executed to address the issue is automatically associated to the incident and the incident is forwarded to a Deployment Specialist.

- 1. The Incident Analyst logs in to Base Services GUI as PMINCANALUSR.
- 2. The Incident Analyst notices, as shown in their console depicted in Figure 10-36, that they are the owner of a new open incident related to bad intranet performance with Ticket ID 1007, Internal Priority 1, and Status QUEUED (highlighted by a red circle in **My Open Incidents** table).

Welcome, PMINCANALUSR			Bulletins: (0) ^A	' <u>G</u> ото Ши <u>р</u>	eports 🃫 Start <u>C</u> enter	. [▲] <u>P</u> rofile ×	<u>S</u> ign Out ? <u>H</u> elp	IBM.
				다. Change	Content/Layout 🕮 [isplay Setting)	s 🛛 🕄 Update Sta	rt Center
Quick Insert 🥒 🗖 🗊	Bulletin Boar	d 💎 Filter 👘 🗇						·····
A New Incident	Subject	Message	Post Date	Ð	piration Date		Viewed?	
🤣 New Service Request								
💡 New Solution		The	e are currently no bu	illetin board me	essages to view.			
	Inbox / Assigni	nents					0	
Favorite Applications 🥒 🗖 🕯								Refresh
/ Incidents	Description	Due Date		Priority	Start Date		Route	
			No Assignments fo	ound for PMIN	CANALUSR			
Problems	My Late Incide	nts i 🔻 Filter > 🚯 i 🗂 i 🖗					0	
	Ticket ID	Description Internal Priority	Status	Owner	Owner Group	Target Sta	art Target Fini	sh
]
Solutions	No Da	ta Found.						
	My Open Incide	ents 🔻 Filter > 🚜 🕽 🄗					0	
Open Incidents 🥒 🗖 🕯	Ticket ID De	escription	Internal Priority	Status	<u>Owner</u> <u>C</u>	wner Group	Target Start Targe	t Finish
Last Run: Upda	ite							
(1007 Ex	periencing Intrantet bad performance	1	QUEUED	PMINCANALUSR			
Incidents that are currently open	Set Graph Optio	18						1 - 1 of 1

Figure 10-36 Incident Analyst console highlighting a new open incident

3. The Incident Analyst opens the incident definition to analyze it and as a consequence of that analysis, they select **Apply Incident Template** from the *Select Action* drop-down menu (as shown in Figure 10-37) to apply a suitable template to it. Figure 10-38 shows the available templates from which the user can choose.

Note: Only active templates are shown in the **Apply Incident Template** panel represented in Figure 10-38.

Find:	Select	Action 🖌 🙀	2	🧷 🔷 🔶 🛟
Activities Related Rel		Change Status View History		Failure Repor
Owner PMINC Source	4	View Costs Edit History Incident		P
		Create	+	
		Apply Incident Template		
ervice		Select Owner Take Ownership		

Figure 10-37 Applying an Incident Template

🛡 Apply Incide	nt Template	🗄 i ? i 🗵
Ticket Templ	ates ≽ Filter > 🚲 📁 🔶 🐳 🔶 1 - 3 of 3 -	🕨 📴 <u>Download</u> ? 🚍
Template	Description	
1009	VPN issue	
1010	Suspiciout Emal - Virus Simptoms	
1008	Web Server Issue	
		OK Cancel

Figure 10-38 Available Ticket Templates

- 4. As a consequence of the template application, the following incident fields are automatically updated:
 - Owner has changed from PMINCANALUSR (Incident Analyst) to GIOVANNIB (Deployment Specialist)
 - Internal Priority has changed from 1 (Critical) to 2 (High)
 - Classification Path and Class Description have been populated according to the incident template definition
 - Summary has been changed from 'Experiencing intranet bad performance' to 'Web Server Issue'
 - Status has been changed from QUEUED to INPROG

Incidents		₽ <u>B</u> ulletins: (0)	🖻 <u>G</u> o To 🔟 <u>R</u> eports 🏚 Sta	art <u>C</u> enter 🔺 <u>P</u> rofile 🗮 <u>S</u> ig	n Out ? <u>H</u> elp	IEM.
	💌 Find: 🕅 🖙 Select Action 💌 👸	a 🖉 🔶 🔶 🞲 👯 🗟 💩 🎯	🍅 🔌 🔿 🕞 📖	🛛 👍 i 😭		
List Incident	Activities Related Records Solution Details	Log Failure Reporting Specification	Ins			^
Incident 1007	Owner GIOVANNB Source	Owner Group Created By PMN	Status	INPROG	Attachments	Ø
User Information						-
Reported By	SRMSELFSERV #	Affected Person SR	RMSELFSERV A			
Name	Service A	Name	ervice	1		
Phone	0659665511	Phone	P			
E-mail	c.white@uk.ibm.com	E-mail				
Incident Details						-
Summary	Web Server Issue	Cla	Classification		₽	I
Details	Since 12pm today I am experiencing bad performance when accessing	the Classifi	fication Path 21\2102\2102	10	P	
	intranet web site.	Class I	Description IT Issue \ Softw	are \ Performance Issue	₽	
		Indica	cated Priority			
		Repor	orted Priority 2			
Asset			Impact 1	ritical		
Location	/	3	Urgency 2	igh		
Configuration Item	NC117177.ROMELAB.IT.IBM.COM~457	inter	ernal Priority 2 H	igh		
Target Description		Ser	ervice Group	1		
GL Account	₽		Service			
Asset Site	P		Vendor			3
			Site ROMA			
		SL	LA Applied?			
		Create V	WO Options MULTI	2		

Figure 10-39 Updated incident after applying template

5. Moreover, as shown in Figure 10-40, the **Activities** tab shows that a new activity (related to the Job Plan HTTP_RES associated to the incident template 'Web Server Issue') has been associated to the incident. In fact, if a template activity contains job plans, the system creates an incident activity for each template job plan.

Incidents					P <u>B</u> u	ulletins: (0) <u>G</u>	o To 🛄 <u>R</u> eports 🕇	Start <u>Center</u> A Profil	e × <u>S</u> ign Out	? <u>H</u> elp	IBM.
×	Find:	🚺 🔫 Select Act	ion 💉 🐌	۵ 🖉 ا	🍦 i 🎲 i 🎎 🗉			📖 🛛 🛵 I 🕯	۲*		
List Incident	Activities R	Related Records	Solution Details	Log Fai	lure Reporting	Specifications					
Incident 1007	Web Ser	verissue				Site	ROMA	Statu	INPROG		
Activities 🕨 Filter > 🖉	12 + + +1-1	of 1 🤿							[Download	? =
Sequence A □ ▼ 0 1	<u>ctivity</u> <u>Su</u> 004 ≠ Jo	ummary b Plan to restart HTTP	Servers	Location	Asset	Conf	i <u>quration Item</u> 17177.ROMELAB.IT.IB	M.COM~457	Status WAPPR	SLA Ap	plied îî
			Activity Informati	on				Schedu	ling Informati	on	
Activity* Location	1004	Job Plan to restart H	TTP Servers					Target Start Target Finish			
Asset Configuration Item	NC117177.ROMELAE	B.IT.IBM.COM~457	_ A					Scheduled Start			
Status GL Account	WAPPR							Actual Start			
Vendor Owner	P							Estimated Duration *	0:30		
Owner Group			1					Time Remaining			
Sequence Priority	0										
								Activity Process	ing : 🔻	New I	Row

Figure 10-40 New activity associated to incident after applying template

Step 4: Deployment Specialist runs an Assisted Workflow

The Deployment Specialist to whom the incident has been assigned uses the **Start Assisted Workflow** option to run a Provisioning Task that restarts the HTTP server. After the successful execution of the provisioning task, the specialist forwards the incident back to the Help Desk operator.

- 1. The Deployment Specialist logs in to Base Services GUI as GIOVANNIB.
- 2. The Deployment Specialist notices, as shown in their console depicted in Figure 10-41, that there is a new activity associated to them. The activity, highlighted by a red circle in the figure, is related to the Configuration Item NC117177.ROMELAB.IT.IBM.COM-457, has a HIGH priority, regards site ROMA, and has summary 'Restart HTTP Server'.

Note: The *Activities and Tasks* table, showing the new activity for the Deployment Specialist, was not included in the default console for GIOVANNIB (as member of group TPDEPLOYMENTSPECIALIST) and has been added by using the **Change Content/Layout** option.

- ジャマ Welcome, Bianchi		🖸 Web Replay 🕨 <u>B</u> ulletins:	(0) 🤗 <u>G</u> o To	Let Reports P Start Center	Profile X	Sign Out ? <u>H</u> elp	IIM.
		There are curren	tly no bulletin b	oard messages to view.			2
Favorite applications 🥒 🗖 📋							
Provisioning Computers	Status of my recent provisioning) tasks 🛛 🔻 Filter > 🕅 📋 🖗	`	01.115		/ =	, <u>a</u>
	Idsk	Status		Start time			
Provining Groups							
		No Data Found.					
Provisioning Task Tracking	Task and compliance KPIs					10	10
Discovery Configurations	My recent failed provisioning tas	sks 🔻 Filter > 🕅 🗊 褅				10	1 10
Discovery Wizards	My in-progress provisioning tas	ks 🔻 Filter > 🚜 🕽 褅				/ 0	
	Data model object finder 🔻 Filte					1 =	1
Software management applications 🥒 🗇 🗊	Name			Object Type			
Patch management applications 🥒 🗇 🗎	Favorite Computers			Computer Group			
	Favorite Software			Group			
OS management applications 🥒 🗖 💼	RXA Platform Discovery			Discovery Types			
	TPC Discovery			Discovery Types			
My favorite reports 🔻 Filter > 🖓 🗄 📄 🔗 👘 🥒 👘	TPC Servers			Computer Group			
Description	Set Graph Options					1 - 5 of 857 <u>Next Pa</u>	age »
Are computers compliant with their compliance checks?	Activities and Tasks : V Filter > d	N 1 20 1 @				1 =	1
Do Windows computers comply with the patch policy?	Configuration Item	Priority	Site	Summary	Task	WORKORDERID	2
Do Windows computers comply with the patch policy?						5	
How many tasks are in a specific state?	NC117177.ROMELAB.IT.IBM.COM~4	57 2	ROMA	Restart HTTP Server	10	5	
What computers have never had a compliance check run on them?	Set Graph Options					1-	- 1 of 1

Figure 10-41 Deployment Specialist console highlighting a new activity for themselves

3. The Deployment Specialist selects the activity to open it. Figure 10-42 shows its content, which has been automatically defined according to the previously created Job Plan.

Activities and T	ſasks				D Web Replay 🛛 🖡 <u>B</u> ulletins: (0) 🎓	<u>Go To 💷 R</u> eports	Start Center A Profile	X Sign Out ? Help	irm.
Y	Find:	Select Action	💌 🖬 🧶 🗼 🏟 🎲 🎎		🗴 । 🔨 💷 🥥 🗙 । 🔂 ।	۲*			
List Activities a	and Tasks Resources	Related Records	Log						^
Task Location Asset Configuration Rem Target Description Class Idescription Class Description Launch Entry Name	ACTIVITY 10 Exelect HTTP NC117177 ROMELAB_IT.BM TPTASK1TPTASKDEPINITIO Provisioning Task Definition	COM~457			Activity Type Priority SLA Appled? Under Flow Control? Suspend Flow Control? Flow Action Flow Action Assist?	1004	Attachments Status Status Date Service Group Service Owner Owner Group Assisted Workflow	UAPPR 2009-08-08-06-44-09 GIOVANNB TPCREATASK Assisted Workflow	
Parent Process	1004				Implementation Task?			File	_
Target Start Target Finish Scheduled Start Scheduled Finish Actual Start Actual Finish Estimated Duration Predecessors	51		Launch Task Scheduler		Asset Location	Configuration Item No rows t	Target 5 o display Select :	Clear All New Row	
Attributes > Filter > Attribute TPTDEFID		Description Provisioning Task D	Data Type Alphanumeric \ efinition ID TABLE	/alue	Numeric Va	P	Table Value	Download i?	Û
TPTASKID	de la companya	Provisioning Task ID	TABLE		P .	A	P	New Row	

Figure 10-42 New activity for Deployment Specialist

- 4. The Deployment Specialist selects the option **Start Assisted Workflow** in Figure 10-42: the panel **Provisioning Tasks Definition** in Figure 10-43 is opened. Such a panel allows creating a Tivoli Provisioning Manager Task on the flight in order to address the issue highlighted by the incident.
- 5. They leave the default value, **Provisioning Workflow**, for the **Type** option.
- 6. In the *Provisioning Workflow* field, they select the workflow HTTP_Restart_Redbook, which has been previously created in order to restart an HTTP server.
- 7. In the Target Parameter field, they select DeviceID and save the new task.

Provisioning Task Definitions		🕑 Web Replay 🛛 🦞 <u>B</u>	uletins: (0) 🌾 <u>G</u> o To 💷 <u>R</u> eports	* Start Center * Profile	[¥] <u>S</u> ign Out ? <u>H</u> elp	IEM.
Find:	🖻 Select Action 🛛 🛃 🐊 🧶 🍬 🔅					
List Task						2
Provisioning Task* SM Task Type O Provisioning Workflow Script O Activity Plan	A Task created for ISM Task into	gration				_
Select the provisioning workflow and the target paramete For example, the target parameter might have a name suc When you run the provisioning workflow, the target para	in that will be used for the target computer in this provisioning workt in as Server(D), meter values will be set by the target computers.	low.				
Pro	visioning Workflow* HTTP_Restart_Redbook Target Parameter* DeviceD	م[م				
Workflow Parameters 🛛 🕨 Filtar > 🖓 🗦 😂 🔶 🔶	1 - 3 of 3 ->				E/ Download	? =
Workflow Parameter DeviceID	Default Value					
returnCode						
returnResult						

Figure 10-43 Provisioning Task Definition

8. The Deployment Specialist selects Run Provisioning Task from the Select Action drop-down menu: The Run Provisioning Task panel is displayed. As shown in Figure 10-44, the Targets table has been automatically populated with the Computer nc117177.romelab.it.ibm.com, which corresponds to the Configuration Item NC117177.ROMELAB.IT.IBM.COM-457 that has been originally associated to the Service Request opened by the end user as the affected Configuration Item (see Figure 10-31 on page 311). As shown before in this chapter, such association is based on the correspondence between the Configuration Item 'Provisioning Object' in Figure 10-17 on page 299 and the Computer's 'Globally Unique Identifier' in Figure 10-18 on page 299.

Moreover, the **Provisioning Workflows** table in Figure 10-44 is automatically populated with the name of the previously chosen workflow (HTTP_Restart_Redbook) and the **Notification** table is populated with the name of the Deployment Specialist (GIOVANNIB) in order to automatically notify them about the task execution's result.

🛡 Run Provisioning Task	
Targets ≽ Filter > 🏔 🗊 🛧 🐳 🔶 1 - 1 of 1 🤿	Download 1?
Target	Description
nc117177.romelab.it.ibm.com	Computer 🗊
	Select : 🔻
Provisioning Workflows > Filter > 🛝 🗊 🛧	🔹 👟 1 - 1 of 1 🔿 📑 <u>Download</u> ? 🚍
Provisioning Workflow	Concurrency Level
HTTP_Restart_Redbook	5
Data Model Object Finder	
Scheduling	
Click Schedule to change options.	
Scheduled: Now	Schedule
Notification	-
Recipients Filter > 🐴 👔 🛧 🐙 🐳 1 - 1 of	1 🔶 🗁 <u>Download</u> i ? i 🗖
Recipient	
GIOVANNIB	×
	Add Recipient Add E-mail
Events Filter > 🙈 🚉 🔺 🖌 🐟	Download ?
Description	
No rows to dis	play
	Add Event
	Submit Cancel

Figure 10-44 Run Provisioning Task panel

9. The Deployment Specialist selects **Submit** in Figure 10-44 in order to start task execution. Figure 10-45 shows the result of the task submission. The task has a **Submitted** status, while the associated workflow has a **Scheduled** status. By selecting the red-circled icon on the right of the *Message* field, it is

possible to read a short message about the state of the workflow execution. By selecting the red-circled icon on the right of the *Provisioning Workflow Log* field, it is possible to monitor the detailed state of the workflow execution.

Provisioning Task Tracking	🕑 Web Replay	₽ <u>B</u> ulletins: (0)	
Find: 📕 Select A	ion 💌 👀 🔜 🧶 💠 🖕		
List Task			
Provisioning Task SM Task@2009/08/08 07:03:18 Type Provisioning Workflow Created By GIOVANNB Changed By		Definition Start Date End Date Status Base Services Task	ISM Task 2009-08-08 07:03:18 Submitted 1005
Provisioning Workflows 🎽 Filter > 🍂 🗔 🛧 🐳 🐳 1 - 1 of	>		Download ? =
Provisioning Workflow Status		Start Date End	Date Concurrency Level Subtask
HTTP_Restart_Redbook Scheduled	1	2009-08-08 07:03:18	5 W0
	Details		
Targets Workflow Parameters			
$ \Rightarrow Filter \Rightarrow \bigotimes \bigcirc \Rightarrow \Rightarrow \Rightarrow 1 + 1 \text{ of } 1 \Rightarrow$			Ct <u>Download</u> ? =
Target S nc117177.romelab.it.ibm.com	tus <u>Message</u> heduled		Provisioning Workflow Log

Figure 10-45 Status of task execution

10. The Deployment Specialist selects the **Refresh** icon on the right of the *Select Action* drop-down menu. The updated window, shown in Figure 10-46, highlights that the task execution was successful, which means that the workflow HTTP_Restart_Redbook successfully performed a remote restart of the HTTP server installed on nc117177.romelab.it.ibm.com.

Provisioning Task Tracking			Web Replay 🤑 <u>B</u> ulletins: (0)	<u> <u> G</u>o To <u> <u> M</u> <u>R</u>eports </u></u>	Start <u>Center</u> Start <u>Center</u>	× Sign Out ? Hel	p IEM,
Find:	🔥 🔝 Select Action	🖌 ا 🕭 🗟 ا 🌜 💌	\$				
List Task							
Provisioning Task ISM Task@2009/08/08 0 Type Provisioning Workflow Created By GIOVANNB Changed By Provisioning Workflows L = Filter	17:03:18			Definition Start Date End Date Status Base Services Task	ISM Task 2009-08-08 07:03:18 2009-08-08 07:03:39 Success	C* Down	/
Provisioning Workflow	Status		Start Date	End Date		Concurrency Level	Subtask
 HTTP_Restart_Redbook 	Succeeded	1	2009-08-08 07:03:18	2009-08-08 07:03	:39	5	WO
			Details				
Targets Workflow Parameters							
► Filter > A1 □ ♦ ♦ ♦ 1 - 1 of 1 →						Downlo	<u>ad</u> ? =
Target nc117177.romelab.it.ibm.com	Status Succeeded	<u>Message</u>	1			Provisioning Wo	nrkflow Log 11,611 🎤

Figure 10-46 Final result of task execution

11.Because their assigned task has been completed successfully, the Deployment Specialist assigns the incident back to the Incident Owner (in order for the Incident Owner to verify if the original issue has been addressed) by accessing the incident, selecting **Select Owner** from the *Select Action* drop-down menu, and saving the modified incident. Moreover, in order to notify the Incident Owner of the task that was run, the Deployment Specialist updates the incident's Log tab as shown in Figure 10-47.

Incidents	🕩 Web Replay 🛛 🔒 <u>B</u> ulletins: (0)	🖉 🥐 Go To 🛛 🕮 Reports 🏘 Start Center 🔺 Profile 🕺 Sign	Out ? Help IIM,
「 V Find: 月前 マ Select Action	💌 🗓 🙍 🖉 💠 🔅 🖓 🖓 🕘 🔘	🌣 🖉 i 🖓 i 🖓 i 🖓 i 🖓 i 🖓 i 🖓 i 🖓 i	
List Incident Activities Related Records Solution	Details Log Failure Reporting Specifications	\$	
Incident 1007 Web Server Issue		Site ROMA P Status INPROC	3
Work Log Communication Log			
Work Logs ≽ Filter > ఈ ⇔ ⇒ ⊕ + 1 - 1 of 1 ⇒			Download ? ==
Record Class Is Global Issue C	reated By Date 🗢 Type	Summary	Viewable
▼ 1007 // INCIDENT	AXADMIN 2009-08-08 08:51:40 CLIENTNOTE	Server restarted: please check issue's status	
	Details		
Record 1007 Summary	Server restarted: please check issue's status		
Class INCIDENT Details	The web server has been restarted according to the incident ter check if the original issue has been addressed and change incid	mplate applied by PMINCANALUSR. Please tent status or owner accordingly.	
Created By MAXADMIN			
Date 2009-08-08 08:51:40			
Viewable?			

Figure 10-47 Incident's Log tab is updated to notify Incident Owner of the task's result

Step 5: Help Desk operator closes the incident

The Help Desk operator checks if the original issue has been addressed and closes the incident.

- 1. The Help Desk operator logs in to Base Services GUI as PMINCOWNUSR (Incident Owner).
- 2. The Help Desk operator notices, as shown in their console depicted in Figure 10-48, that incident 1007 has been assigned back to them, and opens it in order to read the Incident log shown in Figure 10-47.

*** Welcome, PMINCOWNUSR			<mark>₽</mark> <u>B</u> ulletins: (0)) 🌈 <u>G</u> o To 💷 <u>R</u> eport	s † Start <u>C</u> enter [≜] <u>F</u>	Profile × Sign O	ut ? Help <u>] E</u>]
				🕼 Change Cont	ent/Layout 👜 Displa	y Settings 🛛	Update Start Cente
Quick Insert	🧷 🚍 🍵 👂 Bulletin Board	; 🔻 Filter 🤉 💏 👔 💭					1
A New Incident	Subject	Message	Post Date	Expiratio	n Date	Viewe	d?
New Service Request						N	
Vew Solution			There are currently no	o bulletin board message	s to view.		
	Inbox / Assignm	ents					/ = =
Favorite Applications	/ = 1						Refresh
Incidents	Description	Due	Date	Priority	Start Date		Route
TA Problems			No Assignment	ts found for PMINCOWN	IUSR		
	My Late incident	S 💗 Filter > 🖓 🖹 🕽 🖗					/ = 1
Service Requests	Ticket ID	Description Internal F	Priority Status	<u>Owner</u>	Owner Group	Target Start	Target Finish
Solutions	No Data	Found.					
	My Open Inciden	ts 💗 Filter > 🚜 🖄 🖗					/ = =
Open Incidents	Ticket ID D	escription Int	ernal Priority Status	<u>Owner</u>	Owner Group	Target Start	Target Finish
Last Run:	Update						
	1007 V	/eb Server Issue 1	INPROG	PMINCOWNUSR			

Figure 10-48 Incident is shown back in Incident Owner's open incidents

- 3. Because the Deployment Specialist has run the HTTP restart task successfully, the Help Desk operator checks to see if the original issue has been addressed and if the intranet performance is improved.
- 4. As the intranet performance seems OK now, the Help Desk operator proceeds with the incident closure as shown in Figure 10-49. Next, Figure 10-50 shows the incident after its closure.

💌 Find: 🚺 😽 🤝 St	elect Action 🛛 💌 😹 🧟 । 🐥 🛛 🎲 I 🎇	🗟 🕘 🗿 🎯 🧶 🔊 🖓 🔜 💈	💩 i 📐 i 🎌
List Incident Activities Related Record	ds Solution Details Log Failure Reporting	Specifications	
Incident 1007 Web Server Issue		Site ROMA	Status INPROG
Work Log Communication Log			
Work Logs ▶ Filter > ♦ ♦ ♦ 1 - 1.of 1 ♦			🖄 Download ? 🚍
Record Class is Gi ▶ 1007 ■ NCDENT ✓	obal issue <u>Created By Date</u> 은 MAXADMIN 2009-08-08 08:51:40	Type Summary CLIENTNOTE P Server restarted: ple	Viewable ase check issue's status ✓ New Row ✓
	투 Change Status	□ : ? : ⊠	
	Incident 1007 Web Server Issue		
	Status INPROG In Progress		
	New Status * M Status Date Closed & Memo Pending Queued Resolved	OK Cancel	

Figure 10-49 Incident Owner closes the incident

Inciden	nts		♥ <u>B</u> ulletin:	s: (0) 🏾 🎓 <u>G</u> o To) 💷 <u>R</u> eports 🏠 :	Start <u>C</u> enter 🏼 Å <u>P</u> rofile
	Find:	🔻 Select Action 💌 🦉 浸 🥒 💠	🔶 I 🛟 I 🎇 🛃 🔬 I	000		Z 👍 🔂 I 🎌
List In	ncident Activities Related	Records Solution Details Log Faile	ure Reporting Specific	cations		
Advanced	Search 🔻 🎑 Save Query 🔻 🔗 B Filter>∰ [⊉] ♦ ♦ ♦ 1 - 1 of 1 ⊲	ookmarks				
Incident 🕈	Summary	Reported By		Internal Priority	Status	<u>Owner</u>
			1		P	/
<u>1007</u>	Web Server Issue	SRMSELFSERVICEUSR		1	CLOSED	PMINCOWNUSR
Select Rec	cords					

Figure 10-50 Incident is shown as closed in Incidents panel

11

IBM Service Management integration scenarios: Problem and Change Management integration with Tivoli Service Request Manager and CCMDB

In this chapter we describe a scenario where Incident, Problem, and Change Management processes come together to demonstrate the powerful capabilities of Tivoli Service Request Manager and IBM Tivoli Change and Configuration Management Database (CCMDB). The scenario describes a basic process that starts with a Service Request, goes through Incident Management, and then on to Problem resolution, applying a standard Change process.

The Change is applied through a Provisioning Task, which shows the interactions between CCMDB V7.1.1.5 and Tivoli Provisioning Manager V7.1.1.

We cover the following topics:

- "Problem and Change Management according to ITIL" on page 326
- "Scenario process flow" on page 328
- ▶ "The scenario" on page 333

11.1 Problem and Change Management according to ITIL

This chapter presents a scenario that shows the integration between the main ITIL V3 processes. In Chapter 10, "IBM Service Management integration scenarios: Incident Management integration with Tivoli Service Request Manager and ITIL" on page 271, we saw the scenario and the description of an Incident Process. In the current chapter, we use an Incident to demonstrate the integration of the Problem Management process and Change Management process.

Our discussion takes the following five ITIL V3 core books into consideration:

- ITIL V3 Service Strategy, ISBN 0113310455
- ► ITIL V3 Service Design, ISBN 0113310471
- ► ITIL V3 Service Transition, ISBN 011331048X
- ► ITIL V3 Service Operation, ISBN 0113310463
- ITIL V3 Continual Service Improvement, ISBN 0113310498

The Problem Management process is described in the Service Operation book, and the Change Management process is described in the Service Transition book.

The application of the Change is executed through a Provisioning Task, which allows you to show the Integration between CCMDB Configuration Items and Provisioning objects.

11.1.1 IBM Tivoli Change and Configuration Management Database (CCMDB)

IBM Tivoli Change and Configuration Management Database is a platform for storing deep, standardized enterprise data. By integrating, automating, and optimizing data, workflows, and policies, it helps align the ongoing management of IT infrastructure with business priorities. CCMDB contains the core of any Service Management strategy, because it enables the standardization and sharing of information that integrates people, processes, information, and technology for real business results. It includes an open data model and helps reduce Incident and Problem Management costs.

11.1.2 Change Management

The CCMDB Change Management process enables you to manage changes from the initial request to the final review. A Configuration Item (CI) can be

chosen as a target of a Change process. The relationships between CIs can help you to understand the potential impact of the Change on other CIs. Change Management is integrated with Configuration Management process.

The Change Management process can be classified through the following Change Types:

- ► A Standard Change: A Change that follows the normal flow of subprocesses and activities defined in the Change Management process-
- A Pre-approved Change: A Change that has been pre-approved inside the Change Management process. It follows only a subsystem of the activities of a standard Change because it is a routine Change, with low risks. The impact has been evaluated before and does not change through time.
- An Emergency Change: A Change that requires an immediate intervention to establish the service again. The authorization activities of an Emergency Change can be owned by a specific group defined in the Emergency Change flow.

Some important information about IBM Tivoli Release Process Manager

IBM Tivoli Release Process Manager is the product that manages, audits, and coordinates simple and complex release tasks that need to be completed in the correct order. It allows users to assess the impact on their IT infrastructure and business-critical functions before a release, and manages software releases as a consistent and repeatable ITIL-based process to reduced time to implement and increased efficiency and productivity of the users' staff. Release Management processes faster with a set of best practice ITIL flows, and coordinates and manages releases throughout the life cycle.

This book does not include a scenario for Tivoli Release Process Manager. An extensive description of the Tivoli Release Process Manager process is available in *End-to-End Service Management Using IBM Service Management Portfolio*, SG24-7677. At the time this book was written, Tivoli Release Process Manager V7.1.1 was developed for Tivoli Provisioning Manager Version 5.1.1, when the Tivoli Provisioning Manager product was not yet integrated with CCMDB.

Today, CCMDB V7.1.1, Tivoli Service Request Manager V7.1, and Tivoli Provisioning Manager V7.1.1 share the same Base Services. The Tivoli Provisioning Manager V7.1.1 interface is integrated with the CCMDB and Tivoli Service Request Manager Interfaces. As described in this chapter, a connection is available between the Configuration Item and the Tivoli Provisioning Manager object that allows the delivery of a Tivoli Provisioning Manager Task, Software Package, or Patch on a Change process basis; this connection is based on the GUID parameter. As described before, the actual last levels of Tivoli Service Request Manager, CCMDB, and Tivoli Provisioning Manager allow integration between processes that automatically deploy with the Provisioning Application. We describe this feature later on this chapter.

At the time this book will be published, Fix Pack 5 of Tivoli Service Request Manager will be available. It allows installation of Tivoli Release Process Manager V7.1.1.5 on top of CCMDB V7.1.1.5. If Tivoli Provisioning Manager V7.x has been installed on top of CCMDB V7.1.1.5, the Tivoli Release Process Manager V7.1.1.5 installation is still possible, but Tivoli Release Process Manager V7.1.1.5 has no interaction with Tivoli Provisioning Manager V7.x.

Tivoli Release Process Manager V7.1.1.5 supports interaction with Tivoli Provisioning Manager V5.2.

For the most current information about the future direction and supported versions for Tivoli Release Process Manager, refer to the following address:

http://www-01.ibm.com/software/tivoli/products/release-process-mgr/

11.1.3 Problem Management

The Problem Management process is described in the *ITIL v3 Service Operation* book. Tivoli Service Request Manager is aligned with ITIL best practices to support Incident and Problem Management processes. As we have seen in Chapter 10, "IBM Service Management integration scenarios: Incident Management integration with Tivoli Service Request Manager and ITIL" on page 271,

the goal of Incident Management is to minimize the disruption to the business by restoring service operation to agreed levels as quickly as possible. The record of basic details described in the Incident is the information starting point for Problem Management activities.

A Problem record is created to capture an initially unknown, underlying cause of one or more Incidents. A Problem is solved when its root cause is identified, so that similar Incidents are prevented in the future or their impact is reduced.

11.2 Scenario process flow

Figure 11-1 describes the process flow defined for this scenario:

- 1. The Application Payroll has stopped, and shows a message error.
- 2. A Service Request is opened by the Self Service User.

- 3. The Service Request is accepted by the Request Manager and assigned to the Incident Owner.
- 4. The Incident is created from the Service Request as its base.
- 5. The Incident Specialist creates a Problem record to solve the root cause behind the outage. The Problem record is created from the Incident record.
- 6. The Problem is investigated by the Problem Analyst.
- 7. The Problem Analyst creates a Change to implement the problem solution: Install a software patch. The Change is created from the Problem.
- 8. The Change Manager classifies the Change and assigns it to the Change Owner. The Change Owner manages the activities of the Job Plan that are their own responsibility.
- 9. The Deployment Specialist applies the Change, and the patch is installed on the Target Server. The Problem is solved.
- 10. The Incident Specialist moves the Incident to Resolved.
- 11. The Service Request is automatically moved to Resolved.



Figure 11-1 Flow of Problem and Change Management integration with Tivoli Service Request Manager and CCMDB

11.2.1 Users of the scenario

The users involved in the scenario are:

► SRMSELFSERVICEUSR:

This is the default self service user in Tivoli Service Request Manager, member of SRMSELFSERVICE group. It maps the end user in the incident management scenario.

► PMINCOWNUSR:

This is the default incident owner user in Tivoli Service Request Manager, member of PMINCOWN group. It maps the help desk user in the incident management scenario.

► PMPRBANALUSR:

This is the default Problem analyst user in Tivoli Service Request Manager, member of PMPRBANAL group. It maps the Problem analyst user in the scenario.

► LUCAB:

This is a custom user (defined for this scenario) member of the PMCHANGEMGR group. It maps the Change Manager user in the Change Management part of the scenario.

MICHELEB:

This is a custom user (defined for this scenario) member of the PMCHANGEOWNER group. It maps the Change owner user in the Change Management part of the scenario.

► GIOVANNIB:

This is a custom user (defined for this scenario) member of the TPDEPLOYMENTSPECIALIST group. It maps the Deployment specialist user in the automatic deployment of the Change scenario.

11.2.2 Users and groups as defined in WebSphere

Users and groups are defined in WebSphere through the Integrated Solution Console, selecting from the main menu (Figure 11-2):

- Manage Users
- Manage Groups

All tasks						
ome itartup Pages Ma	anage Us	ers				
ed Activities	IM User I	Management				
ers						
ications	Search f	or Users				
rces	Search b	v *Search	for *Maximur	n results		
у [User ID	*	100			
nment	Search	1				
em administration						
rs and Groups	35 users	matched the se	arch criteria.			
dministrative User Roles	Cro	ata Da	ata la Lu		[
dministrative Group Roles			Select an	action		
anage Groups	Select	User ID	First name	Last name	E-mail	Unique Name
oring and Tuning		SIOVANNIB	Giovanni	Bianchi		uid=GIOVANNIB,ou=users,ou=SWG,o=IBM,c=US
eshooting		UCAB	Luca	Balestrazzi		uid=LUCAB,ou=users,ou=SWG,o=IBM,c=US
ce integration	1	AICHELEB	Michele	Balestrazzi		uid=MICHELEB,ou=users,ou=SWG,o=IBM,c=US
4°		MINCADMUSR	PMINCADMUSR	PMINCADMUSR		uid=PMINCADMUSR,ou=users,ou=SWG,o=IBM,c=US
ngs		MINCANALUSE	PMINCANALUSR	PMINCANALUSR		uid=PMINCANALUSR,ou=users,ou=SWG,o=IBM,c=US
	<u> </u>	MINCMGRUSE	PMINCMGRUSR	PMINCMGRUSR		uid=PMINCMGRUSR,ou=users,ou=SWG,o=IBM,c=US
		MINCOWNUSR	PMINCOWNUSR	PMINCOWNUSR		uid=PMINCOWNUSR,ou=users,ou=SWG,o=IBM,c=US
	<u> </u>	MPRBADMUSR	PMPRBADMUSR	PMPRBADMUSR		uid=PMPRBADMUSR,ou=users,ou=SWG,o=IBM,c=US
		MPRBANALUSR	PMPRBANALUSR	PMPRBANALUSR		uid=PMPRBANALUSR,ou=users,ou=SWG,o=IBM,c=US
		MPRBMGRUSR	PMPRBMGRUSR	PMPRBMGRUSR		uid=PMPRBMGRUSR,ou=users,ou=SWG,o=IBM,c=US
		MPRBOWNUSR	PMPRBOWNUSR	PMPRBOWNUSR		uid=PMPRBOWNUSR,ou=users,ou=SWG,o=IBM,c=US
		MSCADMUSR	ServiceCatalog	Administrator		uid=PMSCADMUSR,ou=users,ou=SWG,o=IBM,c=US
		MSCOAUSR	Operations	Analyst		uid=PMSCOAUSR,ou=users,ou=SWG,o=IBM,c=US
		MSCOSUSR	Operations	Specialist		uid=PMSCOSUSR,ou=users,ou=SWG,o=IBM,c=US
		MSCSDGNUSR	Service	Designer		uid=PMSCSDGNUSR,ou=users,ou=SWG,o=IBM,c=US
					- 60	

Figure 11-2 WebSphere Console

The users and groups are imported inside the Tivoli process automation engine based on a cron task execution process defined inside the CCMDB. The name of the cron task is VVMSYNC; it invokes WebSphere VVM APIs to populate database tables with user group and group membership records.

The Cron Task Application can be selected through the menu, $GoTo \rightarrow$ System Configuration \rightarrow Platform Configuration \rightarrow Cron Task Setup.

In the list page of the Cron Task Setup Application, selecting VVMSYNC task displays the panel with the Task Configuration, as shown in Figure 11-3.

	Cron Task Setup			🕞 Web Replay	Bulletins: (0)	🏫 <u>G</u> o To	In <u>R</u> eports	Start <u>C</u> enter	A Profile	<mark>≭ S</mark> ign Out	? <u>H</u> elp	IRM.
	Find:	🛱 🔝 Select Action	💌 🖏 🗟 🖉 اې	10								
List	Cron Task											
	Cron Task Class Access Level	VIMMSYNC Invokes WebSphe psdi.security.vmm.VIMSyncCronTask FULL P	ere VMM APIs to populate dat	l								
Cron	Task Instances 👂 Filter > 🎮	📋 🛊 🐳 🔶 1 - 1 of 1 🧇								E	Downloa	<u>d</u> ? ==
•	Cron Task Instance Name	<u>Schedule</u> 5m,*,*,****	r.	Run as Use MAXADMIN	<u>r</u> I P	<u>Active</u> √	Keep Histor	ĸ	Max	Number of H	listory Rec	ords 0 î
Pa	arameters History								[Duplicate	New	Row
Сго	on Task Parameters 🌗 Filter	> 🎊 📴 🝦 🍦 🔶 4 1 - 5 of 8 🤣								Eţ/	Download	? =
	Parameter *		Value				Description					
•	Credential		•••••				VMM admin cr	edentials.				
•	GroupMapping		xml version="1.0" encodi</th <th>ing="UTF-8" ?><!--DO</th--><th></th><th></th><th>The USER XMI</th><th>used by the V</th><th>MM task.</th><th></th><th></th><th></th></th>	ing="UTF-8" ?> DO</th <th></th> <th></th> <th>The USER XMI</th> <th>used by the V</th> <th>MM task.</th> <th></th> <th></th> <th></th>			The USER XMI	used by the V	MM task.			
•	GroupSearchAttribute		cn				VMM search a	ttribute to query	group recon	ds.		
•	Principal		cn=wasadmin,ou=users,ou	=SWG,o=IBM,c=US			VMM admin pri	ncipal.				
•	SynchAdapter		psdi.security.vmm.Default∨	MMSyncAdapter			VMM synchron	ization adapter				

Figure 11-3 VMMSYNC Cron Task Setup

The Schedule field shows a 5m value, which means that on a time interval of five minutes, Users and Groups defined through the WebSphere Console on LDAP Server are imported inside CCMDB. Check the **Active** box to switch on the cron task.

Users are automatically imported and defined through the VVMSYNC cron task both in the Security and People Applications.

Groups are automatically imported and defined only in the Security Application. It is necessary add the Group definition manually in **Go To** \rightarrow **Administration** \rightarrow **Resources** \rightarrow **Person Groups** (Figure 11-4), then click **New Person Group** to define it. It is important to create the New Person Group using exactly the same name defined in the WebSphere Administration Console (and imported with the same name in the Security Application).

എന്ന് Person Groups			Web Replay	Bulletins: (0)	🖻 <u>G</u> o To 💷 <u>R</u> eports	✤ Start <u>C</u> enter ▲ <u>P</u> rofile	¥ <u>S</u> ign Out ? <u>H</u> elp	IRM.
Find:	🕅 🔝 Select Action	🔽 🐌 🗟 🖉 🔷						
List Person Group								<u>^</u>
🕅 Advanced Search 🔻 🗟 S	ave Query 👻 🔗 Bookmarks							=
Person Groups 🛛 🧡 Filter > 🚜	∰ ∲ 🐳 ⇔ 1 - 15 of 15 ⇒.						E Download	2
Person Group	Description	_	G	roup Default				
REQUESTR	All Process Management Requesters		rr	naxadmin				44
PMCHGMA	All IT Change Managers							↔
PMCHGADM	Change Administrators							↔
PMCHGANA	Change Analysts							🦗 🔽

Figure 11-4 Person Groups

Note: User definitions are automatically defined through the VMMSYNC cron task on applications:

- $\blacktriangleright \quad \text{Go To} \rightarrow \text{Administration} \rightarrow \text{Resources} \rightarrow \text{People}$
- ▶ Go To \rightarrow Security \rightarrow Users

Group definitions are automatically defined through the VMMSYNC cron task on applications:

► Go To → Security → Security Groups

Then the group needs to be added on:

► Go To \rightarrow Administration \rightarrow Resources \rightarrow Person Groups

For a scheduled time interval of five minutes in the VMMSYNC schedule field, it is necessary to configure double time (10 minutes) for the cron task to complete the process.

11.3 The scenario

In the following topics, we detail the integration between Incident, Problem, and Change Management processes, and the integration between the Change Process and the automatic deployment through the Provisioning Task.

11.3.1 From Service Request to Incident

In Chapter 10, "IBM Service Management integration scenarios: Incident Management integration with Tivoli Service Request Manager and ITIL" on page 271,

we saw that the Application Payroll stopped with an out-of-memory message. A Service Request is created by the Self Service User to track the error in the Payroll Application. In our scenario, the Service Request is opened by SRMSELFSERVICEUSR (the Self Service User). See Figure 11-5.

Create Service Request	d guletnis (0) ♥ go To ULI geports ♦ Start Center ▲ Profie ★ Sign Out ? Heb 🎫 🤼
AD View Service Requests	
Create Service Request Use his form to fill out a new request for service. When you are done, select the Submit choosing/selecting an appropriate value Reported By Reported B	Juilton below to create the record. For additional details about a field description, place the cursor in the field and press Ait + F1. The loons located next to a field may be used to assist in Affected Asset Affected Asset Affected Configuration the Northed Pointy Reported Date 2009-08-06 00:03:10 Classify
Please enter a summary and a more detailed description of your Service Request. Summary Problem on Payroll System Detaile Out of Memory Message on Payroll System on Server on 17177	Use this section to choose the best classification or grouping for this request. You can do it filing the Classification or the Class Description fields. Classification [21/20106]
	Attachments #Filerow 21 + + + Cescription Pacument Attachments #Filerow 21 + + + Cescription Cescripti
Attributes > Filter > Attributes 10 1 + 10 4 + 10 + 10	🖙 Download (?) 🖻
<u>Attribute Description Data Type</u>	Abbanumeric Value Int of Measure Table Value

Figure 11-5 Service Request creation

The following steps are performed by the specified individuals:

1. The Self Service User enters information into the Service Request window and then selects the **Submit** button. A window opens (Figure 11-6) that informs this user that a new Service Request has been created.

e Service Request Submitted			813	: X	
	Service Request 1008 has been submitted. Record your Service Request for future reference,				
View Details	Return to Start Center	Create Another S	ervice Request		

Figure 11-6 Service Request submission

2. In this window, the Self Service User can see details about the Service Request. Return to the Start Center or create another Service Request, as shown in Figure 11-7.
| View Service Requests | Buletos: (0 |) P Go To Le Reports P Start Center Profile Sign Out ? Help IEFE. |
|--|---|--|
| | | Contractor Contractor of Contractor |
| 2 Create Service Request | | |
| | | |
| Service Request 1008 | • | 🖡 Previous Record 🛛 🌳 Next Record 🕴 🕮 Search 🛛 👾 Print View 🕴 🎌 Route Workflow |
| | | |
| Service Request Id 1008 | Classification | 21/2101/210106 |
| Status NEW | Classification Description | Il Issue (Haroware (Other |
| Asset | Summar | Problem on Payroll System |
| Configuration Inc. 117477 DOMELOR IT INV COM. 457 | Detait | Out of Memory Message on Payroll System on Server nc117177 |
| Toronal Contract | | |
| Target Contact | | |
| Target Sight | | |
| Reported Date 2009-08-08 00:03:10 | | |
| Reported Priority 3 | 0. | |
| | 電算 Download Remote Diagnostics Agen | |
| Attributes 🐌 Filter 👬 😂 🛧 🐳 🐟 | | 🕞 Baymland ? 🗖 |
| Attribute Description Data Type Alphanumeric Value | Numeric Value Unit of Measure Section | n Inherited from Apply Down Hierarchy |
| | No rows to display | |
| Attachments > Filter > 66 [20] + + + +> | | 🕞 Bownlood ? 📼 |
| Document | Description | |
| | No rows to display | |
| | | Attach File Attach Web Address Link |
| Log > File: > Al D + + + + + | | Gr Domitord 1 ? |
| Created By | Date \$ | Summary |
| | No rows to display | |
| | | Add Log Entry |
| Solutions : Filter > A 12 1 + + + + | and the second se | Greenbert 1 ? : = |
| Originator Originating Class | Relationship | Solution Description |
| | No rows to display | |
| | | |
| | | |

Figure 11-7 Service Request Details

As discussed in Chapter 10, "IBM Service Management integration scenarios: Incident Management integration with Tivoli Service Request Manager and ITIL" on page 271, the Service Request is received and accepted by the Service Request Manager and assigned to the Incident Owner. See Figure 11-8.

All Open Service	Requests	🔻 Filter 🗃 🖍					/ = 1
Internal Priority	<u>Owner</u>	Owner Group	Service Request	Status	Summary	Target Finish	Target Start
1			1011	QUEUED	Experiencing bad performance of Intranet web		
			1008	NEW	Problem on Payroll System		
Set Graph Options	<u>8</u>						1 - 2 of 2

Figure 11-8 Start Center: List of All Open Service Requests

3. The Incident Owner recognizes what is described by the Service Request as an Incident and creates the Incident using the Service Request window; in this way, a relationship is created between the Service Request and the Incident. The Incident Owner creates the Incident by selecting Select Action → Create → Incident. A message is displayed for two seconds stating that the Incident is being created. See Figure 11-9.

Note: Starting from this point, the Incident is linked to the Service Request. You can view this relationship by clicking the **Related Records** tab.

Service Requests			C Web Replay P Bulletins: (0)	🕈 💁 To 🕮 Reports 🕈	Start Center & Profile X Sign Out ? Help	IBM.
Find:	n 🕫 🔝 Select Action 💌 🔞 🚮	🖉 🔶 🔶 🖓 🖓 🖉	ا 🔬 🕲 🔛 😭 🔊 🖓	🎌 i 💷 🚭		
List Service Request Rela	ted Records Solution Details Log	Specifications				
Service Request 1008	Problem on Payroll System		Site	P	Status NEW	
Related Tickets 🕨 Filter > 🖄 😂 🛊	↓ ↓ + 1 - 1 of 1 +				S ¹ Downlog	ad ? =
Related Record Key *	Description		Class	Status	Relationship	
1010	Problem on Payroll System		INCIDENT 🔎	NEW	FOLLOWUP	Û
					Select Ticket Nev	w Row

Figure 11-9 Service Request and Incident related record

11.3.2 From Incident record to Problem and Change record

The Incident record is used to document a deviation from an expected standard operation. In our scenario, the Incident Owner decides to use the Problem application and create a Problem record to capture the root cause of the Incident.

The Problem record, as with Service Requests and Incidents, is a type of ticket. In our scenario, it is possible to define a relationship between tickets by performing the following steps:

- 1. The Incident Specialist recognizes the record as a Problem and decides to open a Problem record to track it.
- From the Incident window, the Incident Specialist selects Select Action → Create → Problem. A new Problem is created that has a relationship with the Incident. See Figure 11-10.

Incidents			Ulletins: (0)	na <u>G</u> o To <u>III R</u> eports	* Start <u>C</u> enter * Profile	×Sign Out ?Help IEM.
Y Find:	et Action 🛛 🖌 👔 📄 🧶 i 🍬 🖬	🔶 i 🗯 🎎 🗟 🏨 i ời ời 🤞	🔊 i 🔿 i 🔂 📖 🕱 👍 i 🔂 i 🎌			
List Incident Activities Related Rect	Change Status Failur View History	re Reporting Specifications				
Incident 1010 Own Sour	View Costs Edit History Incident Create Servi	ice Request	Owner Group Created By PMINCOWNUSR	Status	QUEUED	Attachments 🖉
User Information	Apply Incident Template Incide	lent	Affected Person SRMSELFSERV			=
Name Service Phone Phone Phone	Select Owner Take Ownership Chan Modify/Delete Work Log Show Similar Tickets Work	nge ase k Order	Name Service Phone P E-mail		/	
Incident Details	Apply SLA Solut	tion				=
Summary Problem on Payroll System Details Out of Memory Message on Pay	View SLAs Comr Select/Deselect SLAs Catal Attachment Library/Folders > Catal	munication cess Request log Requisition	Classification Classification Path Class Description		م م	
Asset	Duplicate Incident Delete Incident Add to Rookmarke		Indicated Priority Reported Priority Impact	3 p		
Location Configuration item NC117177.ROMELAB.IT.IBM.CO	Workflow Show Known Error		Urgency Internal Priority			
GL Account	Manage Downtime History Run Reports		Service Group Service			
Asset Site			Site			
			SLA Appled? Create WO Options	MULTI P		
Dates				= GI	obal Issues	=
Reported Date 2009-08-10 20:14:29 🔊	Target Contact	#C	Actual Contact	Č	Global issue?	
Affected Date 2009-08-10 20:14:29 🚯	Target Start		Actual Start	6	Related to Global ID	
Creation Date 2009-08-10 20:14:29	Target Finish	10	Actual Finish	õ	Global Class	a,
Multiple Assets,Locations and CIs > Filter > 🚸 🗇 🛧	+ +++					🕞 <u>Download</u> i ? i 🗖
Asset Location	Configuration Item	Target Description			Sequence Progress	Site
		Ne rows to display.			Select : 🔻	Clear All New Row

Figure 11-10 Problem created starting from Incident record

3. When the Problem is created, a message (<u>BuxAAttor</u>) polyeotocreated) is displayed for two seconds at the top of the window. As Incident Specialist, if you select **Related Records**, you can view both the Service Request that originated the Incident record and the Problem record opened by the Incident, as shown in Figure 11-11.

	ncidents						P <u>B</u> ulletins: (0)	Co To 🛄 Repor	is 🌴 Start <u>C</u> ent	er ¹ Profile ¹	× <u>S</u> ign Out	⁹ Help IBM.
	~	Find:	🆍 🤝 Select Action 🛛 💌 🐌 🗔 👌	LI 🔶 🔶 I 🛟 I 🤮	🖁 🗳 🐠 🖄 🍅 🔊	I 🕞 📖 🙎	🗠 ا 🔬 ا 🐿					
List	Incident	Activities	Related Records Solution Details Log	Failure Reporting	Specifications							
In	cident 1010		Problem on Payroll System			Or Originatir	iginating Record Ig Record Class	1008 /		Status QU Site	EUED	ρ
Relate	l Tickets 🛛 🕨 F	ilter > Mail [21]									D/	Download ? =
	Related Record	d Key 🕈	Description			Class		Status		Re	lationship	
	1003	1	Problem on Payroll System			PROBLEM	I 🔎	NEW		FO	LLOWUP	Û
•	1008	1	Problem on Payroll System			SR	P	QUEU	ED	OF	RIGINATOR	Û
										Sei	ect Ticket	New Row
Relate		> Filter > //i	D + + ++								DF.	Download ? =
	Work Order 🗢		Description		Class		Status		Relationship			
					No rows to display					Select Wor	k Order	New Row

Figure 11-11 Incident related tickets

4. The Problem is investigated by the Problem Analyst. In our scenario, the Problem Analyst is PMPRBANALUSR, who analyzes the Problem, and sees that the Incident was defined with a Reported Priority of 3. The Problem Analyst updates it by assigning an Impact of 2 "High" and an Urgency of 2 "High", and notes that the application automatically assigned an Internal Priority of 1 "Urgent". See Figure 11-12.

Indicated Priority		
Reported Priority	3 🔎	
Impact	2 🔎	High
Urgency	2 🔎	High
Internal Priority	1	Urgent

Figure 11-12 Impact and urgency definition

- 5. The Problem Analyst determines that is necessary to install a software patch to solve the memory problem on the target server. To manage and trace the patch installation, it is necessary to open a Change Record.
- Before creating the Change, the Problem Analyst defines the site of the Problem record, because this information is needed to create the change. Otherwise, a window is displayed, prompting for the Site field selection (site ROMA).
- 7. The Problem Analyst opens the Change record from the Problem record to maintain automatically the relationship between them. See Figure 11-13.

Problems			⁹ <u>≘</u> uletins: (0)	▶ <u>G</u> o To ^{IIII} <u>R</u> eports ▶ Start <u>C</u> enter ▲ <u>F</u>	rofile × Sign Out ? Help IEM.
List Problem Activities Related Rec	Select Action 🖌 🔞 📻 🖉	LI 🔷 🔶 I 🛟 I 🎎 🗟 🗐 I 🌣 🕉			
Problem 1003 Own Sour	View Costs Edit History Problem	Service Request	Owner Group Created By PMINCOWNUSR	Status NEW	Attachments Ø
User Information Reported By SRIISELFSERV # Name Service Phone Phone E-mail	Apply Problem Template Select Owner Take Ownership Modify/Delete Work Log Show Similar Tickets	Incident Problem Change Release Work Order	Affected Person SRMSELFSERV		-
Problem Details Summary Problem on Payroll System Details Out of Memory Message on Pay	Apply SLA View SLAs Select/Deselect SLAs Attachment Library/Folders >	Solution Communication Process Request Catalog Requisition	Classification Classification Path Class Description Indicated Priority		_ م[م
Asset Asset Asset Asset Configuration Rev NC117177.ROMELAB.IT.BM.CO	Delete Problem Add to Bookmarks		Reported Priority Impact Urgency Internal Priority Service Group	3 P 2 P High High 1 Urgent	
GL Account Asset Site Is Known Error?	manage downlane riskoly		Service Vendor Site SLA Appled?		
Dates Reported Date 2009-08-14 07:30:11 Affected Date 2009-08-14 07:30:11 Creation Date 2009-08-14 07:30:11 Creation Date 2009-08-14 07:30:11	Target Contact	10 10 10	Actual Contact	Global Issues Global Issues Related to Gk	essue?
Multiple Assets Locations and Cls # Filter > 21 Asset Location	Configuration Rem	Tarcet Description No rows to disple	y	Sequence Progress	Clear Al New Row

Figure 11-13 Change created from the Problem record

8. When the Change is created, a message (<u>BMXAA4321E - Change 1000 created</u>) is displayed for two seconds at the top of the window. Selecting **Related Records** shows that the Service Request originated from the Incident record and the Problem record originated from the Incident.

If you select the **Related Record** tab, you can view the Records that have a relationship with the Problem. In our scenario, the Incident Analyst creates a Change using the Problem, so both the Incident record in the Related Tickets row and the Change record in the Related Work Order row are visible in the Related Record tab, as shown in Figure 11-14.

Problems		 Bulletine: (0) 	^{¢e} <u>G</u> o To ^{IIII} <u>R</u> eports ₱ Start <u>C</u> ent	er ⁴ <u>P</u> rofile [*] Sign Out ? Help IBM,
Find:	🕅 🖙 Select Action 🛛 💌 👸 🖼 🧟 💠 🔶 🛟	I 🎎 🗟 🌒 I V V 🖉 🧶 🕓 I 🔂 📖 💈 🤷 I 💁 👘		
List Problem Activities	Related Records Solution Details Log Failure Report	ing Specifications		
Problem 1003 Problem	m on Payrol System	Originating Record 1	1010 # INCIDENT P	Status NEW
Related Tickets 🕴 🕨 Filter > 🙈 🗄 🚍 🕴 🔶				📴 Download ? 🚍
Related Record Key ≑	Description	Class	Status	Relationship
1010	Problem on Payroll System	NCIDENT 👂	QUEUED	ORIGINATOR
				Select Tickets New Row
Related Work Orders 🕴 🕨 Filter > 🚜 🗄 📰 📋				Download 1 ? =
Work Order 🗢	Description	Class	Status	Relationship
1008	Problem on Payroll System	CHANGE 🖉	WAPPR	FOLLOWUP
			(Select Work Orders New Row

Figure 11-14 Problem related records

- 9. The Change Manager approves the change, classifies it as a Software Change on a J2EE Business Server Application, and assigns the Change to the Change Owner.
- 10. The Change is approved by selecting Select Action → Change Status in the Change window or by clicking the Change Status icon . A new window is displayed that shows the Change Status update. See Figure 11-15.

🗣 Change Status				
Change 1008 Status WAPPR	Problem on Payroll System Waiting on Approval]
New Status * Status Date * Memo Print Work Order(s)?	Approved Canceled In Progress Waiting on Material Waiting on Plant Cond	ок	Cance	1

Figure 11-15 Change Status Approved

Figure 11-16 shows the Number of active Changes that are visible on the Start Center window of the Change Owner user MicheleB (the Change has been assigned to that person).

Number of active Changes 🔻 Filter > 🏟 🚍 褅			2 = 1
Chart Type: PIE			View By: Owner
	Owner	Value	Percent (%)
All active Changes (By Owner)	MICHELEB	1	100
List View			

Figure 11-16 Chart Type Pie for the change

The graphic Chart Type of the Start Center can be selected clicking it. Depending of the area selected, it shows the Changes related to the selection.

11.Depending on the Classification applied, the specific Job Plan that needs to applied to the Change is associated to the Change. In our scenario, we chose a Pre Approved Job Plan. See Figure 11-17.

6 Changes			S Web Rep	olay 🧧 Bulletins: (0) 🎓 Go To 🔤 Bepo	rts 🕈 Start Center 🌲 Profile 🗡 Sign O	ut ^o Help IEM.
Find: 🖌 🕅 🔝 Se	lect Action 🛛 💌 👌 🔒 🧶 I 💠	🔶 i 🤃 🎎 🗟 i 🌣 🖞) () 🗸 📖 🥥 🗙	(1🖳 1 🔭 1 🗉 🖶		
List Change Plans Related Records	Actuals Log Specifications	Process Details	mpact Analysis			
Change 1008 Problem on Payroll S Parent Problem on Payroll S Job Plan CHG-P-F2 Pre-Approved JobPl	an 🗐			Supervisor // // // // // // // // // // // // //	Status APPR Site ROMA]
Children of Change 1008 🎽 Filter > 🚧 🗐 🛊 👙 🔶 1	-3 of 3 🔶					By Download ? =
Sequence Record Record Class	Summary Schedule	Class ACTIVITY	Asset Lo	Configuration Item NC117177.ROMELAB.	T.BM.COM~457	R 🗘 🗊
▶ 2 1051 # ACTIVITY	Provisioning Task : Patch Installation			NC117177.ROMELAB.	T.BM.COM~457 # WAPP	R 🚺 📋
	Post implementation Review	General General	te Activity Schedules	Select Assets Select Loca	tions Select Work Orders	New Activity
Tasks for Change 1008 🔰 Filter > 🚜 📋 🛊 🐳 🛶 🚽						🕞 <u>Bounlead</u> ? ==
Sequence =	Task Summary	No rowe t	Estimated Duratio	on <u>Status</u> <u>Owner</u>	Owner Group	
			, and and a second s		Generate Task Schedules	New Row
Labor Materials Services Tools						
Labor 🎽 Filter > 🏤 🗇 🔶 🔶 🔶 🔶					1	* texnicad ? =
Task Craft Skill Level	Vendor	Qua	ntity Labor	Regular H	tours Rate	Line Cost
		No rows t	o display		Select Craft	Ilew Row

Figure 11-17 Job Plan

12. The Change Owner adds, as the target CI of the Change, the Server that will be the target for Patch distribution. In our scenario, the target is NC117177.ROMELAB, as shown in Figure 11-18.

6 Changes		Norace And		😫 <u>B</u> ulletins: (0) 🕐 Go To 🛛 🗠	Reports 🌴 Start Center 🌲 Profile	×Sign Out ? Help IEN
Find:	th 😎 Select A	Action 💌 🚹 🖃 🗔 🕼 🍁 I 🏥			Sales Service S	
List Change Plan	ns Related Records	Actuals Log Specifications	Process Details Impact Analysis			(
Change 1008	Owner MICHELEB	Owner Group	Status WAPPR	Progress		Attachments 🖉
Change Details						-
Summary	Problem on Payroli System			Classification	PMCHG \ PMCHGSFW \ BUSAPPL \ J2	EEBSVA 🌶
Parent	1			Class Description	J2EE Business Server Applications	P
Asset	7			Priority		
Location				Priority Justification		=
Configuration Item	NC117177.ROMELAB.IT.IBM.COM	~457 🎤		Service Group	P	
GL Account	P			Service	#	
Target Description				Vendor	<i>A</i>	
Asset/Location Priority				Site	ROMA	
Change Type	P			SLA Applied?		
Reason for Change				Under Flow Control?	\checkmark	
Verification				Suspend Flow Control?		
Risk Assessment				Flow Action	P	
Back Out Plan				Flow Action Assist?		
				Launch Entry Name		1
				Predecessors		1
				BPEL Enabled?		
				BPEL In Progress?		
Source Cls 🕴 🕨 Filter > 🚜 🕴 🚍	1 + 1 + +					🕞 <u>Goverload</u> i ? i 🚍
<u>Cl number</u>	Description	Classification	Source Description		Sequence + Pro	gress
			No rows to display			
					Select	Clear All New Row
Target CIs, Assets and Local	lions 🕨 Filter > 🖄 🛱 🔶 🔶	⇔1-1of1⇒				🛤 <u>Download</u> ? 🚍
Asset	Location	Configuration Item	Target Description		Sequence Progress Sit	0
F	1	NC117177.ROMELAB.IT.IBM.COM~457	1		R	MA 🔎 🗊
					Select : 🔻	Clear All New Row
Dates						

Figure 11-18 Change, selection of the Target CI

13. To add the target CI, click Select and then select CIs → Select Value in the *Target CI, Assets, and Location* Change row. The square selection on the left allows you to add one or more CIs. See Figure 11-19.

Search Asset Hierarchy Search Location Hierarchy	F Status Classification	NOT READY		User [Custodian [Refine
🎔 Filter > 🆓 👔 🛊 🍦 🔶 ሩ 1 - 10 of 10 ⇒				Cł,	Download ?
Configuration Item	Description		Asset	Site	Status
					=NOT READY
NC117175.ROMELAB.IT.IBM.COM~2					NOT READY
NC117218.ROMELAB.IT.IBM.COM~117					NOT READY
NC125095.ROMELAB.IT.IBM.COM~230					NOT READY
NC117217.ROMELAB.IT.IBM.COM~341					NOT READY
NC117177.ROMELAB.IT.IBM.COM~457					NOT READY
NC117175.ROMELAB.IT.IBM.COM~115					NOT READY
NC117218.ROMELAB.IT.IBM.COM~229					NOT READY
NC125095.ROMELAB.IT.IBM.COM~340					NOT READY
					NOT READY

Figure 11-19 CI selection

11.3.3 From Change to software patch deployment

The connection between Tivoli Provisioning V7.1.1 and CCMDB and its related applications is the Provisioning Object from CCMDB. See Figure 11-20.

Configuration Items			C Web Repla	y 9 <u>B</u> ulletins: (0)	* Start <u>C</u> enter <u>Profile</u>	× <u>S</u> ign Out ? <u>H</u> elp	IBM.
Y Find:	🛱 : 🔝 Select Action	🖞 🔒 🖉 🔄 🛊 🎼 🎼 🔮)				
List Configuration Item	Related Cls						
Configuration Item Classification	NC117177.ROMELAB.IT.IBM.COM~457 CLTOPCICLASS \ CLSYS.WINDOWS.WINDOWS				Attachments Status	Ø NOT READY	
Class Description	SYS.WINDOWS.WINDOWSCOMPUTERSYSTEM				CI Location	<i>•</i>	
Asset	#				Site	P	
Location		=			Organization		
item		=			Item Set	P	
Service	P	=			Calendar	٩	
Service Group	A	=			Shift	P	
Actual CI	NC117177.ROMELAB.IT.IBM.COM~457				CI Owner	P	
Provisioning Object	2A978E3C949134DE8DB22A7D515D441D	nc117177.romelab.it.ibm.com			Change Window	1	
					Change Number	e e	

Figure 11-20 Configuration ITEM - Provisioning Object field

CCMDB Provisioning Object 2A978E3C949134DE8DB22A7D515D441D has the same value as the Globally Unique Identifier (GUID) in the Provisioning Application, as shown in Figure 11-21.

Provisioning Computers					↑ <u>R</u> eturn	IEM.
Find: A Select A	iction 🛛 🔽 🚯 🛃 🛃 🖉 🖓	4 4 A				
List Computer Hardware Software	Compliance Recommendations	Credentials Workflows Variables D	Deployment Properties			^
Computer* nc117177.rc	melab.it.ibm.com					
Globally Unique Identifier 2A978E3C94	9134DE8DB22A7D515D441D					
Configuration Item NC117177.R	OMELAB.IT.IBM.COM~457	Ξ.				
Configuration		🗖 Last Known S	Status			-
		Operations				
Management IP Address	9.168.117.177		Framework	Scalable Distribution Infras		
Operating System	Windows Server 2003 En		Agent	TCA-1.4.2.0		
Computer Template	P		Agent Status	Running		
Locale	English_United States.125					
Details						
Model Type		Compliance				
Architecture	intel		Security	Configuration required		-
Serial Number	VMware-56 4d da e4 9f 7		Software	0 issues 🥒		
Manufacturer	Phoenix Technologies LTD		Patches	Configuration required 🥒		
Static Drovinianing Crowney 1 Subject 40 1 Miles 2 1 4 4 4	at divis				Bandadi	21.00
State Provisioning Groups : # rine: 7.94 ; a ; # V ; # rin	01 T - P	Description		Ture	-/ Download :	
Static Provisioning Group Windows Application Servers		Description		Computer	â	
				A CONTRACT	Assign to Static Group	
					Addigin to citato proop	
Dynamic Group Association						

Figure 11-21 Provisioning Application

As defined in Change Job Plan, the sequence of activity and task is shown in Figure 11-22.

	Sequence ≑	Record		Record Class	Summary	
•	1	1047	1	ACTIVITY	Schedule	
•	2	1051		ACTIVITY	Provisioning Task : Patch Installation	
•	3	1060		ACTIVITY	Post Implementation Review	

Figure 11-22 Sequence of activity for Change 1008

After Activity 1, *Schedule* is completed, Activity 2, *Provisioning Task: Patch Installation* is managed by Deployment Specialist GiovanniB.

Go to the **Changes** application in the **Plans** tab, where you can select Activity 2 by clicking the arrow key it to the right of Sequence 2 of the activity, then click the **Go To Activities and Tasks** button. In our scenario, the Activity record number is 1051.

Deployment Specialist GiovanniB has the responsibility to apply, starting from the Change Application, the appropriate Provisioning Task to solve the Memory Problem on Server NC117177.ROMELAB that stopped the Payroll Business Application.

The Activity, *Provisioning Task: Patch Installation*, has been classified as TPTASK\TPPATCHINSTALL. This Classification has been configured to automatically insert TPCREATASK into the Assisted Workflow field. See Figure 11-23.

Activities and Ta	sks						↑ <u>R</u> eturn	IBM.
	Find: Select Action	💌 🖬 🖉 🔷 🔶 🕄	ାକ୍ଷି 🖪 ାହି ହାର୍ଚ୍ଚା 🗸 ।	📖 🎯 🗙 i 🚉 i 🎌 i 🗦 🔗				
List Activities and	d Tasks Plans Actuals Re	lated Records Log						^
Task	ACTIVITY Provisioning Task : Patch Installe	ition		Activity Type	1051 P	Attachments Status Status Date	Ø WAPPR 2009-08-16 23:14:59	
Asset	/			Reported By	SRMSELFSERV #	Service Group	8	
Configuration Item	NC117177.ROMELAB.IT.IBM.COM~457	2	8	SLA Applied?		Service	7	
Target Description				Under Flow Control?	✓	Owner		
Classification	TPTASK \ TPPATCHINSTALL	<i>A</i>		Suspend Flow Control? [Owner Group		
Class Description	Patch Installation	P		Flow Action	1	Assisted Workflow	TPCREATASK 🖉	
Launch Entry Name Parent Process	1008	8		Flow Action Assist?		St	art Assisted Workflow	

Figure 11-23 Job Plan Activity

The Deployment Specialist selects the Start Assisted Workflow button.

The application switches automatically to the Patch Installation Application, where, in the row Selected Targets, nc117177.romelab.it.ibm.com has been automatically included as the target of the Patch Distribution based on the Configuration Item Provisioning Object - GUID correspondence, as shown in Figure 11-24.

Patch Installation	O Web Replay 🔒 Buletina: (0) 🐣 Go To 🔐 Reports 🔶 Start Center 🎍 Profile	×Sign Out ?Help IBM.
Patch Installation		^
Provisioning Task* Install Patch 2,607		
Reboot if required?		
Commit Patch?		
Distribute Before Installation?		
Selected Patches Filter > A 2 + + + + + + +		Bownload i ? i =
Patch Vendor	Version Build Number	
	No rows to display	
		Select Patches
	Validate Targets?	=
Selected Targets + + + + 1 - 1 of 1 +		By Download ? =
Target	Description	
nc117177.romelab.it.ibm.com	Computer	×
		Select : 🔻

Figure 11-24 From Assisted Workflow to Provisioning: Patch Installation

From the Patch Installation window, the Deployment Specialist clicks the **Select Patches** button to select the identified patch that solves the problem on the payroll system. The patch has been defined previously in the Provisioning Repository.

In our scenario, we define the new patch manually, but the Provisioning platform allows us to download patches automatically from official patches catalogs for the operating system, as explained in Chapter 13, "Patch Management scenarios" on page 371.

To define a new patch manually with its related definitions and code selection, select **Go To** \rightarrow **IT Infrastructure** \rightarrow **Software Catalog** \rightarrow **Patch**. See Figure 11-25.

Patches O Web Replay B guterns: (0) P Go To A Reports + Start G	center * Profile * Sign Out ? Help IBM.
💌 Find: 🔰 🎁 💌 Select Action 🔍 👀 🄁 🚚 🖉 ! 🌳	
List Felch FielSets Advanced Targets Tasks Workflows Variables	
Patch Patch for Payrol Application	
Last Known Status	
Approval Status * Approval	
Vendor Supplied Details	
Severity High 🗸	Restart application?
Version 1.0	Can request reboot?
Build 1.0 Release Date	Patch can coexist?
Static Provisioning Groups > Filter > A 20 + + ++	Download ? =
Static Provisioning Group DescriptionNo rows to display	Type
Dynamic Group Association	Addigit to State Group

Figure 11-25 Patch definition

To verify that the patch has been installed successfully, go to the Provisioning Task Tracking window, as shown in Figure 11-26.

Provisioning Task Tracking				New Providence		A Return
Find:	No. Select Action		nanananan Malanini ana ana ana ana ana ana ana ana an	And a Market state of the second state of the	Contraction of the second second second	
List Task	(
Provisioning Task Install Patch 2,639				Definition	Install Patch 2,639	2
Type Patch Installation				Start Date	2009-08-26 03:34:13	
Created By GIOVANNIB				End Date	2009-08-26 03:34:19	
Changed By				Status	Success	
changed by				Base Services Task		· · ·
Provisioning Workflows > Filter > # D	∳ # +1=1 of 1 →					By Download ? =
Provisioning Workflow	Status		Start Date	End Date	Concurrency Lev	el Subtask
SoftwareModule.Install	Succeeded	1	2009-08-26 03:34:15	2009-08-26 03:34:19		5 Install Patch 11,443
Notification						=
Recipients > Filter > 00 121 1 + + 1 + +						Br travelogit 121
Recipient						<u></u>
			No rows to display			
Events > Filter > 4 0 + + ++						Gewaleed ? =
Event Type						
			No rows to display			
Patches > Provisioning Task Tracking						

Figure 11-26 Provisioning Task Tracking

The Problem Specialist PMPRBOWNUSR moves the Problem to Resolved. See Figure 11-27.

الله المعالم معالم المعالم المعالم المعالم المعالم مالي المعالم معالم معالم معالم معالم						
Find:	🖍 🔝 Select Action	V 🐌	3 🖉 🖗	🌢 I 🛟 I 🎇 🖳	0 0 10 0	Ø 🔿 🕞 🛄
List Problem Activit	ies Related Records Solution	🖣 🛡 Chang	e Status	and a second second		□ : ? : ⊠
Problem 1003	Owner Source	_				
User Information		Problem	1003	Problem on F	Payroll System	
Reported By SRMSE	LFSERV 🎤	Status	INPROG	In Progress		
Name Service	e	New	Status * Resolv			
Phone	P	Statu	s Date 2009-0	8-26 07:21:41		
E-mail			Memo		-	
Problem Details						
Summary Problem	on Payroll System 📃					
Details Out of M	emory Message on Payroll System on Serve	r			0	Cancel

Figure 11-27 Problem resolved

The Incident Specialist move the Incident to Resolved. See Figure 11-28.

Incidents			
×	Find: Select Action	💌 🐌 🝙 🖉 । 💠 । 🛟 🖏 🛃 🌒 🕉 🌝 🤗	
List Incident	Activities Related Records Solution I	Details Log Failure Reporting Specifications	
Incident 1010	Owner PMINCOWNUSR Source	Change Status	⊟ : ? : ⊠
User Information			
Reported By	SRMSELFSERV #	Incident 1010 Problem on Payroll System	
Name	e Service	Status INPROG In Progress	
Phone		New Status * Resolved	
E-mai		Status Date 2009-08-26 07:27:29	
Incident Details		Memo	
Summary	Problem on Payroll System		
Details	Out of Memory Message on Payroll System on Server	ОК	Cancel

Figure 11-28 Incident resolved

The Service Request that originated the process is moved automatically to Resolved. Figure 11-29 shows, in the Incident Related Tickets row, that the Service Request 1008 in the Relationship chain is the Originator and has been automatically moved to Resolved, as shown in Figure 11-29.

Incidents					↑ <u>B</u> eturn IBM.
Find:	n Select Action 💌 🚼 🛃 🤌 I 🧇	🔹 😂 🕹 🕲 🔅	🖉 na	۲.	
List Incident Activities	Related Records Solution Details Log Fai	lure Reporting Specifications			
Incident 1010	Problem on Payroll System		Originating Record Originating Record Class	1008	Status RESOLVED
Related Tickets 🕴 🕨 Filter > 🏤 🗄 🚍 🕴	÷ 🍦 ÷ 1 - 2 of 2 ⇒				By Download ? =
Related Record Key 🗢	Description		Class	Status	Relationship
) 1003 🎤	Problem on Payroll System		PROBLEM 🔎	RESOLVED	FOLLOWUP
▶ 1008 J#	Problem on Payroll System		SR 🔎	RESOLVED	ORIGINATOR

Figure 11-29 Service Request resolved

12

Tivoli Provisioning Manager integration methods with non-IBM solutions

In the previous chapters, we saw the various integration scenarios for Tivoli Provisioning Manager with other IBM Service Management components such as Tivoli Service Request Manager and TADDM. While fully leveraging the IBM Service Management portfolio provides end users with the quickest time to value, because many of the integrations are fully developed and tested together, we recognize that customer environments are diverse, and that leveraging Tivoli Provisioning Manager for automation and other capabilities might require integration into a complex infrastructure of tools and processes.

In this chapter, we describe the primary methods for Tivoli Provisioning Manager integration, their advantages and disadvantages, and the various IBM solutions that can help incorporate Tivoli Provisioning Manager's automation capabilities to create more streamlined and effective processes.

We describe the following integration patterns:

- "Functional integration" on page 350
- "Data integration" on page 362
- "Data federation" on page 366

We also discuss the following tools and solutions:

- "Tivoli Provisioning Manager workflows" on page 352
- "Tivoli Provisioning Manager Web Services, SOAP Services, and SOAPCli" on page 359
- "Tivoli Provisioning Manager data importing/exporting capabilities" on page 363
- "IBM Tivoli Integration Composer (ITIC)" on page 365r
- ► "IBM InfoSphere Federation Server" on page 367

12.1 Introduction to various integration methods

In today's complex IT environments, most users employ a large set of tools and solutions to maintain productivity among a growing set of software and hardware assets. Even the seemingly simple process of bringing up a new server might require interaction with multiple data sources and tools in the enterprise environment. Because Tivoli Provisioning Manager helps streamline and automate IT processes, most implementations of Tivoli Provisioning Manager will require some form of integration with existing IT tools and data sources. While the type and degree of integration is usually different for each customer based on their environment and needs, the following three types of integration methods are common and prevalent as noted in our experiences.

Functional integration: This is a service oriented type integration where Tivoli Provisioning Manager is utilized as the automation component providing a set of services that other components in the IT process call to perform work. In turn, Tivoli Provisioning Manager can invoke services or APIs of other tools and components in the environment as part of the provisioning action. Although data updates to the calling component and components that Tivoli Provisioning Manager will affect change on are possible, the focus is on well defined services and APIs, and direct data updates should be limited.

An example of functional integration would be the Change Management IBM Service Management scenario described in Chapter 9. The Deployment Specialist executes the change by the <u>Start Assisted Workflow</u> button. Tivoli Provisioning Manager receives the appropriate instructions to execute the actual patch installation on the target machine. The result of the operation along with a descriptive status is returned to Tivoli Service Request Manager and the Deployment Specialist. In this case, Tivoli Provisioning Manager does not directly update the data for the changed CI in the CCMDB. The change to the CI is processed and made by the calling Tivoli Service Request Manager application.

Data integration: In this integration method, data on the IT environment is synchronized among the various tools and components by manual or scheduled export and import operations. While this method does not require any functional interaction of the components, it does require data mapping between the components and data synchronization. This type of integration is usually performed point to point, requiring a data source and a data sink.

An example of data integration is the TADDM Tivoli Provisioning Manager integration discussed in Chapter 10, "IBM Service Management integration scenarios: Incident Management integration with Tivoli Service Request Manager and ITIL" on page 271. In this case, TADDM discovers information about the environment and Tivoli Provisioning Manager imports that data by a TADDM Discovery. After the data has been imported, Tivoli Provisioning Manager can now manage these IT systems independently of TADDM. If Tivoli Provisioning Manager makes changes to these systems, TADDM will not be aware of the changes until another TADDM Discovery is run on the affected systems.

Data federation: This integration method can be thought of as an evolution of data integration. The focus of this method is to provide a singular view of the IT environment and all its encapsulated data without forcing a consolidation of that data into a single data model or a single data source. Tools and components can still operate using their own data model for the IT environment while a Data Federation Server keeps all the shared data synchronized.

In the previous TADDM-Tivoli Provisioning Manager example, if a Data Federation Server existed with knowledge of both the Tivoli Provisioning Manager Data Center Model and CCMDB, it is possible for the CIs to be automatically updated even when users make to a change directly with Tivoli Provisioning Manager. Furthermore, if multiple tools maintain information for a data center object, such as a server, then if one of these tools makes a change to the server's attributes, a Data Federation Server is able to ensure that the set of attributes for all the tools that maintain them will get updated.

In the following sections, we provide more detail for each of these integration methods and tools that can help integrate Tivoli Provisioning Manager into an existing environment.

12.2 Functional integration

As discussed in 12.1, "Introduction to various integration methods" on page 349, the key characteristic of functional integration is the focus on Tivoli Provisioning Manager's services and APIs and the ability for Tivoli Provisioning Manager to invoke other tools' services and APIs in turn. In this section, we further explore the following topics:

- Advantages and disadvantages of functional integration
- Tivoli Provisioning Manager workflows
- Tivoli Provisioning Manager Web Services, SOAP Services, and SOAPCli

12.2.1 Advantages and disadvantages of functional integration

The major advantage of utilizing a functional integration approach is that the tools and components of the IT process involved are directly communicating. The data that each tool maintains on the IT environment is kept up to date in near real time. In the example described in Chapter 9, if the patching of the server encounters a problem, Tivoli Service Request Manager and the Deployment Specialist monitoring the progress of the change will be notified when the result is reported by Tivoli Provisioning Manager to Tivoli Service Request Manager. There is no concern that the data viewed from a specific tool managing the environment is not the most current. This is especially important in the cases where multiple data sources are involved in the automation task.

Consider a simple view of provisioning a new server. For example, Tivoli Provisioning Manager might need to:

- Request a new IP address lease from the DHCP server
- Create a new DNS host entry with the new IP
- Request new SAN storage for the server
- Update an asset database with ownership information

If these steps are not functionally integrated, problems will occur as the various components begin to lose data consistency. For example, if Tivoli Provisioning Manager does not request a new IP from the DHCP server for the new server but instead allocates one on its own, DHCP IP conflicts might start to occur because the DHCP server might have already allocated Tivoli Provisioning Manager's allocated IP to an existing server.

The major disadvantage of functional integration is that all the components involved need to provide a minimum set of services and they need to understand and utilize each other's services. In the previous list of provisioning steps, all the listed components need to have well defined and accessible services, and Tivoli Provisioning Manager must be able to understand and leverage them. This is usually not a problem for well known technologies such as requesting a new IP from a DHCP server. However, most users have specialized tools that can make this type of integration more complex and implementation intensive than pure data integration. With this type of integration, usually some development will be needed.

An additional disadvantage of a purely functional integration approach is that all the work is usually done in band. Look at the last step in the above example. If updating the asset database with the new server information is time intensive, then the overall provisioning process will take more time. If we were to employ data integration on the last step and synchronize the ownership information on a nightly basis, for example, we can save time on the actual provisioning process.

12.2.2 Tivoli Provisioning Manager workflows

Tivoli Provisioning Manager workflows are designed to help make it easy to functionally integrate Tivoli Provisioning Manager into an existing environment. These workflows are scripts that can perform meaningful provisioning actions. They are not to be confused with business process workflows that are part of the Tivoli process automation engine.

While we cannot fully cover all of the capabilities and benefits that Tivoli Provisioning Manager workflows provide users, we discuss some of the key examples of their benefits below. They include:

- Automation Package Development Environment
- DCMQuery
- Logical Management Operations:
 - Device.ExecuteCommand
 - SoftwareModule.Install
- Scripts and scriptlets

Automation Package Development Environment

Automation Package Development Environment (APDE) is an Eclipse based development environment that ships with Tivoli Provisioning Manager. APDE provides a graphical environment where users can easily extend existing workflows or create completely new workflows in order to more consistently and effectively execute common IT tasks. See Figure 12-1.

As a development environment, APDE provides many advanced capabilities, such as:

- Auto-completion for all known Tivoli Provisioning Manager functions, registered workflows, and object attributes.
- Powerful tools such as:
 - An object browser to see what is known in the data center
 - A query tester to help new users develop new data center queries
- A live compiling and debugging environment directly connected to a Tivoli Provisioning Manager server.



Figure 12-1 APDE running on Red Hat Enterprise Linux server

Some areas of note in the foregoing figure are the context highlighting in the main workflow development pane and the Query pane in the lower right showing how users can incrementally refine and test queries to retrieve data stored in Tivoli Provisioning Manager's DCM for provisioning actions.

DCMQuery

In Example 12-1, we see the following line in the workflow development pane.

```
Example 12-1 DCMQuery
```

var serverName = DCMQuery(/server[@id=\$ServerID]/name)

Although the example itself is simple, this line shows one of the most powerful capabilities of Tivoli Provisioning Manager workflows. It demonstrates how Tivoli Provisioning Manager workflows can easily query and leverage known data center information for provisioning operations. Because Tivoli Provisioning Manager's data center model (DCM) stores an extensive amount of information about the datacenter, collected by various direct and indirect discoveries,

this single function enables users to create highly customized and situational relevant provisioning actions. A simple example would be to leverage this function to look up and check for complex software and hardware dependencies on a server before installing a particular application.

Logical Management Operations

For users experienced with Tivoli Provisioning Manager, Logical Management Operations (LMO) is the new terminology used for what was called Logical Device Operations in the 5.x and earlier releases of Tivoli Provisioning Manager. While the name has changed, the concept of an LMO is still the same. Tivoli Provisioning Manager is designed to support an object view of the data center, and LMOs are just generic, well defined operations that are supported by a set of data center objects. In general, we do not distinguish an LMO with the actual Tivoli Provisioning Manager workflow that implements its function. A very simple example would be the LMO *Device.PowerOn*. This simple LMO defines the operation that Tivoli Provisioning Manager can invoke on data center devices that support it to physically turn them on. The primary value of the LMO feature is that:

- It allows Tivoli Provisioning Manager to consistently define supported operations to a similar group of devices, subsequently providing a structured approach to extending such capabilities and allowing users to extend such capabilities themselves over time.
- It allows Tivoli Provisioning Manager to compose more complex automation operations from smaller, more well defined base operations on data center objects and increasing overall code reuse.
- It allows Tivoli Provisioning Manager to simplify end user operation of the environment. For example, the actual process for installing the well known applications, Firefox and WebSphere Application Server is quite different in complexity and the actual installation and configuration. However, end users installing these applications do not necessarily need to understand and deal with the underlying complexity outside of providing some basic configuration parameters for these applications.

In this case, LMOs allow Tivoli Provisioning Manager to present installation of software as a very simple operation of selecting the software, the targets, configuration options, schedule, and notification. Tivoli Provisioning Manager will then automatically perform the correct installation actions necessary that can involve using different communication protocols to access the target, utilizing different binaries for the applications on the different platforms, and so on.

Next we discuss two frequently used LMOs in Tivoli Provisioning Manager for provisioning and automation:

- Device.ExecuteCommand
- SoftwareModule.Install

Device.ExecuteCommand

This LMO defines the operation of executing a command to a physical device. Although this seems to be a simple LMO, it enables users to execute a command on a device and obtain the command's output for processing without having to deal with the underlying technologies involved. For example, if we want to run a command to check for a locked file on the target system, we can use the following workflow snippet to accomplish the task (Example 12-2).

Example 12-2 A simple example of using Device. ExecuteCommand

```
var DeviceId = 1234
var Command = "ls -al /tmp/filelock.lck"
var WorkingDir = "/tmp"
var CredKey = "default"
var Timeout = 300
var TimeoutType = "error"
var ReturnCode
var ReturnMsg
var ReturnResult
Device.ExecuteCommand(DeviceId, Command, WorkingDir, CredKey, Timeout,
TimeoutType, ReturnCode, ReturnMsg, ReturnResult)
```

In this example, some initial variables are configured, and then a call to the LMO is made. The user can then obtain the return values, in the *ReturnCode*, *ReturnMsg* and *ReturnResult* variables, without having to deal with the underlying details such as the communication protocol used for executing this command. This demonstrates how LMOs allow Tivoli Provisioning Manager to easily interact with managed devices.

SoftwareModule.Install

We have already discussed how these LMOs allow Tivoli Provisioning Manager to provide abstraction and extensibility for software installation. Figure 12-2 and Figure 12-3 show a specific implementation of the LMO and the single installation panel that this capability enables in Tivoli Provisioning Manager.

Provisioning Wo	orkflows	🗘 Web Replay	P <u>B</u> ulletins: (0)	🏞 <u>G</u> o To	<u>I</u> <u>R</u> eports	Start <u>C</u> ente	er 🌲 <u>F</u>
×	Find: Select Action	💌 🏷 🥑	💠 🔶 🔒				
Workflows	Status						
isioning Workflow	IBMWAS_SoftwareModule_Install						
itomation Package	IBM-WebSphere-App-Server						
Source Code	 # Licensed Materials - Property of IBM # 5724-F75 # (C) Copyright IBM Corp. 2003 - 2009 # All Rights Reserved # US Government Users Restricted Rights -Use, dupled disclosure restricted by GSA ADP Schedule Contra # prepare the install SRT log debug Jython("prepare SRT") # call Defait SM install or custom install log debug Jython("default install") Default_SoftwareModule_Install(SoftwareIgnoreFunctionalValidation) # run IBMWAS discovery log debug Jython("WAS discovery") var discoveryID = DCMQuery(/Discover Discovery OnDevice(discoveryID, Devi 	lication or act with IBM Corp. vareModuleID, in So tule.Install LocaleIns areModuleID, Softw ceID)	rftwareInstallation) sensitive vareInstallationMec ebSphere Discove	ViechanismiC :hanismiD, D ry"])), in DeviceID, leviceID, Soft	, in SoftwareRe wareResourceT	source 'emplate

Figure 12-2 The IBMWAS_SoftwareModule_Install workflow which implements the SoftwareModule.Install LMO

Note that in this implementation of *SoftwareModule.Install*, a default workflow is called to handle the normal process of narrowing and finding a more specific *SoftwareInstallable.Install* workflow to actually perform the software installation.

However, after the installation process is complete, an additional call is made to discover the installed WebSphere environment. This call will gather additional information about application server instances and other configuration data on the WebSphere Application Server installation that just completed. This demonstrates how extensions to common IT operations can be quickly added in the Tivoli Provisioning Manager automation environment. For example, if users need to extend installations to acquire/report on licenses, users can easily add the necessary calls before and after the installation operation to get that effect.

Software Product Installation	U 🕑 Web Replay 🛛 🕈 Bulk	etins: (0) 🏾 🕈 <u>G</u> o To	Let Reports T Start Center	A Profile 🕺 Sign Ou	t ? Help <u>IR </u> i
Software Installation		an a			
Details					
Provisioning Task* Install Software 1400					
Selected Software 👔 🛊 🖕 1 - 1 of 1 🌩					Download ?
Software Module			Vendor	Version	
IBM WebSphere Application Server V6 FP2.11 🥒			IBM	6.0.2.11	×
					Select Software
				/alloate Targets?	
			Targets missing sel	ected software?	
Selected Targets 🔺 🔹 🗢 1 - 1 of 1 🗰					Download ?
Target Description					
lele01 Computer				×	
					Select 🖉 🔻
Scheduling					
Click Schedule to change options.					
Scheduled: Now					Schedule
Notification					
Recipients 🎽 Filter > 🏨 😂 🛧 🛊 🐳 1 - 1 of 1 🌩					Download 2
Recipient					
MAXADMIN				×	
				Add Recipient	Add E-mail
Events 19 Filter > de 10 1 & 11 4 4		and the second			• Revolued 2 C
Description					20210425-2
	No rows to dis	play			
					Add Event
	anning and the second				
Lask settings for sealable distribution innastructure	and maximum work time for	the exclusion distribution	n a la frantsval vez		
Set the task priorit	y and maximum wait time for	the scalable distribution	on intrastructure.		
Priority 3	and the second s				
Maximum Wait Time 2	. Week		~		
					Submit

Figure 12-3 Software installation application in a single page, hiding underlying implementation differences and complexity

Scripts and scriptlets

Most users already have a good amount of reusable assets that help implement change in their IT environment in the form of shell scripts. Tivoli Provisioning Manager provides a mechanism for reusing these scripts through a set of device logical management operations.

Example 12-3 is taken from the Tivoli Provisioning Manager InfoCenter Product Guide:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp

It demonstrates how the Device.CopyFile and the Device.ExecuteCommand can be leveraged to execute existing scripts in the management environment.

Example 12-3 Running existing scripts on managed targets

```
var init_command = "configdb.sh"
#Copy the file
Device.CopyFile(TI0_Server_ID, tools_dir, init_command, Server_ID,
tmp_dir, init_command, "default", "300")
#Run the command.
try
   log info "Running initialization script"
   Device.ExecuteCommand(Server_ID, init_command, "/tmp", "default",
   "120", "error", <null>, <null>, <null>)
catchall
   log info "Error initializing the server."
endtry
```

Other than being able to execute existing scripts. Integrating existing scripts into Tivoli Provisioning Manager also provides the following additional value:

- All Tivoli Provisioning Manager workflows execute in a specific user context. This provides more centralized auditing information about script execution.
- Tivoli Provisioning Manager abstracts the server identifier field to generalization of workflow execution. It is possible to allow users to select individual targets or even groups of targets as values for these identifiers. Then existing scripts can be automatically iterated and run on these targets without the user having to manually run them separately.
- The device logical management operations provide the ability to execute under different configured credentials. Without having the actual credentials, users can run scripts with administrative, normal user, and guest credential on managed systems, depending on their access to Tivoli Provisioning Manager.
- Integrating existing scripts and calling them with Tivoli Provisioning Manager also allows for a centralization of scripts in the management environment. It minimizes the chance that scripts are dispersed on different servers and repositories in the data center.

Beyond leveraging external scripts. Tivoli Provisioning Manager also provides a way for users to create scripts directly within the workflow language. Example 12-4 shows a typical Tivoli Provisioning Manager scriptlet. This further enable users who are familiar with scripting on the manage platforms to easily create and execute them within the Tivoli Provisioning Manager environment.

Example 12-4 A simple Tivoli Provisioning Manager bash scriptlet

```
var greeting = "This is a simple example."
scriptlet(greeting) language=bash <<EOSCR
echo ${greeting}
EOSCR</pre>
```

Note that all the contents within the <<EOSCR and EOSCR delimiters are just the normal content for a bash script.

12.2.3 Tivoli Provisioning Manager Web Services, SOAP Services, and SOAPCIi

We have discussed some of Tivoli Provisioning Manager's tools in leveraging its data center model information to more intelligently, easily, and effectively implement changes to the managed environment. In this section, we see some of the capabilities that Tivoli Provisioning Manager provides to facilitate external tools and solutions in accessing Tivoli Provisioning Manager and these automation features.

External tools can functionally integrate with Tivoli Provisioning Manager primarily through three means:

- The first method is Tivoli Provisioning Manager's Web Services Resource Framework (WSRF) services enabled in an OSGi environment. This method provides external requesting application with Tivoli Provisioning Manager resource access by stateful Web services. This is the deepest level of integration providing requesters with direct, stateful Tivoli Provisioning Manager objects to work with.
- The second method is Tivoli Provisioning Manager's SOAP Services, which is a more decentralized Web services model. The requester and Tivoli Provisioning Manager still exchange structured information and request by SOAP over HTTP, but no stateful services are kept by the requester.
- The third method is Tivoli Provisioning Manager's SOAPCli. This is a set of command line interfaces that help create a SOAP services request for applications, or even scripts that might not have the ability to directly work with SOAP and Web services.

Utilizing stateful Web services might be the most integrated approach because the requester of the service has more direct access to Tivoli Provisioning Manager's Web services and can maintain state between requests. However, it is usually also the most costly approach in terms of integration because it requires modification to the requester application. For more information about this approach, we would recommend starting by looking at the sample WSRF client applications found in the Tivoli Provisioning Manager product documentation:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp?topic =/com.ibm.tivoli.tpm.soa.doc/wsrf/cwsr_wsrfsv.html

The decentralized and stateless request model of SOAP services provides a more agile and on demand approach to invoking Tivoli Provisioning Manager capabilities. If the requesting application needs to provision a patch to a target server, it makes a single SOAP Service Request to activate a corresponding workflow in Tivoli Provisioning Manager. If the requesting application then requires an update to the patch progress, it makes another SOAP Service Request to retrieve that information. All the information is maintained by the requester, and SOAP Service Requests are only made as needed to execute work or retrieve information.

Tivoli Provisioning Manager provides a set of Web Services Description Language (WSDL) services to define groups of SOAP services that can be accessed. The WSDL services include:

- ► TpmLiteSoapService
- CredentialsManagerService
- GroupManagementService
- EffectiveModeService
- OperationsModeService
- FaultManagementService
- RecommendationsService
- ResourceInformationService
- TpmEventBrokerService

Of these WSDL services, the *TpmLiteSoapService* set of *deployment engine* related SOAP services provide the most common integration services. A user can visit the following URL to get the actual WSDL for *TpmLiteSoapService*:

http://YourTPMServerName:8777/ws/pid/TpmLiteSoapService?wsdl

Some of the more commonly used SOAP services under *TpmLiteSoapService* include:

- executeDeploymentRequest: This is a generic SOAP service to start any Tivoli Provisioning Manager workflow using a set of passed in parameters. The output is a task identifier of the task executing the workflow.
- findDeploymentStatus: This SOAP service retrieves the status of a task given a Tivoli Provisioning Manager task identifier.
- findLogDetails: This SOAP service retrieves the log details for a given task.

Tivoli Provisioning Manager's *soapcli* script is the primary command line interface to Tivoli Provisioning Manager's SOAP services. This script can be found in the following location on the Tivoli Provisioning Manager server as shown in Figure 12-4.

•	Windows
	<pre>%TIO_HOME%\soapclient\tpmlteSoap</pre>
•	UNIX and <u>Linux</u> :
	<pre>\$TIO_HOME/soapclient/tpmlteSoap</pre>

Figure 12-4 Location of soapcli script on Tivoli Provisioning Manager server

Example 12-5 shows how you could use the *soapcli* script to invoke executeDeploymentRequest SOAP service to activate a Tivoli Provisioning Manager workflow call, myworkflow.

Example 12-5 Using soapcli to kick of a Tivoli Provisioning Manager workflow

```
soapcli username password
"http://localhost:8777/ws/pid/TpmLiteSoapService?wsdl"
executeDeploymentRequest
myworkflow
"param1=value1,param2=value2,param3=value3"
```

Using this method, scripts and other management tools can easily invoke any available Tivoli Provisioning Manager workflows to perform the desired automation task.

12.2.4 Functional integration summary

In 12.2, "Functional integration" on page 350, we discussed the various capabilities that Tivoli Provisioning Manager provides to functionally integrate into an existing environment. Capabilities such as the Tivoli Provisioning Manager workflows and Logical Management Operations allow Tivoli Provisioning Manager and users to easily access the managed environment and to interact with existing management tools. Other capabilities such as WSRF Web Services, SOAP Services, and SOAPCIi allow other managements tools in the environment to easily and quickly leverage the provisioning and automation capabilities of Tivoli Provisioning Manager.

12.3 Data integration

In this section, we discuss integration of Tivoli Provisioning Manager into an existing environment following the data integration approach. Topics covered in this section include:

- Advantages and disadvantages of data integration
- Tivoli Provisioning Manager Data importing/exporting capabilities
 - DCMExport/xmllmport
 - IBM Tivoli Discovery Library Adapter
- ► IBM Tivoli Integration Composer

12.3.1 Advantages and disadvantages of data integration

The major advantage of utilizing data integration when implementing Tivoli Provisioning Manager in an IT environment is the ease and the time savings of the approach. Because there is no need to integrate on a functional level, neither Tivoli Provisioning Manager nor any other components in the environment need to be modified to understand the other's data model and APIs. Integrating on a data level simply requires a mechanism to manually or periodically synchronize the shared data maintained by the management solutions in the environment. This is especially true when there is a singular, centralized data source, such as a CMDB, in place.

The major disadvantage to integration on a data level is that not all of the data sources might contain the most updated information at a given time. For example, suppose that data between Tivoli Provisioning Manager's DCM and an existing CMDB is synchronized on a nightly schedule. If an emergency change is needed and performed during the day by Tivoli Provisioning Manager, the CMDB then might not contain the most updated information about the environment for part of the day. While some real time methods can be applied, such as keying synchronizations based on database triggers, this might introduce other problems, such as these synchronizations impacting the performance of the running systems. Keeping various management solutions in the environment with the current information is a potential concern and issue when integrating on a data level.

12.3.2 Tivoli Provisioning Manager data importing/exporting capabilities

Tivoli Provisioning Manager DCM objects can be represented in XML format. Tivoli Provisioning Manager offers several data integration features by leveraging this capability. This includes data center model object import/export capabilities to/from XML files. Additionally, Tivoli Provisioning Manager also has the ability to export data center objects to XML, using an alternative schema, by a set of Discovery Library Adapter workflows.

DCMExport and XMLImport

These two command line scripts can be found on the Tivoli Provisioning Manager server in the directory, **TI0_HOME/tools**.

The usage of these scripts is shown in Figure 12-5 and Figure 12-6.

Syntax	
Windows	dcmexport.cmd -d output_file_name
> UNIX	dcmexport.sh -d output_file_name
Figure 1	2-5 dcmexport usage

Syntax	
Windows xmlimport.cmd file_URL	
UNIX Linux xmlimport.sh file_URL	

Figure 12-6 xmlimport usage

A sample XML file of what an exported data center might look like is provided with Tivoli Provisioning Manager. Users can find this **venice.xml** file in the directory, **TIO_HOME/xml**.

With the ability to import and export the Tivoli Provisioning Manager DCM objects in XML format, the sample **venice.xml** file can be used to generate mapping that will allow Tivoli Provisioning Manager DCM XMLs, possibly with the help of XSLT tools, to be converted to the target management solution's schema for import and vice versa.

Note: Two additional tools to import and export data are made available with Tivoli Provisioning Manager V7.1.1. These are **ccexport** and **ccimport**. They are used to export or import compliance checks that defined for individual computers or for groups of computers.

Discovery Library Adapter

Tivoli Provisioning Manager provides a set of workflows that make up the Discovery Library Adapter. This set of workflows will scan the DCM for selected objects to be exported into an XML file using the common data model schema.

Figure 12-7 shows the usage flow for Discovery Library Adapters. The steps in orange and circled are the ones supported by Tivoli Provisioning Manager. The other steps represent how other management solutions can leverage Discovery Library Adapters to perform data integration with IBM CCMDB.



Figure 12-7 Discovery Library Adapter usage flow

As with the data center model XML file created by dcmExport, users can directly map this DLA generated XML file for consumption by other management solutions or even create a Discovery Library Reader[™] to handle the generated XML. Again, common XSLT tools can help with these transformations.

12.3.3 IBM Tivoli Integration Composer (ITIC)

IBM Tivoli Integration Composer is another tool that helps with importing IT data from a data source to a target data store. Although it is geared towards integrating products running on Tivoli process automation engine platform, the shipped mapping files are targeted for those products, it can be used in some situations as a more generic data integration tool.

With IBM Tivoli Integration Composer, users can:

- Create data source definitions with connection parameters for data import/export.
- Create mappings that define how to transform data instances from a data source to a target data store.
- Perform the data transformation and import.

For more information about ITIC, refer to the following URL in the Tivoli Service Request Manager:

http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/topic/com.ibm.s
rm.doc_7.1/installing/src/c_ccmdb_icoverview.html

12.3.4 Data integration summary

In 12.3, "Data integration" on page 362, we discussed some of the advantages and disadvantages of integrating Tivoli Provisioning Manager into an existing environment by data integration. We described some of the built-in capabilities of Tivoli Provisioning Manager such as dcmExport, xmIImport, and the Discovery Library Adapter for performing data integration. We also covered IBM tools such as IBM Tivoli Integration Composer which is another option for data integration.

Finally, there are other IBM solutions for data integration such as Tivoli Directory Integrator. The tools and options covered in this section are not meant to be the only ones, or necessarily even the best options. In each individual environment, just as you would evaluate and decide whether to integrate on a functional or a data level, you should examine the environment and pick the right solution for data integration if it is the right integration option.

12.4 Data federation

Data federation is the natural evolution of the data integration approach as discussed in 12.3, "Data integration" on page 362. Where as the simplified data integration approach has the goal of keeping the common data synchronized and consistent, the goal of a data federation server is to provide a consolidated view of data in support of key business processes and decisions. This difference can be seen in the following simple example (Table 12-1).

Computer Attributes	Computer (Tool A)	Computer (Tool B)	Computer (Federated)
Hostname	\checkmark	~	~
IP Address	\checkmark	\checkmark	✓
Hardware Inventory	√	X	\checkmark
Software Inventory	х	✓	✓

Table 12-1 Data synchronization versus data federation

In this example, the data integration approach would only operated on the fields *Hostname* and *IP Address* because they are the common attributes for a computer object between the two management tools. If one of these fields changes, synchronization must occur to keep this common data consistent. In this same environment, no action would be taken if Tool A updates the *Hardware Inventory* of a computer because it is not common data. However, to a data federation server, all the attributes are important because a single change in any of the computer attributes can directly impact the global, federated view of the computer object.

Next, we discuss data federation as a data integration strategy for implementing Tivoli Provisioning Manager. We cover:

- Advantages and disadvantages of data federation as an integration strategy
- ► IBM InfoSphere™ Federation Server

12.4.1 Advantages and disadvantages of data federation

There are many obvious advantages to implementing data federation in a complex IT environment. Some of the key ones are:

- Consolidated view of IT assets in the enterprise, enabling better information and decisions in key business processes
- Centralized view of all IT assets speeds up new business application deployment
- ► Improved security and consistency of data through centralized management

With data federation providing so many benefits, the only disadvantage to implementing such a system is that the effort can be complex and costly. Such a project might become a greater effort than the initial Tivoli Provisioning Manager integration issue, and that is the only disadvantage to this method.

12.4.2 IBM InfoSphere Federation Server

IBM InfoSphere Federation Server is an enterprise data federation server. It is beyond the scope of this guide to fully explain all the benefits and capabilities of the IBM InfoSphere Federation Server. We list here some of the capability highlights directly from the IBM product Web site:

- Gain virtualized real-time access to disparate data sources
- Speed time to market for new projects
- Access more data sources
- Extend your warehouse or mart with remote data
- Build holistic, unified financial, customer, or product views

If the data federation approach is a viable option, we strongly recommend visiting IBM product Web sites to get more information about the IBM InfoSphere Federation Server.

Additionally, the following guides are helpful references when working with InfoSphere Federation Server:

- IBM DB2 Universal Database Administration Guide for Federated Systems, SC19-1020
- WebSphere Information Integration: Application Development Guide for Federated Systems, SC19-1021

They can be found at the following IBM.com Web site:

http://www.ibm.com/shop/publications/order



Part 4

Patch Management, Operating System Deployment, and IBM Tivoli Monitoring agent for Tivoli Provisioning Manager

With version 7.1.1, Tivoli Provisioning Manager V7.1.1 has seen some important enhancements in the Patch Management and Operating System Deployment areas.

In this part of the book, we cover these enhancements and go over some typical scenarios that you can implement in your production environments. We also provide an overview of the IBM Tivoli Monitoring Agent for Tivoli Provisioning Manager.

370 IBM Tivoli Provisioning Manager V7.1.1: Deployment and IBM Service Management Integration Guide
13

Patch Management scenarios

In this chapter we provide an overview of the enhancements to Patch Management in Tivoli Provisioning Manager V7.1.1.

We cover the following topics:

- "Changes and improvements to Windows and UNIX Patch Management capabilities" on page 372
- "Patch Management in small Windows environments" on page 372
- "Patch Management in large Windows environments" on page 380
- "Patch Management in AIX environments" on page 396
- "Patch Management in SUSE Linux Enterprise environments" on page 404

Note: For more information about Patch Management in Tivoli Provisioning Manager version 7.1.1, you can refer to:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp?to
pic=/com.ibm.tivoli.tpm.scenario.doc/patch/ccom_overview.html.

13.1 Changes and improvements to Windows and UNIX Patch Management capabilities

Patch Management was not changed significantly in Tivoli Provisioning Manager version 7.1.1. New in version 7.1.1 is the support for Patch Management for Red Hat enterprise Linux version 5 and enhancements for Solaris and HP-UX target computers.

This version supports scalable Patch Management on Linux RHEL 5 target computers using the scalable distribution infrastructure.

Also new with this version, the Patch Management solution for SUSE Linux environments has been enhanced to use the **rug** command-line tool, provided with SLES 10 operating systems.

Patch Management is now also supported for HP-UX environments using Software Assistant (SWA).

For Sun Solaris environments, the Patch Management solution has been improved for using Sun Update Connection Enterprise.

13.2 Patch Management in small Windows environments

A small environment from a Tivoli Provisioning Manager perspective is a Windows environment that requires managing patches for a small number of desktop computers (fewer than 20). Tivoli Provisioning Manager uses Microsoft Windows Server Update Services (WSUS) to manage patches in these environments. See Figure 13-1.



Figure 13-1 Patch Management for small environments

The solution requires a Microsoft Windows Server Update Service (WSUS) machine connected to the Internet for downloading the patches from Microsoft. The required version is WSUS v3.0 with installed .NET Framework 3.5.

Target computers belong to Provisioning Groups. An association between the WSUS Server and the provisioning group allows verifying systems for installed patches and installation of approved patches. Multiple groups can point to the same WSUS server. To update the WSUS server itself, it must be allowed to direct obtain patches from the Microsoft Update Web site.

If there are more than one WSUS server in the environment, then at least one machine must have direct access to the Microsoft Update Web site. This can then be the source for the other WSUS servers.

The Windows Update Agent (WUA) resides on the target computers and is used for comparing installed patches with a list of patches that should be installed. It can be configured so that clients download patches either direct from the Web or from the WSUS server. If the target computers use a proxy server to connect to the Internet, then the connection settings from Internet Explorer are used to authenticate on the proxy server. The supported Windows Operating Systems for WUA are

- Windows Server 2008 Standard Edition (x86 32-bit and 64-bit)
- Windows Server 2008 Enterprise Edition (x86 32-bit and 64-bit)
- ► Windows Vista Ultimate Edition (x86 32-bit and 64-bit)
- ► Windows Vista Enterprise Edition (x86 32-bit and 64-bit)
- ► Windows Server 2003 Standard Edition SP2 (AMDTM 64-bit)
- Windows Server 2003 Enterprise Edition SP2 (AMD 64-bit)
- Windows Server 2003 Standard Edition SP2 (x86 32-bit and 64-bit)
- Windows Server 2003 Enterprise Edition SP2 (x86 32-bit and 64-bit)
- ► Windows XP Professional (32-bit and 64-bit) any Service Pack

13.2.1 Predefined roles for Patch Management

Tivoli Provisioning Manager has some predefined roles for Patch Management. Here is a short overview:

- The Provisioning Administrator is responsible for setup and configuration of servers and infrastructure as well as discovery and groups of target computers.
- The Provisioning Configuration Librarian acquires patches, scans target computers for missing patches, organizes and maintains the patch catalog, creates and maintains patch groups, and also can delete patches from the data model.
- The Compliance Analyst can approve patches in the data model and is responsible for setup compliance, performing patch checks, approving, and verifying compliance.
- The Deployment Specialist can install patches on target computers, publish, distribute, and unpublish patches, implement compliance recommendations to install missing patches, monitor patch installations, and also uninstall patches from targets.

13.2.2 Requirements for Patch Management

Here are the requirements for implementing Patch Management in Tivoli Provisioning Manager:

- On the target computer, you need to install a Tivoli Common Agent (TCA) to take advantage of all Patch Management features.
- If no TCA is planned to install on the target computers, then OpenSSL and OpenSSH should be configured for a secure communication between server and targets.

- If OpenSSH is used, Version 4.4 and higher are recommended, using password authentication. There are some problems with OpenSSH Version 4.3.
- To associate the WSUS server with the target computers, a variable named "WSUServer" with the value "http://<WSUS_server_name>:<port_number>" or "https://<WSUS_server_name>:<port_number>" is required, where WSUS_server_name is the name of the WSUS server. This computer must already exist in the data model.
- If using the https:// notation, the target computers have to trust the certificate from the WSUS server.
- If the global variable is not set, the Windows Update Agent will try to directly connect to the Microsoft Update Internet site to search for and install the latest patches for the Windows Operating System. If the variable is set, but has a wrong value, then the error shown in Example 13-1 is seen.

Example 13-1 Error if variable WSUServer has a wrong value

```
COPCOM123E A shell command error occurred:
Exit code=1, Error stream="",
Output stream="different WSUS in registry
different WUStatusServer in registry
Restarting Automatic Update
Scanning...
```

Scan failed. Cannot connect to WSUS server."

If the variable is set correctly, then the Windows Update Agents contact the WSUS server to search for updates and download the patches if approved.

13.2.3 Web Replay scenarios

To simplify the Patch Management process, some Web Replay scenarios that are shipped with Tivoli Provisioning Manager V7.1.1 can be used for tasks such as these:

Discover Computers (Compliance category).

Run initial discovery and assign the discovered computers to a new group or an existing group.

Install WUA on Target Computer (Compliance category).

Installation of Windows Update Agent on a group of computers to enable Patch Management on Windows.

Windows Patch Acquisition (Compliance category).

Patch Acquisition into the data model.

Patch Compliance (Compliance category).

Approving patches in the patch catalog, set up an Operating System Patches and Updates compliance check for a group of computers, and run discovery and compliance checks to report missing patches.

Recommendation Approval (Compliance category).

View and approve compliance recommendations for a group of computers.

Remediation (Compliance category).

Schedule remediation for approved recommendations for a group of computers.

Discovery and Agent Installation (Agent category).

Creation of an Initial Discovery wizard and run Discovery followed by installation of the common agent.

To run a Web Replay scenario, click **Web Replay**, if the panel is not yet displayed at the bottom of the window. On the Web Replay panel, click the appropriate category in the *Categories* field. Right-click the scenario and select **Run**.

13.2.4 Patch Management in small Windows environments

For the Windows Patch Management scenario in small environments, the automation package, *MS_WSUS*, is used for distributing packages with either the deployment engine or the scalable distribution infrastructures (SDI).

The following operations can be performed:

- Download Windows Update Agent.
- Install Windows Update Agent.
- Scan for missing patches on the target computer
- Scan for missing patches on the target computer.
- Distribute the missing patches to the target computer.
- Install the missing patches on the target computer.

Follow the steps as indicated by the scenario to perform the task.

The MS_WSUS automation package provided by Tivoli Provisioning Manager includes the workflow MS_SOA_GetWindowsUpdateAgent.

This workflow helps to automate the process of downloading the Windows Update Agent executable and storing it in Tivoli Provisioning Manager's local file repository. The location is \$TI0_HOME/repository/wua/windowsupdateagent. After running that workflow to acquire the Windows Update Agent, users can install the software product on multiple Windows endpoints by scheduling the software install from Tivoli Provisioning Manager's Web interface.

Generally, you have to do the following steps for Patch Management on Windows computers:

- 1. Make sure that target computers are known in DCM.
- 2. Make sure that target computers are grouped.
- 3. Update WSUS to download information about all available patches from Internet
- 4. Approve the patches on the WSUS Server.
- 5. Scan for missing patches on target computers. This is done with a compliance check and generates a list of missing patches for every endpoint respectively target computer.

Note: The compliance scan running on target computers discovers and reports as missing only the patches that have been approved on the WSUS server previously.

Patches not been marked as approved on the WSUS will not be considered for the scan, and therefore will not be listed as missing.

For the Compliance Scan, perform the following steps:

- 1. Select Go To \rightarrow Deployment \rightarrow Provisioning Groups.
- 2. Select the group of target computers, open it, and click the **Compliance** tab.
- 3. Click **New Compliance Check** → **Patch Check**. By default, all approved patches are verified on target computers.
- 4. Click Save.

Note: To automatically approve recommendations when they are generated, click **Enable Automatic Approval** and click **OK** in the message box. All recommendations that are generated by this compliance check will be created in the Approved state.

Now a new Compliance Check is created and can be executed as follows:

- 1. Click Go To \rightarrow Deployment \rightarrow Provisioning Groups.
- 2. Select the group of target computers.
- 3. Click the **Compliance** tab.
- 4. Click Run and select from the drop down list Scan and Check.
- 5. On the *Provisioning Task Tracking* page, click **Refresh** to update the task status and see when the task is finished.

Note: The difference between **Check** and **Scan and Check**, which can be selected from the drop-down list on the **Run** button, is that the check reads the already existing information from the database and scans the target computer.

The workflow *MS_WUA_Scan* is invoked and the .vbs Script wua.vbs is send to the target computers if RXA protocol is used.

The script is copied to directory %WINDIR%/tmp and is executed with:

cscript //Nologo wua.vbs 1 http://wsus_fully_qualified_name
wua_missing_updates_device_id

The results are collected in the file wua_missing_updates_device_id and data are uploaded in DCM (if necessary). If a patch is Approved on the WSUS, it will be uploaded (if not already present in the DCM) and its status is set as Approved.

Approval of recommendations

To approve compliance recommendations, click Go To \rightarrow Deployment \rightarrow Provisioning Groups.

Select the group of target computers and then the **Recommendations** tab. In the recommendations list, select the check boxes corresponding to the missing patches that have to be approved and click **Approve**.

As a result, the selected patches are displayed with a status of *Approved* on the *Recommendations* tab.

Installation of missing patches on all required target computers

The Patches can be distributed and installed within a single task, but it is also possible to separate the distribution from the installation step. The installation is done based on the patch recommendations,

The patches can be installed by using a software stack, but it is also possible to install individual patches on a group of endpoints. Here is the sequence:

- 1. The Logical Device Operation *ComplianceRecommendationGroup.Remediate* is invoked.
- 2. Workflow *Default_Compliance_Recommendation_Group_Remediate* is started
- 3. A Software Stack containing the approved patches is created and then the workflow *MS_WUA_Install_Updates* is invoked.
- 4. This workflow creates a script named wua_updates_XXXXX.vbs, where xxxxx is the device ID of the target.
- 5. This script is downloaded onto the target and executed. It contains a list of the patches to install on the target. An example is given in Example 13-2.

Example 13-2 Sample content of wua_updates_xxxx.vbs

ArrayOfUpdates(0) = "d3ac165e-d7c4-4bdf-83f0-e249ecbe8734" ArrayOfUpdates(1) = "336530d3-9ae4-42df-9606-4fb35d46cefc"

ArrayOfUpdates(8) = "33a7edf1-2350-4102-8082-9540eff65722"

- 6. The patches are retrieved from WSUS Server and installed on the target computer.
- 7. If a reboot is required, it is done as the last step when script ends.
- 8. Then the WUA scan checks for additional updates after installation, using the workflow MS_WUA_Scan.

Verification of patch installation

After installing patches, the patch compliance can be verified for endpoints. In the **Group's recommendations** tab, the Status column shows the installation status. The column shows Implemented for the patches that were installed successfully.

13.2.5 Patch Management in large Windows environments

The scalable distribution infrastructure allows you to manage a large number of target computers in a variety of topologies, and provides a fast and reliable way to scan, distribute, and install patches on target computers that require them. From a Tivoli Provisioning Manager perspective, a large environment for Patch Management corresponds to 20 or more target computers.

Depending on the number of targets and the number of patches that have to be downloaded, it can take up to 2 hours to discover all target computers and 4 to 6 hours for verifying patches on the Microsoft site and for downloading the required patches. This amount of time needs to be considered for the first time only, because here all of the information has to be collected. Any further patch installations only require the delta installations, so those go much faster.

Tivoli Provisioning Manager use the functionality of Microsoft Windows Update to automate Patch Management for all Microsoft products defined in the Microsoft Windows Update offline scan CAB file.

In this Patch Management scenario, we take advantage of the Tivoli Provisioning Manager's scalable distribution infrastructure, especially when scanning target computers for patches and when distributing or installing patches to those computers.

Tivoli Provisioning Manager downloads the latest Microsoft Windows Update offline scan CAB file (wsusscan.cab). All software definitions for patches will be added in the Tivoli Provisioning Manager data model. After software definitions for the available Microsoft patches have been created, users can select and approve the patches in the data model.

Tivoli Provisioning Manager scans endpoints for missing patches using Windows Update Agent. This scan identifies previously installed patches on each computer in the data model, and compiles a list of missing patches on the target. For the scan, the information from the patch catalog is read to find the approved patches that are not yet installed on the target computer. The patch catalog is built from the information in the CAB file and the approved patches. For each target computer, a software patch stack is built.



The "big picture" of Patch Management is shown in Figure 13-2.

Figure 13-2 Windows Patch Management Big Picture

To store the patches, it is required to have a Microsoft Patch download server running a Windows Operating System. This server also should have direct Internet access. The Microsoft WSUS Automation Package is used on Tivoli Provisioning Manager server.

To distribute and install patches on target computers, you must define a region, a zone, and a depot server in the Tivoli Provisioning Manager server, using this:

Go To \rightarrow Administration \rightarrow Provisioning \rightarrow Dynamic Content Delivery Configuration

If the provisioning server has the AIX or Red Hat Linux operating system installed, you can configure a Microsoft patch download server to download and extract the CAB files from the Internet. This computer must have the Windows operating system installed.

The steps to define a Microsoft patch download server are as follows.

- 1. Click Go To → Administration → Provisioning → Provisioning Global Settings.
- 2. Click the Variables tab.
- 3. Find the *wsus-download-server-name* variable and set its value to the fully-qualified name of the Microsoft patch download server.
- 4. Click Save.

Alternatively, if you want to manage patches when the provisioning server has the AIX or Red Hat Linux operating system installed, but without a Windows computer as the Microsoft patch download server to extract CAB files containing patches, consider the following suggestions:

- 1. Create a variable named *cabextractcommand*.
- Set its value to cabextract <cab_file_name>-q -d <extract_directory>, for example, cabextract wsusscn2.cab -d /tmp/update.

As a result, the wsusscn2.cab file is extracted into the /tmp/update directory.

Notes:

- The cabextract utility that you use must be supported by the AIX or Red Hat Linux operating system that is installed on the provisioning server.
- Do not include any paths in the cabextract command.
- Make sure that the executable file is in the system path.
- Downloaded patches are saved in .zip format. If you download a large number of patches, ensure that the native extract utility installed on the AIX or Red Hat Linux provisioning server has large file support.

To define a proxy server for an Internet connection in the data model, perform the following steps:

- 1. Click Go To \rightarrow Deployment \rightarrow Provisioning Computers.
- 2. In the *Computer* field, type the name of the computer where the Windows patches will be downloaded (Microsoft patch download server or provisioning server). In the list, click the computer name.
- 3. Click the Credentials tab.
- 4. Click Add Credentials → New Service Access Point.
- 5. Type a name for the service access point.
- 6. In the *Protocol Type* field, click **Network protocol IPv4**.
- 7. In the *Application Protocol* field, click **HTTP Access**.
- 8. In the *Context* field, type WUA.
- 9. Type the port number for the proxy server, for example, 8080.

The Port 8080 is the default port for most proxy servers. If you are using a different proxy server port in your environment, type the correct proxy server number.

- 10. In the *Domain* field, type the fully-qualified host name or IP address of the proxy server.
- 11.Select the Host check box.
- 12. If the proxy server requires authentication, select the **Authentication** check box. Otherwise, leave this check box blank.
- 13. Click New Password Credential.
- 14. In the Search Key field, type wua-download.
- 15. Type the user name and the password for the proxy server.
- 16.Click Save.

Then the Internet browser must also be configured to use a proxy server (Figure 13-3).



Figure 13-3 Patch Management in larger environments

For the target computers The Windows Update Agent (WUA) is required. But they do not need to have access to the Internet. The Windows Update is controlled by the Provisioning Manager Server.

The *MS_SOA_GetWindowsUpdateAgent* workflow helps to automate the process of downloading the Windows Update Agent executable and storing it in Tivoli Provisioning Manager's local file repository. Notice that by default, WUA version 3.0 is downloaded and installed on the target computers. Users can install the software product on multiple Windows endpoints by scheduling the software install from Tivoli Provisioning Manager's Web interface.

To install Windows Update Agent (WUA):

The target computers have some limitations using the built-in firewall if running on Windows 2008, Windows XP, or Windows Vista. The firewall is disabled by default, but it blocks traffic from RXA protocol if enabled. For Windows XP systems with installed Service Pack 2 and 3, an exception record for *File and Printer Sharing* can be added to the firewall to allow access to RXA protocol.

The common agent is required to take advantage of all Patch Management features. If you do not plan to install the common agent on the target computers, OpenSSH and OpenSSL should be configured to secure communication between the provisioning server and the targets. If OpenSSH is used, then version 4.4 and higher are required to avoid problems with known bug from version 4.3. The password authentication for securing communication must be used.

The general steps for doing Patch Management in a larger environment are:

- 1. Acquire patches to add the new Microsoft patches in the DCM.
- 2. Approve patches in the catalog.
- 3. Add compliance patch check for a group of computers (or a single computer).
- 4. Run compliance scan and check.
- 5. Approve compliance recommendations.
- 6. Implement the missing patch remediation task.
- 7. Verify the compliance results.

Acquiring patches and adding to the Data Center Model

A model must be set up to specify the patches that should be checked against the ones made available by the vendor. The options to set also include the Product Family, locale, and the severity of the patches. After setting up options, a task is used to bring these patches into the data model.

For this step, the role *Provisioning Configuration Librarian* or equivalent is required. If target computers run on Windows 2003, then the Windows automatic updates must be disabled:

- 1. Click Go To \rightarrow IT Infrastructure \rightarrow Software Catalog \rightarrow Patch Acquisition.
- 2. In the Operating System list, click **Select Value** and then pick **Windows** from the list of operating systems.

- 3. In the Infrastructure list, click **Select Value** and select **Scalable Distribution** Infrastructure.
- 4. In the Product Family list, click **Select Value** and choose the appropriate product.

Optional: To approve the acquired patches automatically, in the *Initial Patch Status* list, click **Select Value** and click **APPROVED**. This option is useful to mark as approved all the patches that have been made available by the vendor, without having to approve them in a later step.

- 5. To select patches based on severity, the corresponding check boxes in the **Severities** must be selected from the button **Select Severity** on the right.
- Use the button Select Products to select the software products for patch acquirement.
- 7. Select **Locale** to select the check boxes corresponding to the locales for the patches.
- 8. Tasks can be scheduled. Scheduling options can be entered clicking the **Schedule** button. A notification about task status can be given to users, and also an e-mail can be sent. In addition, events can be generated to automate status processing.
- 9. Click Submit button on the bottom right.
- 10.On the *Provisioning Task Tracking* page, click **Refresh** periodically to update the task status until the task is completed.

The task invokes the workflow *MS_SOA_DiscoverWindowsUpdates* for the Microsoft Updates Discovery. The cabextract.vbs script runs to download the offline CAB file from Microsoft's Web site and extract the xml file.

Example 13-3 cabextract.vbs for downloading and extracting offline CAB file

```
cscript cabextract.vbs //Nologo true wsusscn2.cab
http://go.microsoft.com/fwlink/?LinkId=76054 "" "" wsusscanToDcm.cmd
MicrosoftWeb 4562 <tpm_server_name>:<proxy - authentication user>
<proxy - password> "" false
```

```
The XML file is extracted from offline CAB file into repository %TIO_HOME%\repository\wua\wsusscancab\update
```

The patch information is read from the extracted XML file and stored in the Data Center Model.

As a result, the patch acquisition task is displayed with a status of *Success* on the *Provisioning Task Tracking* page. The patches are brought into the data model.

Download Address information is read from the CAB file and stored in the software definition. It is used to download the patch to Tivoli Provisioning Manager at installation time.

To view the patches catalog, in the Start Center, click **Patches** under Favorite applications.

We recommend testing the patches in a test environment before distributing to the field. Doing this can identify possible problems and conflicts and avoid bigger problems in the production environment. The patches can be installed on a test computer using the Patch Installation application, but the actual testing of patches is to be performed outside of the provisioning applications.

Patch approval

To approve patches, the required user role is Compliance Analyst or equivalent.

At first the patches should be approved for the entire organization (at data model level). Only the approved patches will be considered when the target computers are scanned for missing patches. Then the Compliance Analyst can decide to approve patches for certain computer groups (only). This second step in the approval process is done when scanning for missing patches. It also can be decided to not approve some patches immediately because further testing is required before approving them.

The steps to approve patches in the data model are:

1. Click Go To \rightarrow IT Infrastructure \rightarrow Software Catalog \rightarrow Patches.

(or select Start Center \rightarrow Favorite Applications \rightarrow Patches).

- Press Enter to display all patches from the catalog or enter patch name or other attributes to filter list.
- 3. Click **Select Records** and select the patches that should be approved, and then click **Approve**.

Note: To be able to select records, you must filter down your list of patches to a maximum of 200. If you want to approve more than 200 patches at the same time, filter down your patches, then click **Approve** and click **OK** on the confirmation message.

4. Patches that you have approved are displayed with a status of *Approved* on the *Patches* page as a result.

Setting up a compliance check

The compliance check is for verification if patches are required on the target computers. Compliance checks define the compliance state of target computers and are used to detect, report, and recommend how to fix noncompliance.

To set up the compliance check, perform the following steps:

- 1. Click Go To \rightarrow Deployment \rightarrow Provisioning Groups.
- 2. Select a group of target computers and click the name in the list.
- 3. Click the **Compliance** tab.
- 4. Click New Compliance Check \rightarrow Patch Check.
- 5. In the *Patch Approval Group* field, click **Select Value** and select a group of patches to be scanned, then click Save.

Tip: By default, all patches that have been approved in the data model are scanned, and target computers are verified against all approved patches to see if computers are compliant. You can also select a patch approval group, which will be used to specify a set of allowed patches, or approval lists. The patch approval group will limit the patches for which recommendations are generated to the specified set of patches only. You might want to use this option to tightly control patches for critical computers where more exhaustive testing of patches is needed before they are required to be installed.

- 6. To automatically approve recommendations when they are generated, click **Enable Automatic Approval** and click **OK** in the message box. All recommendations that are generated by this compliance check will be created in the Approved state. This step is optional.
- 7. Click Save.

As a result, the Operating System Patches and Updates compliance check is displayed in the list of compliance checks defined for the group of target computers.

Scan for missing patches

The software that exists on target computers can be compared with the list of approved patches for the entire organization to see which patches are missing on which computers (Figure 13-4).



Figure 13-4 Compliance check definition and verification

Follow these steps to scan for missing patches:

1. Click Go To \rightarrow Deployment \rightarrow Provisioning Groups.

Or in the Start Center under Favorite applications, click **Provisioning Groups**.

- 2. Select the group of target computers.
- 3. Click the Compliance tab.
- 4. Click Run Scan and Check.

This task also can be scheduled to execute it at a later time by entering the required information under **Schedule Scan**.

- 5. In the **Notification tab**, specify notification options if users have to be notified about the task status.
- 6. On the *Provisioning Task Tracking* page, click **Refresh** to update the task status until the task is completed.

Attention: Wait until the task completes before starting another compliance scan task on the target computers. If you run concurrent compliance scan tasks on a target computer, the tasks might fail.

After finishing a task, the scanning and checking task is displayed with a status of *Success* on the *Provisioning Task Tracking* page. Recommendations to install missing patches are generated. On the Compliance tab for the group, the patch check displays either Yes or No in the Compliant column, depending on whether or not all required patches are installed on the target computers. If notification was set up, recipients will be notified that recommendations need be approved.

For the Compliance scan, the Microsoft Windows Update offline scan CAB file and the patch scan script are distributed to each Windows target.

The compliance check uses the Windows Update Agent (WUA) to scan the computer using the CAB file and generates a list of missing patches.

The executed Visual Basic® script writes results from WUA into .xml file. This.xml file is send back to the Tivoli Provisioning Manager server. Then the information from this result file is imported in the data center model (DCM) and the Tivoli Provisioning Manager generates a list of missing patches for the target in the data model.



Figure 13-5 Compliance scan

The workflow invoked is MS_WUA_SOA_Scan. The patch scan logfile saved on the target computer can be analyzed in case of problems. It can be found in the Administrators home directory:

```
%USERPROFILE%\%TEMP%\<date>__patchscan__<timestamp_.log</pre>
```

Where *<date>* is the date and *<timestamp>* is the time when the scan was executed. In this user temp folder, the patchscan.vbs and the wsusscn2.cab files are also stored.

Approving compliance recommendations

After scanning the target computers to see which patches are missing on them, compliance recommendations are generated. Based on these recommendations, it can be decided which patches will be installed on the target computers. To approve the compliance recommendation, a user role of Compliance analyst or an equivalent role is required.

To approve compliance recommendations:

- 1. Click Go To \rightarrow Deployment \rightarrow Provisioning Groups.
- 2. Select a group of target computers.
- 3. Click the Recommendations tab.
- 4. In the recommendations list, select the check boxes corresponding to the missing patches that should be approved and click **Approve**.

As a result, the selected patches are displayed with a status of *Approved* on the *Recommendations* tab.

The compliance recommendations show only patches that have been previously approved in the data center model and are still not yet installed on the target computers. You can decide which patches inside the recommendation can be installed on your target computers.

Therefore users can double check for missing patches:

- > At the beginning by approving a patch in the data center model
- Before applying and approving the recommendation

Distributing and installing patches

When patches are approved, they can be distributed first and then installed on the target computers. During distribution, the patch binaries are downloaded into the data model, and then the patch binaries and other files (for example, CAB file, vbscript) are published to a depot server. From the depot server, patches are distributed for installation on target computers. The patch distribution task can also be scheduled for a specified date and time. Here the user role of Deployment Specialist or an equivalent role is required.

To distribute the patches:

- 1. Click Go To \rightarrow Deployment \rightarrow Patch Management \rightarrow Patch Distribution.
- 2. Click **Select Patches** and select the patches that are planned to be distributed, then click **OK**. The list also can be filtered for easier selection.
- 3. Click Select \rightarrow Groups and select the group of target computers, then click OK.
- 4. Under **Notification**, specify notification options to inform users about the task status.
- 5. Click Submit.
- 6. On the *Provisioning Task Tracking* page, click **Refresh** to update the task status until the task is completed.

As a result, the patch distribution task is displayed with a status of *Success* on the *Provisioning Task Tracking* page.



Figure 13-6 Patch distribution and installation

After patches are approved, you can install them on the target computers where they are missing.

To install patches:

- 1. Click Go To \rightarrow Deployment \rightarrow Provisioning Groups.
- 2. Click the group of target computers.
- 3. Click the **Recommendations** tab.
- 4. Select all the patches that are approved from the recommendations list and click **Schedule**.

Attention: The Run button is not supported for Windows large environments.

- 5. In the Scheduling dialog box, specify the options and click Submit.
- 6. On the *Provisioning Task Tracking* page, click **Refresh** to update the task status until the task is completed.

As a result, the patch installation task is displayed with a status of *Success* on the *Provisioning Task Tracking* page.

Most of the patches released by Microsoft have versions differentiated by locale, operating system version, and processor architecture.

When users run the Compliance and Compliance check from Tivoli Provisioning Manager prior a patch installation, Tivoli Provisioning Manager matches the correct installable with each computer when building recommendations. However, when the user wants to install patches on target computers without running these scans, Tivoli Provisioning Manager performs filtering operations to avoid distributing unnecessary installable files.

Tivoli Provisioning Manager publishes all potentially matched installable files to the depot server, along with the Microsoft Windows Update offline scan CAB file, and the two VBScripts:

- ► patchinstall.vbs
- installableselect.vbs

The scripts are distributed to the target computers and used to determine which installable is needed. After being determined, the installable will be distributed and the appropriate patch will be installed:

- 1. Install patches on target computer using WUA.
- 2. Run the WUA scan again and return the resulting .xml file.
- 3. Update DCM based on the new scan results.

Verification of compliance results

After installing patches on the target computers, you can verify that patches are installed successfully. To do this, a user role of Compliance Analyst or an equivalent role is necessary.

You can verify compliance results either by running the compliance scan again and verifying the list of recommendations or running patch reports that provide information about missing patches.

Running the compliance scan again

To run the compliance scan again, perform the following steps:

- 1. Click Go To \rightarrow IT Infrastructure \rightarrow Provisioning Inventory \rightarrow Provisioning Groups.
- 2. Click to select the group of target computers.
- 3. Click the **Compliance** tab.
- Click Run → Check to run a compliance check before displaying the recommendations so that the results are accurate.
- 5. Click the **Recommendations** tab now.
- 6. In the list of recommendations, verify that the installed patches are no longer displayed as missing.
- 7. Click OK.

As a result, the installed patches are no longer included in the list of recommendations because they are no longer missing from the target computers.

Generating patch compliance reports

To generate patch compliance reports, perform the following steps:

- 1. Click Go To \rightarrow Deployment \rightarrow Provisioning Groups.
- 2. Click and select the group of target computers for the report.
- 3. Click the **Compliance** tab.
- 4. Click $\mathbf{Run} \rightarrow \mathbf{Check}$ to run a compliance check before running the report so that the results are accurate.
- 5. Click Go To \rightarrow Administration \rightarrow Reporting \rightarrow Report Administration.
- 6. Search for the report with the description **Do Windows servers comply with the patch policy?** and click the report name.
- 7. Click Generate Request Page.

- 8. After the report is generated, click **Close**. The report lists all the target computers that have a patch compliance check defined. The *Is Compliant* column lists the compliance status of the target computers.
- 9. Click Preview and in the dialog box that is opened, click Submit.

Tip: You can also generate the report with the description, **What patches are missing on what Windows servers?** to list all the missing patches and their corresponding target computers.

The resulting report will show that installed patches are not listed because they are not missing from the target computers.

10. In the **Group's recommendations** tab, you also can check the *Status* column for the group. For the patches that were installed successfully, this column displays Implemented.

Users can download the approved Windows patches before installing them on the target computer. If the user has not yet downloaded the Windows patches before the installation, the download is automatically performed as part of the patch installation process. If the patch download is performed as part of the installation process, the user can either use the default location for the download, which is the local file repository on the provisioning server, or can create and configure a new file repository for the download. The download time depends on the number of updates that must be downloaded.

Uninstalling the patches

There are situations where a patch has to be uninstalled again from a computer, for example, the patch caused problems in the environment, or the patch was installed in a test environment and is no longer needed.

Tivoli Provisioning Manager does not have an out of the box solution for uninstall patches. To remove patches from large computers, the commands or tools provided by the Windows Operating system must be used, for example, **Add or Remove Programs.** Another option is to develop automation packages to create your own patch uninstallation solution, depending on requirements.

13.3 Patch Management in AIX environments



The Patch Management process in AIX environments is shown in Figure 13-7.

Figure 13-7 AIX Patch Management overview

The first step again is to run Initial Discovery to insert all AIX machines into data model.

To manage patches for AIX environment, the configuration setup must be done before. The required components are the target computers and the AIX satellite server. The patches are downloaded from the AIX Fix Center over the Internet to a satellite server or optionally to an FTP server. The AIX satellite server is defined as a target computer in your configuration.

Downloaded patches are moved to the provisioning server. The patches are distributed to the target computers from the provisioning server. Optionally, you can use a proxy server to provide Internet access to the AIX satellite server. In this configuration, you must set up Service Update Management Assistant (SUMA) to work with a proxy server. For information about how to configure SUMA, see the System p^{TM} and AIX information center.

Note: Start of change downloaded patches are saved in .zip format. If you download a large number of patches, ensure that the native extract utility installed on the AIX or Red Hat Linux provisioning server has large file support.



Figure 13-8 AIX Patch Management components

There are a number of requirements that must be met by the AIX satellite server to manage patches in AIX environments.

- ► The operating system should be AIX 5L[™] Version 5.3 TL5 (5300-05) or higher.
- ► The SUMA must be installed. SUMA is included with AIX 5L Version 5.3.
- Internet access is required, either directly, or using a proxy server.
- We recommend mounting a file system on the directory where you plan to download patches. This directory must have a minimum of 20 GB of space and the possibility to extend it. To obtain the directory that is used by your system, run the command suma -D. The output displays the patch download directory in the *DLTarget* field. The default directory is /usr/sys/inst.images.

It is also possible to use the provisioning server as the AIX satellite server to manage patches. For setup, the role of Provisioning Administrator or the equivalent is required.

Follow these steps:

- 1. Click Go To → IT Infrastructure → Provisioning Inventory → Provisioning Computers.
- 2. Select the Tivoli Provisioning Manager server.
- 3. Click the Credentials tab.
- 4. Click Add Credentials → New service access point.
- 5. Enter the required information
 - Service access point: Set any name.
 - Protocol type: Select
 Network protocol type which is further defined by specifier.
 - Application Protocol: Select Run command on local server.
 - Port: Set any port number that is not in use.
- 6. Add a New Password Credential with the following information:
 - Search key: rootlocal
 - User name: root (or root equivalent)
 - **Password**: password of the root (or root equivalent) user
- 7. Add a New Password Credential with the following information:
 - Search key: default
 - User name: tioadmin
 - Password: password of tioadmin user
- 8. Enter the password credential with search key default as Default Credential.
- Click the Workflows tab and then assign the Deployment Engine service access point device driver to the service access point.
- 10.. Create another service access point by repeating steps 4 to 9. For this new service access point, clear the **Host** check box.

11.Click Save.

When running scriptlets on target computers, the provisioning server expects that the command prompt ends in \$ or # on the target. The PS1 environment variable governs the appearance of the prompt. There has to be a blank character at the end of the prompt on an AIX target computer in order to run on it a workflow containing a scriptlet (bash / perl). If a blank character is not present, then the scriptlets (both perl and bash) called inside a workflow will stop and do not return to the executing workflow.

In addition, openSSH 4.4 or higher, openSSL, perI-5.8.4 and bash packages must be installed. The OpenSSH for AIX 5 can be obtained from:

https://sourceforge.net/projects/openssh-aix.

The location of the shells or script interpreters is important because scripts that are run must include this information about the first line of the script. Ensure that the packages are installed in the following locations:

- Bash location: /usr/bin/bash
- Expect location: /usr/bin/expect
- Perl location: /usr/bin/perl

Note: Expect is only required to be installed on a target computer if a certain automation package runs expect code on the target computer itself. This installation is optional depending on the requirements.

The xIC.rte 6.0 runtime code can be downloaded as a fix from the AIX Support site at:

https://techsupport.services.ibm.com/server/aix.fdc

13.3.1 Acquiring patches

You are required to set up your own model to specify which patches have to check for from the ones that are made available by the vendor. It can be checked for all AIX patches available regardless of the version or it can be checked for a specific version only, such as for patches to apply on AIX 6.1 only. After setting up options, these patches can be downloaded into the data center model:

- 1. Click Go To \rightarrow IT Infrastructure \rightarrow Software Catalog \rightarrow Patch Acquisition.
- 2. In the *Operating System* list, click **Select Value** and pick **AIX** from the list of operating systems.
- 3. In the *Satellite Server* list, click **Select Value** and select the name of the satellite server.
- 4. Click **Refresh TL/SP Definitions** to bring all available AIX patches, whether for version 5.2, 5.3, or 6.1 into the data model.
- 5. Click Submit.
- 6. On the *Provisioning Task Tracking* page, click **Refresh** to update the task status until the task is completed.
- 7. Click Go To \rightarrow IT Infrastructure \rightarrow Software Catalog \rightarrow Patch Acquisition.

- 8. Under *Technology Levels and Service Packs*, select the check boxes corresponding to the patches that you want to acquire and click **Download Patches**. This step is mandatory for the selected patches to be considered for installation.
- 9. Under *Scheduling*, specify scheduling options if the task should be scheduled for a later time.
- 10.Under *Notification*, specify notification options.
- 11.Click Submit.
- 12.On the *Provisioning Task Tracking* page, click **Refresh** to update the task status until the task is completed.

The result of the patch acquisition task is displayed with a status of *Success* on the *Provisioning Task Tracking* page. The patches are brought into the data model.

Then, patches can be tested as described for Windows in "Acquiring patches and adding to the Data Center Model" on page 385.

13.3.2 Setting up compliance

The compliance check is to verify if patches are required on the target computers. Compliance checks define the compliance state of your target computers and are used to detect, report, and recommend how to fix noncompliance. The user role is Compliance Analyst or equivalent is required.

We demonstrate how to set up compliance using the Latest Level scan model. The scan model can be customized afterwards. Follow these steps:

- 1. Click Go To \rightarrow Deployment \rightarrow Provisioning Groups.
- 2. Find the group of target computers and pick the name from the list.
- 3. Click the Compliance tab.
- 4. Click New Compliance Check \rightarrow Patch Check.
- 5. In the *Select Patch Group* dialog, click **Save**.
- 6. To automatically approve recommendations when they are generated, click **Enable Automatic Approval** and **OK** in the message box. All recommendations that are generated by this compliance check will be created in the Approved state. This is optional.
- 7. Click Save.

As a result, the Operating System Patches and Updates compliance check is displayed in the list of compliance checks defined for the group of target computers.

13.3.3 Scanning for missing patches

The existing software on a target computer can be compared with the list of patches that are available to see which patches are missing on which computers. The AIX patch scan generates recommendations based on AIX patch updates available in the data model. The required user role is Provisioning Configuration Librarian or equivalent.

- 1. Click Go To \rightarrow Deployment \rightarrow Provisioning Groups.
- 2. Select the group of target computers.
- 3. Click the **Compliance** tab.
- 4. Select Run Scan and Check.

This task can be scheduled for a later time also.

- 5. Click the Notification tab to specify notification options.
- 6. On the *Provisioning Task Tracking* page, click **Refresh** to update the task status until the task is completed.

Attention: Wait until the task completes before starting another compliance scan task on the target computers. If you run concurrent compliance scan tasks on a target computer, the tasks might fail.

As a result, the **s**canning and checking task is displayed with a status of *Success* on the *Provisioning Task Tracking* page. The recommendations to install missing patches are generated. On the Compliance tab for the group, the patch check displays either *Yes* or *No* in the *Compliant* column, depending on whether all required patches are installed on the target computers. If notification was set up, recipients will be notified that recommendations need be approved.

13.3.4 Approving compliance recommendations

After scanning target computers to see which patches are missing on them, compliance recommendations are generated. Based on these recommendations, it can be decided which patches will be installed on the target computers. The AIX patch scan generates recommendations based on AIX patch updates available in the data model. To do this, the required user role is Compliance Analyst or equivalent. Follow these steps:

- 1. Click Go To \rightarrow Deployment \rightarrow Provisioning Groups.
- 2. Click your group of target computers.
- 3. Click the Recommendations tab.
- 4. In the recommendations list, select the check boxes corresponding to the missing patches that should be approved and click **Approve**.

As a result, the selected patches are displayed with a status of *Approved* on the *Recommendations* tab.

13.3.5 Distributing patches

After patch approval, the already downloaded technology levels or service packs can be distributed to the target computers before installation. Because the size of the AIX patches is quite large, it is recommended to distribute the AIX patches before installing, especially if the maintenance window for installing the patch is not very long. The distribution can be done immediately or the task also can be scheduled. The user role Deployment Specialist or equivalent is required.

- 1. Click Go To \rightarrow Deployment \rightarrow Patch Management \rightarrow Patch Distribution.
- 2. Click Select Patches and select the patches. Then click OK.
- 3. Click **Select** \rightarrow **Groups**, select a group of target computers, then click **OK**.
- 4. Under Scheduling, specify scheduling options if required.
- 5. Under Notification, specify notification options.
- 6. Click Submit.
- 7. On the *Provisioning Task Tracking* page, click **Refresh** to update the task status until the task is completed.

As a result, the patch distribution task is displayed with a status of *Success* on the *Provisioning Task Tracking* page.

13.3.6 Installing patches

When patches are approved, they can be installed on the target computers where they are missing. The required user role is Deployment Specialist or the equivalent. Follow these steps:

- 1. Click Go To \rightarrow Deployment \rightarrow Provisioning Groups.
- 2. Select the group of target computers.

- 3. Click the Recommendations tab.
- 4. Select all the patches that are approved from the recommendations list and click **Run**.
- 5. On the *Provisioning Task Tracking* page, click **Refresh** to update the task status until the task is completed.

The patch installation task is displayed with a status of *Success* on the *Provisioning Task Tracking* page.

13.3.7 Verifying compliance results

After installing patches on the target computers, it can be verified that patches are installed successfully. The user role for this is Compliance Analyst or the equivalent.

The compliance results can be verified either by running the compliance scan again and verifying the list of recommendations or by running patch reports that provide information about missing patches.

This is the same as described in "Verification of compliance results" on page 394.

13.3.8 Uninstalling patches

It might be that a patch must be uninstalled from a target computer if, for example, the patch caused problems to your environment or if the patch was installed on a computer for the purpose of testing and is no longer needed.

The required user role is Deployment Specialist or equivalent. Patches that will be uninstalled from the target computers must be installed in a previous Tivoli Provisioning Manager task. To uninstall a patch, it must not be committed during installation.

Attention: You cannot uninstall Technology Levels using this method, but only Service Packs. To uninstall Technology Levels, use the commands or tools that are provided by the AIX operating system.

Follow these steps for uninstalling patches:

- 1. Click Go To \rightarrow Deployment \rightarrow Patch Management \rightarrow Patch Uninstallation.
- 2. Select patches and select the check boxes corresponding to the patches that should be uninstalled, then click **OK**. To search for a particular patch, type the patch number in the *Patch* field, for example, AIX_SP 6100-00-02.

- 3. Click **Select** \rightarrow **Groups** and select a group of target computers, then click **OK**.
- 4. Under Scheduling (if required), specify scheduling options.
- 5. In the Notification pane, specify notification options.
- 6. Click Submit.
- 7. On the *Provisioning Task Tracking* page, click **Refresh** to update the task status until the task is completed.

As a result, the patch uninstallation task is displayed with a status of *Success* on the *Provisioning Task Tracking* page.

13.4 Patch Management in SUSE Linux Enterprise environments

This section provides some reference information about the Patch Management solution for SUSE Linux operating systems. It is intended as a quick reference for the supported SUSE Linux versions and platforms, the various components that are part of the supported configurations, and the requirements for managing patches. Also, it gives at-a-glance information about the global variables that are needed to set and the related automation packages.

The basic steps for Patch Management are the same as described in "Patch Management in large Windows environments" on page 380 and "Patch Management in AIX environments" on page 396.

13.4.1 Patch Management solutions

The Patch Management solution for SUSE Linux environments uses the **rug** command-line tool, which is provided with SLES 10 operating systems.

Patch Management solutions for the following SUSE Linux operating systems and versions are supported:

- SUSE Linux Enterprise Server 10, 10 SP1, and 10 SP2 (x86 32-bit and 64-bit)
- SUSE Linux Enterprise Server 10, 10 SP1, and 10 SP2 (IBM System z[™] 64-bit)
- SUSE Linux Enterprise Server 10, 10 SP1, and 10 SP2 (IBM System p 64-bit)

This Patch Management solution supports the following configurations:

SUSE Linux patch server (ZENworks or YUP Package Manager) model



Figure 13-9 illustrates the SUSE Linux patch server model.

Figure 13-9 SUSE Linux Patch Management

The target computers retrieve the patches from a patch server (ZENworks or YUP Package Manager). The patch server is used as a patch repository for the patches downloaded from the SUSE Linux update site over the Internet. The SUSE Linux patch server communicates directly with the target computers. Optionally, a proxy server can be used to provide Internet access to the patch server.

13.4.2 SUSE Linux update site model

Provisioning server SUSE Linux target computers FTP or HTTP proxy (optional)

Figure 13-10 illustrates the SUSE Linux update site model.

Figure 13-10 SUSE Linux Patch Management and Connection to Update site

The target computers are connected to the SUSE Linux update site over the Internet to download the patches. Optionally, a proxy server can be used to provide Internet access to the target computers.

The following servers are required:

- The ZENworks server is a computer that has SUSE Linux 10 or SUSE Linux 10 SP1 and ZENworks Linux Management 7.2 installed, and has Internet access. This computer is used as a patch repository for the patches downloaded from the SUSE Linux update site over the Internet. The system administrator must ensure that the latest patches exist on the ZENworks patch server. This is a manual process performed outside of the provisioning server.
- The YUP server is a computer that has SUSE Linux 10 or SUSE Linux 10 SP1 and the Yum Update Proxy (YUP) package installed, and has Internet access. This computer is used as a patch repository for the patches downloaded from the SUSE Linux update site over the Internet. The system administrator must ensure that the latest patches exist on the YUP patch server. This is a manual process performed outside of the provisioning server.
- The target computers have SUSE Linux 10 installed. In the configuration where the target computers are connected to the SUSE Linux update site directly, they must have Internet access. In the configuration where a patch server is present, Internet access for the target computers is not necessary. For additional requirements for the SUSE Linux target computers, see the topic, Requirements for SUSE Linux Enterprise Server (SLES) target computers.
- Depending on the configuration that you use, you would set up a number of variables at the system level:
 - Set the value for the SUSELinux.Catalog.Name variable to a unique catalog name, for example, SLES10-Updates.
 - If connecting to the SUSE Linux update site directly, set the value for the SUSELinux.Update.Server.url variable to the IP address of the SLES Linux Update site, ftp://ftp.suse.com/pub/suse/update/10.1, for example. Set the value for the SUSELinux.Service.Type variable to zypp.

Note: The site specified for the *SUSELinux.Update.Server.url* variable might change over time. In this case, try and connect to the Novell® Web site for mirror sites, or contact your SUSE Linux representative. The Novell site is:

http://www.novell.com/products/opensuse/downloads/ftp/int_mirrors.html

- If using a ZENworks server, set the value for the SUSELinux.Update.Server.url to the IP address of the ZENworks patch server in the format https://<IP_address_zen>, for example, https://10.77.88.15/. Set the value for the SUSELinux.Service.Type variable to zenworks.
- If using a YUP server, set the value for the SUSELinux.Update.Server.url to the IP address of the YUP patch server in the format ftp://<IP_address_YUP>/SLES10-YUP/<product>/<architecture>, for example, ftp://10.77.88.42/SLE10-YUP/SLES10/i586. Set the value for the SUSELinux.Service.Type variable to yum.
- If using an FTP or HTTP proxy server, create a variable named SUSELinux.proxy.server and set its value to the host name of the proxy server. Either run initial discovery to add the proxy server to the data model or add it manually. Also, define a service access point (SAP) of type http, https, or ftp, depending on the proxy server configuration in the organization. The SAP must have password credentials defined and the *Context* field set to Proxy Server Connection.

Note: If you have a configuration where different groups of target computers use different methods to retrieve the patches, you need to set up variables per group to specify each download method. For example, a group of target computers might be connected directly to the SUSE Linux update site, a group of target computers might use a ZENworks patch server to retrieve the patches, and a group of target computers might use a YUP patch server to download the patches. In this configuration, you must set up the variables for Patch Management at the group level, not at the system level.

The automation packages *sles-operating-system* and *suse_patch* are used for SUSE Linux Patch Management.

14

Operating system provisioning

Manual operating system deployment is a time-consuming and error-prone task when it involves hundreds of computers on different operating systems across multiple sites.

IBM Tivoli Provisioning Manager for OS Deployment offers a central solution to remotely manage the image deployment of different operating systems and deliver fully installed computers without needing to perform any manual operations on the target systems. Thanks to the Preboot eXecution Environment (PXE) protocol, the target computer connects to the Tivoli Provisioning Manager for OS Deployment boot server and starts the scheduled deployment of an operating system profile previously created and customized on the boot server.

The image provisioning does not require any installed software on the target computer because PXE is used by Tivoli Provisioning Manager for OS Deployment to remotely download the Tivoli Provisioning Manager for OS Deployment kernel necessary to boot the computer and undertake the actions to deploy an operating system.

Tivoli Provisioning Server for OS Deployment provides the ability to create, customize, and deploy the following operating system images:

- Windows cloning (capturing a golden master image and taking a point-in-time snapshot) as well as unattended setup
- AIX unattended setup
- Linux cloning (not supported on Linux PPC and Cell Blades) and unattended setup
- Solaris unattended setup
- VMWare ESX unattended setup

We also cover the following topics:

- "Tivoli Provisioning Manager for OS Deployment architecture" on page 411
- "Parent-child boot servers" on page 423
- "Software modules" on page 426
- "Hardware configuration" on page 460
- "Unattended setup" on page 469
- "Cloning computers" on page 489

14.1 Tivoli Provisioning Manager for OS Deployment architecture

Tivoli Provisioning Server for OS Deployment is a database driven, PXE-based deployment solution. Because of a configured DHCP server and the boot sequence in the target BIOS being configured to have the network boot first, the hosts boot into the Tivoli Provisioning Server for OS Deployment boot server by way of PXE and download the deployment engine (a miniature operating system) needed for the deployments to be executed.

A database component stores information about the registered hosts, the operating system images, and the deployment tasks. Target administration, image creation and customization, deployment schedules, and submission are done either through the Tivoli Provisioning Server of the OS Deployment Web user interface or through the Tivoli Provisioning Server Web user interface.

Tivoli Provisioning Server leverages the Java API layer to communicate with Tivoli Provisioning Server for OS Deployment.

The *Java API* is a set of available classes that map to readable and editable data structures in the OS deployment server and can be used to interface directly with all objects and settings. Using the Java API, you could write your own scripts that interact with Tivoli Provisioning Manager for OS Deployment. Advanced users can find sample scenarios about how to use the Java API to create their own scripts in the *Tivoli Provisioning for OS Deployment Guide V7.1.1*, which can be located at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.ti
voli.tpm.osd.doc/osd_install_guide.pdf

Let us now discuss the Tivoli Provisioning Manager for OS Deployment components and their characteristics.

14.1.1 Product components

Tivoli Provisioning Server for OS Deployment leverages the following components to provision computers:

- Server-side components
- Console component
- Client-side applications
- ► A configured Dynamic Host Configuration Protocol (DHCP) server

The server-side components include:

- The OS deployment server (or boot server) represented by the process rembo.exe on Windows and rembo on UNIX. It provides the PXE remote-boot capability and manages the images and their deployment. The parent boot server is generally installed during the Tivoli Provisioning Server installation. Later you can decide to install additional child servers to distribute the deployment workload.
- A database accessed through the standard JDBC interface by the Tivoli Provisioning Server for OS Deployment TCP-to-ODBC/JDBC gateway service, represented by the process dbgw.exe on Windows and dbgw on UNIX. This database stores the Bill of Material (BOM) for every registered target, and the information about software modules and their bindings.

Note: By default, Tivoli Provisioning Server installs only one DBGW, and it runs on the local provisioning server.

The *console component* is provided by the Web Interface Extension service. It is represented by the **rbagent.exe** process on Windows and **rbagent.<platform>** on UNIX (for example, for the Linux platform, it is the rbagent.linux process). This component is installed on the Tivoli Provisioning Server for OS Deployment boot server and on any supported system where it would be required for administration purposes.

The *client-side applications* include two stand-alone management platforms that do not require an operating system. These components are embedded in the boot server and are sent to the target systems during the PXE boot or by way of media, such as a CD-ROM, a diskette, or hard disk partition:

- The deployment engine is a mini-operating system that is needed for all provisioning tasks (installing a Windows or UNIX operating system, partitioning and formatting disks, and accessing and modifying Windows registries). It is downloaded automatically by the boot server to the target using a simple multicast protocol (MTFTP) when the target system PXE boots into the provisioning server by way of the DHCP configuration.
- The Web Interface Extension can be run either as a service or as a command-line tool (rbagent.exe on Windows and rbagent.<platform> on UNIX). For example, on Windows, it can be used to access the system information published by drivers using the Windows Management Interface (WMI) and, on Intel-based operating systems, is able to start the deployment engine in offline mode.

A correctly configured *DHCP server* is required to boot correctly the target systems by way of PXE into the Tivoli Provisioning for OS Deployment boot server. Notice that there are basic DHCP configuration (option 43 and 60) and

additional options required to provision operating systems on specific platforms and to be able to create Linux clone profiles. For more information about this topic, refer to 14.1.2, "DHCP configuration" on page 413.

In order to exploit the PXE network boot, you must, on the target systems, have the boot order configured in the BIOS so that the network boot occurs first. You must also have a network card provided with the PXE boot ROM chip; if the network card does not have that capability, you can emulate PXE on the target through media such as a CD-ROM, a diskette, or hard disk partition.

14.1.2 DHCP configuration

In order to use Tivoli Provisioning Server for OS Deployment and its functionalities available through the Tivoli Provisioning Server, it is necessary to configure correctly the DHCP server.

In order to support PXE clients on a network, the DHCP server needs to be configured by way of options 60 and 43. Basically, option 60 is needed to inform the targets that the location of the PXE server is known, and option 43 is required to indicate that the PXE server does not reside on the same computer as the DHCP server and to give the precise location of the PXE server. In addition, there are other options that are required to provision operating systems on specific architectures (options 66 and 67 for SUN and PowerPC® targets) and to create a Linux cloning profile (options 1, 6, and 15).

You cannot run two PXE servers on the same computer, so if you have another PXE boot tool, such as Microsoft Automated Deployment Services (ADS), you have to disable it before installing Tivoli Provisioning Server for OS Deployment.

Let us now discuss each of the DHCP options required by Tivoli Provisioning Manager for OS Deployment in the following sections.

Options 60 and 43

In order to support PXE clients on a network, the DHCP server must be configured with options 60 and 43:

- Option 60 (Class identifier) must be set to "PXEClient" so that the target knows the location of the PXE server.
- Option 43 is necessary to indicate that the PXE server does not reside on the same computer as the DHCP server and to give the precise location of the PXE server.

In particular, what option or options you set depends on the specific situation:

- If the DHCP server and the OS deployment server are on different machines, and do not know the location of the PXE server, option 60 and 43 must not be set. If the DHCP server already has options 43 and 60 configured, remove them. In this situation, the OS Deployment server detects the DHCP packets sent over the network by PXE bootroms and offers PXE parameters without disturbing the standard DHCP negotiation process. This behavior is called DHCPProxy.
- If the DHCP server and the OS deployment server are on different machines, and they know the location of the PXE server, you must set both option 60 and 43. If the two options are already set, remove and redefine them.
- If the DHCP server and OS deployment server are on the same target, only option 60 is necessary. If option 43 is set, remove it.

If the PXE server is on a separate subnet and cannot listen to DHCP discovery packets or if there are several PXE servers on the same subnet, option 43 is the only viable solution for instructing the client systems on what to do.

Option 43 is also useful if you want a group of target systems to boot on one PXE server and another group to boot on another PXE server on a different subnet (in this case, a router must be configured correctly in order to allow the second group of systems to locate the PXE server on the different subnet).

Options 66 and 67

If you plan to deploy SUN and PowerPC targets through Tivoli Provisioning Manager for OS Deployment and you do not want to use the RARP/bootparams method to network boot them, you can use the DHCP server instead by setting the options 66 and 67. The advantage of using DHCP is that you can work with boot servers in different subnets (after you have configured correctly the involved routers to *not* block DHCP packets).

Option 66 (known as next-server under the ISC DHCP server and tftp-server-name under the Solaris DHCP server) specifies the IP address of the OS deployment server while option 67 (known as filename under the ISC DHCP server and bootfile-name under the Solaris DHCP server) must be set to the fixed value rembo.fcode (which represents the boot file name).

For a ISC DHCP server, you also have to set up the following options:

- Allow booting
- Allow bootp

Options 1, 6, and 15

If you plan to create Linux clone profiles, you have to set the following additional DHCP options:

- Option 1 (also known as subnet-mask under the ISC DHCP server) must be set to the subnet mask value.
- Option 6 (also known as domain-name-servers under the ISC DHCP server) must be set to the IP address of the domain name server (DNS).
- Option 15 (also known as domain-name under the ISC DHCP server) must be set to a non-empty string indicating the domain name.

These options must be manually added to dhcpd.conf for ISC DHCP servers.

Notice that the options 1, 6, and 15 are required only to enable the creation of clone profiles from installed Linux machines and not to PXE boot installed Linux targets.

14.1.3 Deployment basics

This section describes the common operating systems tasks and how they can be planned and executed through Tivoli Provisioning Server.

Basically, a computer is installed in one of two ways:

- 1. From the image stored on an operating system media, that is, on a CD/DVD or through a reference image file (for example, a Microsoft Windows Imaging (WIM) image). In Tivoli Provisioning Server for OS Deployment, this is known as an *unattended image*.
- 2. From a clone image captured from a referenced machine. This is called a *golden master image*.

In addition to these two methods, Tivoli Provisioning Manager for OS Deployment offers various additional powerful features available through the Tivoli Provisioning Server WEBUI:

- Point-in-time snapshot image capture and restore
- Hardware configuration
- Software modules installation
- Deployment from CD/DVD

We review these features in the following sections. We also show how a sample deployment scenario works and the way a system profile can be customized.

Unattended image

An unattended image is created from a source CD/DVD and represents an operating system setup that does not require user interaction. This is supported for Windows, AIX, Linux, Solaris, and VMWare ESX Server V3.x. You can create an unattended image profile by way of the Tivoli Provisioning Server WEBUI by selecting **Go To** \rightarrow **Deployment** \rightarrow **OS Management** \rightarrow **Unattended Setup Image** and choosing either **Unattended setup (scripted install)** or **Cloning from a reference image file**. The latter can be a Microsoft Windows Imaging (WIM) file, a Solaris Flash Archive (.flar) file, or a Rembo Toolkit header file.

Golden master image

This is a depersonalized boot device image captured from an installed machine. Only Windows and Linux on Intel are supported. This image can be installed on computers different than the one from which it was captured. You can create a clone image by way of the profile wizard after preparing the reference machine. For Windows, you can either let Tivoli Provisioning Manager run the system preparation tool (Sysprep) during the image capture operation or you can run Sysprep manually on the reference machine before starting the capture.

To create a clone profile by way of the Tivoli Provisioning Server WEBUI, select **Go To** \rightarrow **Deployment** \rightarrow **OS Management** \rightarrow **Image Capture** and then specify the reference machine or select the computer, selecting **Go To** \rightarrow **Deployment** \rightarrow **Provisioning Computers panel**, and select **Select Action** \rightarrow **Capture Image**. If you want Tivoli Provisioning Manager to run Sysprep for you when cloning Windows machines, you have to select the check box **Run Sysprep?** in the image deployment page. This check box is present only if Tivoli Provisioning Server knows the Windows operating system type of the reference machine, that is if you performed an initial discovery of the computer by Tivoli Provisioning Manager before starting the cloning operation.

Point-in-time snapshot image

This is an operating system profile captured from an already installed machine without using a system preparation tool to make the image generic. This is supported only for Windows and is only suggested when you want to take a quick snapshot of a system. After restoring the image on the same machine, it is possible that some software applications with a complex configuration might not work properly. You can create a point-in-time snapshot image by way of the Tivoli Provisioning Server WEBUI by selecting Go To \rightarrow Deployment \rightarrow OS Management \rightarrow Image Capture, or by selecting the computer, selecting Go To \rightarrow Deployment \rightarrow Provisioning Computers, and selecting Select Action \rightarrow Capture Image.

Hardware configuration

Hardware configuration is a task that can be easily accomplished by selecting **Go To** \rightarrow **Deployment** \rightarrow **OS Management** \rightarrow **Hardware Configuration Image** for the RAID configuration, BIOS update, BIOS settings, and custom configuration. It requires a hardware environment (created through the same WEBUI link) for each hardware vendor (IBM, HP, Dell, and so on) to be configured. A hardware environment is the place where the hardware configuration task runs. See 14.4, "Hardware configuration" on page 460 to learn about how to create hardware environments and hardware configuration tasks.

Software modules

A software module is a software or drivers package that can be used for deployment and post-installation configuration. A software module can be created by way of the Tivoli Provisioning Server WEBUI by selecting **Go To** \rightarrow **Deployment** \rightarrow **OS Management** \rightarrow **Software Modules** and then selecting **New Software**. Depending on the target operating system you specify in the wizard, Tivoli Provisioning Server for OS Deployment has the capability to install the following items:

- Windows Vista / 2008:
 - Language pack
 - HotFix (MSU)
 - A Windows application installation, using Microsoft Installer (MSI)
 - A Windows driver to include in a deployment
 - A custom action on the target computer; it can be one of these:
 - WinPE 2.0 Ramdisk image
 - A configuration change to perform on the target computer (a command to execute, a registry patch, and so on)
 - A set of files to copy on the target computer (with an optional command to execute)
- Windows 2000 / 2003 / XP:
 - Windows application installation, using Microsoft Installer (MSI)
 - A Windows driver to include in a deployment
 - A Windows Hardware Abstraction Layer (HAL) to include in a clone deployment
 - A custom action on the target computer. This can one of the following:
 - A WinPE 1.5 Ramdisk image

- A configuration change to perform on the target computer (a command to execute, a registry patch, and so on)
- A set of files to copy on the target computer (with an optional command to execute)
- ► Linux:
 - A Linux application installation, using RPM
 - A custom action on the target computer; it can be one of these:
 - A configuration change to perform on the target computer (a command to execute)
 - A set of files to copy on the target computer (with an optional command to execute)
- Solaris:
 - A Solaris package installation, using pkgadd
 - A custom action on the target computer; it can be one of these:
 - A configuration change to perform on the target computer (a command to execute)
 - A set of files to copy on the target computer (with an optional command to execute)
- ► AIX:
 - An AIX application installation, using RPM
 - A custom action on the target computer; it can be one of these:
 - A configuration change to perform on the target computer (a command to execute...)
 - A set of files to copy on the target computer (with an optional command to execute)

Through these options, Tivoli Provisioning Server for OS Deployment can cover most software deployment scenarios (inject drivers during a Windows installation, install applications on various platforms, patch the operating system, and modify the Windows registries) and provide the ability to create universal operating system images. The software module feature can be used also to automatically install the Tivoli Common agent on the deployed operating system.

Tivoli Provisioning Server for OS Deployment provides the way to make the software modules deployment automatic on the target computers through the definition of bindings. In 14.3, "Software modules" on page 426, we provide a detailed explanation about the various software modules and the possible bindings that can be defined.

Deployment from CD/DVD

This feature allows you to create a deployment CD/DVD that is used for installing onto machines in offline mode, or a PXE CD for using Tivoli Provisioning Manager for OS Deployment on PXE-less environments. The generated CD/DVD can be protected by way of an activation code generated by providing a password. This activation code can be time-based and prevents unauthorized personnel from using the image. You can create these CDs by way of the Tivoli Provisioning Server WEBUI by selecting **Go To** \rightarrow **Deployment** \rightarrow **OS Management** \rightarrow **Software Modules** and then clicking the **Generate CD** button. The wizard guides you through the creation of the CD/DVD ISO images.

The available options are:

- ► Create a deployment CD/DVD.
- Create a Network boot CD/DVD.
- Generate a new CD/DVD activation code.

When creating a *deployment CD/DVD*, you can include a deployment scheme, software modules, and system profiles. The process builds an ISO file on the boot server or on any other machine running the Web Interface Extension that you can later burn onto a CD/DVD.

A *PXE-emulation (Network boot) CD/DVD*_emulates PXE on machines that do not have a network card provided by the PXE boot ROM chip. When you create the CD/DVD, you have to specify if the target will use a dynamic or static IP address and what the address of the boot server is that needs to be contacted in PXE mode.

Sample deployment scenario

In the following sample scenario (Windows unattended setup), we explain in detail how the setup profile creation and image deployment (machine installation) processes work. The procedure is as follows:

- Create the unattended operating system profile by way of the Tivoli Provisioning Server WEBUI. The Profile Wizard guides you through the creation of the image. The source image (for example, a Windows image from a CD/DVD) must be on a machine with the Web Interface Extension installed. You can download and install the Web Interface Extension by opening the Tivoli Provisioning Server for OS Deployment WEBUI (by default, http://<tpmfosd_server_IP>:8080) from the machine where you want to install it, go to the Server Status → Web interface extension panel, and download the package for your specific platform.
- 2. After the system profile has been created, you can define one or several software modules (for example, a custom action to perform on the target or a set or drivers to be installed) and decide to bind (to associate) them with the

profile configuration, with a specific target computer (explicitly), or with hosts by automatic binding rules. Refer to 14.3, "Software modules" on page 426 for further details.

- 3. You can define also hardware configurations (for example, a BIOS update or RAID configuration). Refer to 14.4, "Hardware configuration" on page 460 for further details.
- 4. Invoke the Image Deployment application by selecting Go To → Deployment → OS Management → Image Deployment and select the target machine and the image you want to deploy. If Tivoli Provisioning Manager has credentials and can execute commands on the target machine, then it will restart the target computer. In case Tivoli Provisioning Manager cannot manage the target computer, you have to restart the computer yourself.
- 5. Because the boot sequence in the target BIOS is set to network boot first and the DHCP is configured as a PXE client, the target PXE boots into the Tivoli Provisioning Server for OS Deployment boot server and loads the deployment engine, which can perform all kinds of tasks, including operating system installation.
- 6. The target queries the Tivoli Provisioning Server for the relevant OS configuration for deployment.
- 7. The target performs a hardware inventory through DMI and PCI system calls.
- 8. The target queries the ODBC/JDBC database for all relevant information about the operating system and software modules to be installed and generates dynamically a deployment script. If a hardware configuration is sent with the deployment, it is executed before the OS image installation.
- 9. The target hard disk is partitioned according to the information retrieved from the database. A small bootstrap is also written to the hard disk to be able to take over any subsequent reboot on the hard disk.
- 10. The target gets the files from the boot server and stores them in a temporary storage location on the hard disk. This file transfer is done using a secure, robust, and efficient unicast or multicast protocol.
- 11. The operating system installation is executed and, after it terminates, the deployment engine removes itself from memory and allows the computer start the operating system as though the computer was booting normally from the hard disk.

Note: In order to be deployed, the target computer must be managed by Tivoli Provisioning Manager and must have at least one of the following defined:

- Universal Unique Identifier (UUID). This is a property of the server object called: computer.uuid.
- Serial number. This is a property of the server object computer called computer.serialNumber.
- A NIC (network interface card). A NIC that is PXE-enabled and capable of booting from network during computer's startup sequence is also required.

Also, it must meet the minimum hardware requirements to install the operating system.

How to customize a system profile

After your image profile has been created, you can change its properties by selecting **Go To** \rightarrow **Deployment** \rightarrow **OS Management** \rightarrow **Images**. Double-click the image you want to customize and select the **Properties** tab.

C X C Intervence Links Proce Most Vlasted Customize Links Proce Images Images Virtualities Proc List Noge Virtualities Noge Virtualities Proc List Noge Virtualities Virtualities Proc List Virtualities	com https://tpm.rome.com9 otmail Windows Marketpi	9443/maximo/u (login lace) Windows Media) Web Report ⁽¹⁾ Euletins: (0	Windows Mindows	값 • 🚮 •	Google
Most Visited Customize Linis Free H	otmal Windows Marketp	lace 📑 Windows Media 📑	Windows Aligo To i ^{I M} Beports i Align (Center 🖡 Profile 🗮 Ston	
Images Im	A Report Action	Web Review P Bulletins (0	🖉 go To 🔤 Beports 🖷 Start (Center 🔺 Protile 🗮 Sign	
Images Fint List Inoge Variables Pro-		Web Reploy P Bulletins: (0	🕐 😳 To 👘 Beports 🕐 Start (Çenter 🎍 Brotile 🗮 Sign	
Find Indge Variables Pro	th v Select Action	State State State			on dee IBM
List Inoge Variables Pro	an conner conner	- 1 . 2 4	۵		
	isioning Workflows	redentials Properties			
Intege • Safus Windows Server 2003, Enterpl Locale Status • Net Tested •	■	Proper	ies Source Computer Device Driver Creation Date	inage 7/18/09 12:36 AM	
Details					
Boot Server • tonuone Computer Template	con			Image Type • Unattended S	etup 🛩
Software Stack # Filter als 10 10 10	1-1+1+1+				Deenlead ?
Software Stack					
Setup : Windows Server 200 Edition Stack), Enterprise				û
					Select Software Stack
Requirements and Capabilities 🗧 💌 filler - s	1	high an	hina pana pana pana pana pana pana pana p	on phone and a second second second	in an in the growing of the
Requirement		Requirement Typ	•		
		No rows to displ	ψ		

Figure 14-1 Profile properties

In the OS configuration details panel for your image profile, you can edit various tabs, as shown in Figure 14-2.



Figure 14-2 OS configuration details panel

You can edit the following tabs:

- In the General tab, you can set the minimal settings required for the OS configuration to work (for example, the Windows product key, the time zone, the language, and so on) and you can specify the partitions (if any) that you do not want to overwrite with the installation.
- In the Disks tab, you can change the partition layout (add, remove, or size partitions) and browse the contents of the primary partition.
- In the Targets tab, you can configure dynamic target properties by using special keywords that are replaced at run time. The following keywords are supported:
 - [IP]: Full IP address (received by DHCP)
 - [MAC]: Hardware address
 - [SN]: Serial number found in DMI (SMBIOS)

- [BOMID]: Unique target identifier in the OS deployment server database
- [AT]: DMI asset tag
- [GRP]: Deepest administrative group name to which the target belongs
- [DHCPNAME]: Target name known to the DHCP server

If you set the value pc[MAC] in the target name, the computer with MAC address 00-16-41-A8-E9-E4 will be named pc001641A8E9E4. Every keyword supports a range extension that starts with the value 0. For example, [IP3] corresponds to the last byte of the IP address because IP addresses bytes are separated by dots.

- In the Bindings tab, you can see all the bindings linked to the current OS configuration.
- The Windows tab allows you to set Windows-specific information and select the Windows system customization actions that you would like to perform automatically on the target machine (for example, you might want unsigned drivers to be installed automatically without any confirmation during the deployment).

14.2 Parent-child boot servers

We suggest using the parent-child architecture to distribute the deployment workload when handling a large number of computers in different locations. You can keep the files and information up-to-date between parent and child servers through a replication process: all images are automatically replicated from the parent server to all the child servers. For example, all profile images built on children servers are replicated to the parent server, which then distributes those images to all the child server.

The database for such architecture is a central database stored on the provisioning server. The child servers do not have their own database; they point to the parent database. You can decide, at any time, to promote a child boot server to become a parent one: in this case, the OS deployment database will remain the one on the Tivoli Provisioning server even if the parent boot server is on a remote machine.

When you install Tivoli Provisioning Server, you can decide to also install Tivoli Provisioning Server for OS Deployment or you can do it later:

If you install Tivoli Provisioning Server for OS Deployment at the same time you install Tivoli Provisioning Server, a primary boot server will be installed on the provisioning server and this will represent the parent server. You can install child servers later. If you do not install Tivoli Provisioning Server for OS Deployment at the same time you install Tivoli Provisioning Server, you have to rerun the Tivoli Provisioning Server installation again to install the parent boot server on the provisioning server. In this situation, you have to also run the OS deployment server discovery by selecting Go To → Discovery → Provisioning Discovery → Discovery Configurations and clicking the New Discovery Configuration button, as shown in Figure 14-3.

🚱 🖂 C 🗙 🏠 📘	rome.com https://tpm.rome.com:9443/maximo/uijlog	in	公 •	Google	
🙍 Most Visited 📄 Customize Links 📄 i	Free Hotmail 📄 Windows Marketplace 📄 Windows	Nedia 📄 Windows			
Discovery Configurations					
R Discovery Configurations	Constant of the second second Constant of the second second second second second second second second second s	delina:(0) ₱ <u>G</u> o To ⊯ <u>R</u> e	porta 🐧 Start Çentar 🔺 Protile	Sign Out ? Help	IBM.
Find	🚯 🔻 Select Action 🛛 🖌 🔊	214 \$			
List Discovery	New Dis	covery Configuration CTRL+	ALT+I		
🖄 Advanced Search 🔻 📓 Save Query	y 🔻 🖗 Bookmarks				
Discovery Configurations	🚯 : 🚍 : 🛊 🍦 👳 1 - 20 of 43 👳			Ph. Devolgad	7 =
Discovery Configuration *	Description	Category	Method		
AIX Acquire Patches	Acquire patches for AIX 5.2, AIX 5.3 and AIX 6.1.	Software Discovery	AIX Patch Acquire Updates		××
	Scan AIX servers for ML/TL and other and also an extension of the MERCON Resets OFFICE				

Figure 14-3 New discovery configuration

Complete the Name field, select the **Software Discovery** radio button, and select **TPMfOSD Installation Discovery**, as shown in Figure 14-4.

Discoverv	Details
	Name * boot server discovery
	Description
Discovery	Configuration
Category	
C Offwar	re biscovery
C Other	TPMrOSd Installation Discovery

Figure 14-4 Add Discovery Configuration

Click **OK**. In the next panel, shown in Figure 14-5, enter the port number you specified during the Tivoli Provisioning Server for OS Deployment installation into the HTTP server port field (the default values are 8080 for Windows and 8088 for UNIX platforms) and specify the Java API password used for the Tivoli Provisioning Server for OS Deployment installation. When finished, click the after the save your entries and then click **Run Discovery**.

🚱 🔄 🕑 🗶 🏠 🔃 rone.com ktaps://tam.rone.com/9413/maximo/lu/kgin	☆ 🔹 🚺 Google	ß
🚊 Most Vested 📋 Customize Links 📄 Free Hotmail 📄 Windows Narkstplace 📄 Windows Media 📄 Windows		
Discovery Configurations		
C Discovery Configurations	A grotie Sign Cut ? Help	IBM.
₩ Finit # ¥ Select Action ₩ ¥ # List Discovery		
Discovery Configuration • boot server discovery Method TPWrOSid Installation Discovery Cotegory S	Software Discovery	
Discovery Parameters		
HTTP server port = 8000 Pessword ====================================	Run O	peorery

Figure 14-5 Run Discovery Configuration

Select the Tivoli Provisioning Server as your target and click Submit.

The same discovery can be necessary if the creation of an unattended profile image did not exit properly. In such a case, the discovery will be able to discover images that, after the task has finished, can be displayed by selecting **Go To** \rightarrow **Deployment** \rightarrow **OS Management** \rightarrow **Images**.

Note: An existing Tivoli Provisioning Server for OS Deployment V7.1.0 installation is not supported. This is because the Tivoli Provisioning Manager installer will install not only Tivoli Provisioning Server for OS Deployment but will also configure the Java API so that Tivoli Provisioning Server can communicate with it. Furthermore, Tivoli Provisioning Manager for OS Deployment installed through the Tivoli Provisioning installer will use the same database engine as Tivoli Provisioning Server.

If you want to install a child boot server, it must be an existing Tivoli Provisioning Manager managed computer and should satisfy the requirements given in the *Tivoli Provisioning Server 7.1.1 Provisioning User's Guide* at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ibm.t ivoli.tpm.scenario.doc/tpm_user_guide.pdf

You can create a child server by selecting Go To \rightarrow Deployment \rightarrow OS Management \rightarrow Boot Server Installation, select the machine that you want to install as an OS deployment server, and click Submit.

If you want to promote a child boot server to become a parent boot server in order to reduce the workload on the provisioning server, you have to select **Go To** \rightarrow **Deployment** \rightarrow **OS Management** \rightarrow **Boot Servers**, check the **Select Records** check box, choose the child server to be promoted, and select **Select Action** \rightarrow **Promote a child boot server to parent**.

OS deployment servers are configured to replicate objects automatically. Objects are always replicated from the parent to child servers. If a child add objects to a child server, the changes are not replicated to the parent. To view the current replication state, select **Go To** \rightarrow **Deployment** \rightarrow **OS Management** \rightarrow **Boot Servers** and click the name of the server you want to view. Click the **Replication** tab.

14.3 Software modules

In this section, we provide some practical examples about how to create and manage the various software packages for the various supported platforms through the Tivoli Provisioning Server WEBUI.

We also show how to create a software module to install the Tivoli Common Agent on the deployed machine.

Finally, we discuss in detail the various bindings and their usage.

14.3.1 Windows platforms

Here we discuss software modules for the Windows operating system.

A Windows application installation using Microsoft Installer (MSI)

This method is available for Windows 2000, 2003, XP, Vista, and 2008. To use this option, you must copy your MSI file and the related files (cab files and so on) into an empty directory locally on the boot server or on another machine with the Web Interface Extension running. If you do not have an .MSI file but have a self-extracting archive (.EXE), you first execute the archive to extract the MSI file.

After you set up the .MSI file through the wizard, Tivoli Provisioning Server for OS Deployment validates the .MSI file and accesses the vendor package information. During the software module creation, you will be asked for information about the destination folder on the target (where the package will be copied) and the command to be executed for the installation. Default values are provided, but you can customize the various fields based on your needs. See Figure 14-6.

When to app	ly this software module:
Package filer	name on the OS deployment server:
msiimage52E	3E9633E6.pkg
Destination p	bath on the target:
c:\install\setu	pmsi
Command lin	e to run on the target:
MSIEXEC/qt	p /l "chinstall\setupmsi\setup.msi"

Figure 14-6 MSI installation stage, destination folder and command to be run

For example, it could be useful to change the destination path to have all software packages copied to the same location on the target machine or it could be necessary to run a custom MSIEXEC command if you also have a response file (placed in the same directory as the .MSI file) to make the software package installation unattended. You can choose when to install the package during the deployment. Generally this is done when the OS is installed or after one or additional reboots to avoid conflicts with other software packages installations in the same deployment.

After you click **Finish**, the software module is created. You can then change the software module properties through the Software Modules panel by right-clicking the module and clicking **Edit software module**, as shown in Figure 14-7, or by selecting it in the context menu at bottom left of the panel.

SContextual actions
 View software module Edit software module Change icon Delete software module
▶ Cut ▶ Search

Figure 14-7 Contextual actions

When you are in edit mode, you can browse the software module content and, if necessary, upload new files and create new subdirectories. This can be done by clicking the link **Edit software module files**, which will bring up the window shown in Figure 14-8, and selecting one of the options available in the context menu, as shown in Figure 14-9.

🚽 🔍 🔹 🧲 💢 🏠 📋 rome.com https://tpm.rome.com:9443/inaximo/uj/login	습 · 🚺 Google
Most Visited 📄 Customize Links 📄 Free Hotmail 📄 Windows Marketplace 📑 Windows Media 📄 Windows	
Software Modules	
Software Modules	artCenter A Profile Syn Out ? Help IBM.
Fisesame on the US deployment zervet, was mage1CAR653565.prg	
Destination path on the client: c/anstallheetupmei	
Command line to execute: MSIEXEC /gb // "e:Vinatal/Vaetupma/Vaetup.mai "	
Sothware application order: Stage 3 (When the OS is installed)	
Options: none	
Comment by IBM Corporation	
Edit software module files	
MSI Info	
Additional information about the MSI to install.	
Product name: IBM Tryoli Provisioning Hanager for DS Deployment	
Product version: 7.1.08078	
Manufacture: IBM Corporation	
Maintractions: IBM Corporation MSI free and contact and a	
Mainteduxe: IBM Corporation MSITMename: autocati	
Manifecture: IBM Corporation MSI filename: aslup.mai	

Figure 14-8 Software module properties

Bie Edit Yew History Socianaria Toola E	eip			
🔇 🕑 - C 🗙 🏠 🗋 rome.com	https://tpm.rome.com:9443/maximo/ui/k	gin	රු ∙ 🚺• Google	
🛓 Most Visited 🎴 Customize Links 🍈 Free Hotmai	📋 Windows Marketplace 🌔 Window	is Media 📋 Windows		
Software Modules				
Software Modules	C Web Replay	annins: (0) 🕈 Qo To 🔤 Beports 🕈 Stort ()	anter Algrafile Xigin Cut 7 Help	IBM.
		and a second		
Software image explo	orer			- 1
ц, р. (
Folders El Camsimage 10009633E6 pkg	Fielname Fielname	+ Size		
C C manual arconococococo	setup.msi	90 MB		
	🗏 setup <i>ir</i> sp	0 KB		
Contextual actions				
 Expand on local disk 				
• opdate from local disk				
Upload file Add plue directory				
Cut Capy				
+ Delete				_
Back				

Figure 14-9 Upload file

For example, you might need either to align your package to a newer .MSI version or add new additional files. In such a case, use the Delete option to delete the outdated files and use the Upload file option to load the new files.

Including a Windows driver in a deployment

This option is available for Windows 2000, 2003, XP, Vista, and 2008, and is used to provide the appropriate driver files for unattended and clone profiles installation. It can be also useful for injecting drivers for the disk controller (mass storage driver injection) of the target system to avoid deployment failure (which is reported by the appearance of code 0x0000007b on a blue screen).

You have to save your driver files (.inf, .cat, and .sys files) into a directory on the boot server or on a machine with the Web Interface Extension running and provide the path to the Software Module wizard, as shown in Figure 14-10.

Software Wizard	
Please select the folder under multiple drivers are found un prompted for the one(s) you wa single .exe file, you may need folder first.	which the driver files can be found. I ider the selected folder, you will be int to package. If your driver comes as a to uncompress this file in a temporar
Folder: C:\repos\images\e1000dr	v
	 Browse local disk
RHIGHN II NEHICAP III NEHICIN	
	< Prev Next > Cancel

Figure 14-10 Folder where drivers are located

The folder you specify might also contain multiple subfolders with various drivers.

During software module creation, the wizard will ask you if you want to create automatic binding rules based on PCI hardware ID, Baseboard ID, or Target Model name, as shown in Figure 14-11.

You can create binding rules of	describing when your driver must b
deploying among the operating	system. Therefore this driver will b
automatically deployed without	any human intervention. These bindir
rules can be based on several ta	rget characteristics.
 No, do not create automatic b Yes, create binding rules base PCI hardware ID Baseboard ID Target Model name Rules definition will also dep 	ed on: ed on: end on targeted OS type
If you do not create automatic bi	nding rule, you will have to create the
manually later, or you will have t	o deploy this driver explicitely each tim
a deployment requiring it will be p	performed.

Figure 14-11 Automatic binding rules for drivers

You can select one or several options:

If you choose PCI hardware ID, in the next panel, shown in Figure 14-12, you will be prompted to specify whether the drivers will be deployed when the exact device is found on a target machine or even when similar devices are detected. A driver/device will be considered an exact match when the PCI vendor ID, device ID, and subdevice ID matches. If only the PCI vendor ID and device ID match, it will be considered a similar match.

S	oftware Wizard
Yo th W	but can choose to create rules to deploy this driver module only when nis exact device is found, or you may choose to use this driver module then a similar device is found.
A de m	O Use this driver for the exact same device only. • Use this driver for similar devices driver/device will considered an exact match when PCI vendor ID, evice ID and subdevice ID matches. If only PCI vendor ID and device ID hatches, it will be considered similar.
	< Prev Next > Cancel

Figure 14-12 Rules applied to exact or similar devices

If you choose **Use this driver for similar devices** and checked **PCI hardware ID**, Tivoli Provisioning Server for OS Deployment will evaluate the Vendor ID and Device ID values from the PCI device scan for the target machines in a deployment and will check if they match the same information inside the driver .inf files included in the software module. It they match, the driver is applied to the machines that satisfy the rule.

If you choose Baseboard ID, you will be prompted to specify the target machine baseboard ID that should be matched to apply the driver. If you choose Target Model name, in the next panel, shown in Figure 14-13, you will be prompted to specify the target machine model that will satisfy the rule. You can select an already recognized model or just type a sub-string that might be contained in the model name.

⊛the n Othe n	nodel name con nodel name is o □ VMware ESX	tains ne of the follo Guest	wing:	-
	🗆 VMware Virtu	ial Platform Ni	one	

Figure 14-13 Model matched to apply the driver

After specifying the information related to the automatic binding rules, as shown in Figure 14-14, if you decided to select any, you have to specify at which installation stage the drivers will be installed and the path where the installation files are stored on the target system.

When to apply this	software module:
When the OS is Package filename or	nstalled
edrv2A489633E6.pk	
Destination path on	the target:
\drivers\Net-93B26F	2
Note: Drivers must l	be stored in the \drivers folder

Figure 14-14 Installation details for the drivers

In the field, *When to apply this software module*, select **When the OS is installed**. The path in the field, *Destination path on the target* must start with \drivers.

Additional instructions for Windows Vista/2008

For Windows Vista/2008 targets, because WinPE manages the operating system installation, a driver need to be injected into the WinPE software package automatically created when you create the first Windows Vista/2008 unattended profile. Therefore, for Windows Vista/2008 software modules with drivers, you have to do the following steps:

 Install the Microsoft tool Windows Automated Installation Kit (WAIK) tool and the "Web Interface extension" on a machine (or just install WAIK on the Tivoli Provisioning Server for OS Deployment machine), as shown in Figure 14-15.



Figure 14-15 WAIK installation wizard

Notice that WAIK requires a reboot of the computer after its installation. The WAIK is licensed to you by a third-party vendor and not by IBM.

- 2. Create a standard software package with drivers, as described in, "Including a Windows driver in a deployment" on page 430.
- Select Go To → Deployment → OS Management → Software Modules, select the WinPE2 package created automatically by the Vista/2008 unattended image creation, right-click and select Edit software module, and select the Update drivers link, as shown in Figure 14-16.

Ele Edit View History Bookmarks Iools Help				
🌀 🔄 - C 🗙 🏡 📄 rome.com https://tpm.rome	.com:9443/maximo/ui/login		☆·	3 Good
🔊 Most Visited 📋 Customize Links 📄 Free Hotmail 📋 Windows M	arketplace 📄 Windows Media 📄 Window	vs		
Software Modules				
Software Modules	O Web Replay 🤷 Building: (0) 🤌 g	20 To 🤄 Beports 🕈 Start Center	Profile	× Sign Out
Software details				
This page shows details about the selected so automatic binding rules for this software module.	oftware module, and shows the	list of		
Software module information		Edit		
Description: Microsoft Window Vernion: 1 (2003.07.34.17) Seffware models type: A Windows Vista Compatible 05: Windows Vista Required 05 Build: 50,8000 Required 05 Build: 50,8000 Filename on the 05 deployment server: stporndv/286388 Destination path on the elifent: Software application order: Stage 3 (When the Options: none Comment: Version 6.0 build	vs Longhern Win PE 8.0.8000 :37:03.925) (disk image :5.pkg te OS is installed) a ticcoo Fickly virtual disk Updates	image		
Software binding rules				
New rule Back				

Figure 14-16 Update drivers

4. Select the machine that has WAIK and the Web Interface Extension installed on it and select the drivers software module to be updated, as shown in Figure 14-17.

6.0.6000 t	be updated with:	ant Microsoft	windows Longr	iorn wine
II 🕮 🖂	tel Net driver (2) tel Net driver (ver. O	8/20/2008 - 12	2/11/2008)	1
		0/20/2000 - 12	., 11,2000,	
				-

Figure 14-17 Drivers to be updated in the WinPE2

Follow the wizard to finalize the update operation.

A custom action on the target computer: a WinPE 2.0 Ramdisk image

This option is available only for Windows Vista and 2008. You can create a WinPE2 software module from the Vista/2008 installation files. The WinPE2 software package creation requires that the computer where the source images for Vista/2008 are located has:

- A Windows 32-bit operating system
- ► The Web Interface Extension started with local administrator privileges
- ► The Windows Automated Installation Kit (WAIK) installed

To create the software module, select **Go To** \rightarrow **Deployment** \rightarrow **OS Management** \rightarrow **Software Modules** and click the **New** software button. Then select **A WinPE 2.0 Ramdisk image** and follow the wizard by providing the machine where the Windows Vista/2008 CD/DVD image is available and where the Web Interface Extension is running.

Language pack and HotFix (MSU)

These two options are available only for Windows Vista and 2008. You can deploy software modules with Language Packs and HotFixes with:

- A golden master image
- Unattended setup
- Unattended profiles (cloning) from a reference file (WMI file)

Select Go To \rightarrow Deployment \rightarrow OS Management \rightarrow Software Modules, click New software, select Windows Vista / 2008, and then choose either Language pack or HotFix (MSU). The wizard guides you in creating the Language Pack/HotFix software module. Notice that the source image must be on a computer with the Web Interface Extension running and:

- For Language pack: The directory containing language pack files must contain a file with a .cab extension.
- ► For HotFix: The directory containing the HotFix files must contain a file with a .msu extension.

A custom action on the target computer: a configuration change to perform on the target computer

This option is available for Windows 2000, 2003, XP, Vista, and 2008 and is useful if you want to execute one of the following operations:

- Copy and execute a single file.
- Apply a Windows registry change.
- Apply a Windows .ini file change.
- Copy a single text file.
- Execute a single command file.
- Boot a virtual floppy disk.

For example, if you want to boot your computer from a virtual floppy disk located locally on the target or on another machine running the Web Interface Extension, you can choose to boot a virtual floppy disk. To do this task, select **Go To** \rightarrow **Deployment** \rightarrow **OS Management** \rightarrow **Software Modules**, click **New Software**, and choose the specific Windows operating system type. Then select **A custom action on the target computer**, select **Configuration change**, and finally select **Boot a virtual floppy disk**.

The computer where the bootable diskette is read from can be either the local computer or another computer running the Web Interface Extension. The option "On the server itself" must not be used. If the diskette drive is added after the Web Interface Extension is started, it might be necessary to stop and start the Web Interface Extension to enable it to detect the diskette drive.

A custom action on the target computer: a set of files to copy on the target computer (with an optional command to execute)

This is available for Windows 2000, 2003, XP, Vista, and 2008, and allows you to copy the content of a directory to the target computer and to execute a command.

For example, we have a software image setup (an executable with additional files) and we want to run the setup command with additional options to make it run in unattended way during the deployment. Select **Go To** \rightarrow **Deployment** \rightarrow **OS Management** \rightarrow **Software Modules**, click **New software**, click either **Windows Vista / 2008** or **Windows 2000 / 2003 / XP** (depending on your needs), then click **A custom action on the target computer**, as shown in Figure 14-18.



Figure 14-18 Custom action selection

Finally, click **A set of files to copy on the target computer (with an optional command to execute)**, as shown in Figure 14-19.

OA WinPE 1.5	Ramdisk image			
○ A configurati (a command	on change to perf to execute, a regi	orm on the tar; stry patch)	get computer	
A set of files (with an opt	to copy on the tar ional command to	get computer execute)		

Figure 14-19 Set of files to copy on the target computer

After clicking **Next**, you must specify the computer with the Web Interface Extension running where the folder with the source files is located. Specify the full path to that directory, as shown in Figure 14-20.

Software Wizard
Select the folder where you have the files you would like to copy to the target computer during the deployment. IBM Tivoli Provisioning Manager for OS Deployment will package all the files and folders contained in the selected folder.
Folder: C:\repos\images\Mozilla Firefox setup
 Browse local disk.
< Prev Next > Cancel

Figure 14-20 Folder with files to be copied
Specify a meaningful name to identify the specific software module, as shown in Figure 14-21.

Software Wiz	ard and a second se
Please enter Tivoli Provisio	a description to identify your software module in the IBM ning Manager for OS Deployment database.
Description:	Mozilla Firefox setup
Comment:	
	(Prev Nevt > Cancel

Figure 14-21 Software module description

The contents of the previously specified directory will be copied to a destination folder that you specify in the panel shown in Figure 14-22.

Deployment will use to create	e the software module:
When to apply this software	module:
MI After one additional rebo Package filename on the OS	denlovment server:
mzllfrfx754C9633E6.pkg	
Destination path on the targ	et:
c:\install\Mozilla Firefox setup	
Command line to run on the	target:
"c:\install\Mozilla Firefox setup	VFirefox Setup 1.5.0.6.exe" -sm -ma

Figure 14-22 Software module details

Also, you can enter a command in the field, *Command line to run on the target*. In this example, the command, with additional options, launches the Firefox setup in unattended mode. You also must choose when the software module is applied. We suggest choosing either **When the OS is installed** or one of the stages with additional reboots (for example, **After on additional reboot**). The latter options are used when you deploy several software modules and you want to avoid conflicts.

A Windows HAL to include in a clone deployment

This option is available only for Windows 2000, 2003, and XP, and is required to inject a Hardware Abstraction Layer (HAL) when deploying clone profiles to different hardware.

HAL is an abstraction layer acting between the physical hardware and the software that runs on that computer. In case the HAL in the clone profile is not the right one for the target hardware, you receive a blue screen during the deployment that shows the code 0x0000007b.

You can create a software module including a Windows HAL by selecting Go To \rightarrow Deployment \rightarrow OS Management \rightarrow Software Modules, clicking New software, clicking Windows 2000 / 2003 / XP, and then clicking the A Windows HAL to include in a clone deployment option, as shown in Figure 14-23.

Software V	Vizard				
Then choo below:	se the type of p	ackage you	would like to	o create in the	e lis
O A Wind O A Wind O A Wind O A custo	ows application in ows driver to inclu ows HAL to includ m action on the t	nstallation, us ude in a deple le in a clone d arget comput	sing Microsoft oyment deployment ter	Installer (MSI))
			< Prev N	ext > Can	el

Figure 14-23 Windows HAL selection

The HAL DLLs are located either in a standard Windows installation CD-ROM or in a folder in which you have copied the I386 (or AMD64) directory, as shown in Figure 14-24.



Figure 14-24 Folder for HAL files

In Figure 14-25, you have to choose the HAL driver specific to the hardware type of the target machine.

Multiple HAL types h Select the hardware and click on Next to get more details on	lave been found. e type for which you want a package to be created or go to the next step. You can click on each name to the type of hardware.
OS detected:	Windows Server 2003, Enterprise
OS architecture:	i386
Hardware type:	O acpipic_up Omps_up Omps_mp O acpiapic_up ⊙acpiapic_mp

Figure 14-25 HAL selection

Choose the automatic bindings based on the operating system deployed, the HAL type, the target architecture, and model name so that the software module is automatically deployed on hosts matching the criteria, as shown in Figure 14-26.

Software Wizard	
You can create binding rule: deployed among the opera automatically deployed with rules can be based on severa	s describing when your new HAL must be ating system. Therefore this HAL will be out any human intervention. These binding al target characteristics.
 No, do not create automa Yes, create binding rules binding rules ✓ OS Deployed ✓ HAL Type ✓ Target Architecture ✓ Target Model name 	itic bindings rules. based on:
If you do not create automat manually later, or you will ha deployment requiring it will be	ic binding rule, you will have to create them ve to deploy this HAL explicitely each time a e performed.
	< Prev Next > Cancel

Figure 14-26 Bindings rules of HAL

You have also to choose the specific OS architecture (32-bit, 64-bit, or any), as shown in Figure 14-27.

Software Wizard
If you do not choose the right parameters, you may get a blue screen of death at start up time on target computer.
OS achitecture:
HAL Type: Y ACPI Multiprocessor PC', ACPI APIC MP (Halmacpi.dll)
OS targeted:
< Prev Next > Cancel

Figure 14-27 Architecture specification

Specify the target machines models to which the HAL software module will apply, as shown in Figure 14-28.

oftware Wizard	
pecify the target machine model river.	that should be matched to apply th
Deploy driver module only if • the model name contains • the model name is one of the fo • VMware ESX Guest • VMware Virtual Platform	Illowing:

Figure 14-28 Machine model specification

In order to cover all HAL types, you can simply create various software modules, each containing a different HAL type for a particular Windows operating system. If you select the automatic bindings rules option, the correct HAL will be automatically injected when the specific operating system clone profile is deployed on certain hardware.

A custom action on the target computer: a WinPE 1.5 Ramdisk image

This option is available for Windows 2000, 2003, and XP, and allows you to create a WinPE 1.5 Ramdisk image from your Windows 2000, 2003, or XP image CD/DVD. Select **Go To** \rightarrow **Deployment** \rightarrow **OS Management** \rightarrow **Software Modules** and click **New software**. Click **Windows 2000 / 2003 / XP** and **A WinPE 2.0 Ramdisk image**. When prompted, provide the name of the machine where the Windows 2000, 2003 or XP CD/DVD image is available and where the Web Interface Extension is running.

14.3.2 Linux

The following software module options are available for Linux target computers:

- A Linux application installation, using RPM.
- A custom action on the target computer; it can be one of these:
 - A configuration change to perform on the target computer (a command to execute)
 - A set of files to copy on the target computer (with an optional command to execute)

Basically, you can provide an RPM to be installed, or specify a command to be executed or a set of files to be copied on to the target computer with a command to be run. The wizard will guide you through the specific software module creation. This is similar to the related option available for MSI packages (Windows).

14.3.3 AIX

The following software module options are available for AIX target computers:

- An AIX application installation, using RPM.
- ► A custom action on the target computer; it can be one of these:
 - A configuration change to perform on the target computer (a command to execute)
 - A set of files to copy on the target computer (with an optional command to execute)

Basically, you can provide an RPM package to be installed, or specify a command to be executed or a set of files to be copied on to the target computer with a command to be run. The wizard will guide you through the specific software module creation.

14.3.4 Solaris

The following software module options are available for Solaris target computers:

- ► A Solaris package installation, using pkgadd.
- A custom action on the target computer; it can be one of these:
 - A configuration change to perform on the target computer (a command to execute)

A set of files to copy on the target computer (with an optional command to execute)

Basically, you can provide a Solaris package to be installed, or specify a command to be executed or a set of files to be copied on the target computer with a command to be run. The wizard will guide you through the specific software module creation.

14.3.5 Tivoli common agent software modules

Tivoli Provisioning Manager for OS Deployment provides the ability to create a software module that includes the Tivoli common agent installation, which then can be deployed with an operating system image on target computers. This feature requires that the common agent manager be installed on the Tivoli Provisioning Manager server. This is usually done during the Tivoli Provisioning Server installation.

You can create the Tivoli common agent software modules for each supported platform by selecting Go To \rightarrow Deployment \rightarrow OS Management \rightarrow Boot servers, selecting Select Action \rightarrow Create Tivoli Common Agent Software modules, and clicking Yes, as shown in Figure 14-29.

	rome.com https://tp	m.rome.com:9443/maximo/ui/login	습· 🖁
isted 📄 Customize Links [🖞 Free Hotmail 📋 Win	dows Marketplace 📋 Windows Media 📋 Windo	ws
Servers			
ot Servers		O Web Replay P Dublins (0) 🎓	Go To Lid Beports III Start Center ▲ Brotile Sign
Y Find:	n 🗸 Selec	t Action 🛛 🖌 🎽 🖌 🖉	
Boot Server Varia	oles Workflor	Create Tivoli Common Agent Software Modules Delete Bootserver	tion
Boot Server tpm.rome.com		Add to Booknarks	Type × TPM for OS Deployment
Network Interface		Add Credentials	
Filler) (2) 🕈 🛊 🔍			
NC	MAC	Group	Netboot Enabled
		No rows to disp	lay
	sted Customize Links Servers of Servers M Find: Boot Server Varial Boot Server Varial Network Interface Filler	sted Customize Links Free Hotmall Win Servers of Servers W Find: Boot Server Variables Workfor Boot Server Variables Nic MAC	sted Customize Links Pree Hotmal Windows Marketplace Windows Media Windo Servers dt Servers tt Servers Windows Marketplace Windows Media Windows Servers Windows Marketplace Windows Media Windows Media Windows Marketplace Windows Media Windows Media Windows Marketplace Windows Media Windows Media Windows Server Server Variables Workflor Delete Bootserver Add to Bookmarks Add Credentials Media Credentials Mile MAC Group No rows to disp

Figure 14-29 Create TCA software module

This task can be monitored through the Provisioning Task Tracking application.

Before submitting the task, verify that the following requirements have been met:

- The local repository (TIO_HOME\repository) must contain one file named common_agent_1.4.2.0_<date>_<platform>.tar for each of the supported platforms (AIX, Linux_ppc, Linux, Solaris, and Windows). The <date> represents the package date.
- TI0_HOME\tools\prepare_tca_image must contain all the scripts used by Tivoli Provisioning Server for OS Deployment during the offline Tivoli common installation on the target system.
- TI0_HOME\tools must contain the prepareTCAImage script (.cmd or .sh). This is the script used to create the installation packages for each platform with the related response file called caInstall.rsp.

After the task has finished, you will find various TCA software modules under the Software Modules tab, as shown in Figure 14-30. You can view these modules by selecting **Go To** \rightarrow **Deployment** \rightarrow **OS Management** \rightarrow **Software Modules**.



Figure 14-30 TCA software modules

After selecting the image profile (by selecting **Go To** \rightarrow **Deployment** \rightarrow **OS Management** \rightarrow **Image Deployment**), you can install the Tivoli common agent by selecting **Install Tivoli Common Agent**?

14.3.6 Bindings

There are two types of bindings:

- Automatic binding rules
- Manual bindings

Automatic binding rules

Automatic binding rules are used to link software modules/OS configurations to targets without having to specifically bind them on each target. Rules are created in each software module and determine which targets will automatically be bound to the software module/OS configuration. Rules are created from criteria and values. If a target has a matching value for all criteria in the rule, the software module/OS configuration will be bound to that target. The bindings will be displayed with the notation "by rule".

You can add automatic binding rules for software modules or an OS configuration as follows:

 To add automatic binding rules for software modules, select Go To → Deployment → OS Management → Software Modules, right-click the software module, and click Edit software module or select the same option in the context menu at bottom left of the panel. The panel shown in Figure 14-31 opens.

C X A C X A	str • 🛃• Goode
	[4]
🖹 Most Visited 📄 Custonize Links 📄 Free Hotmail 📋 Windows Marketplace 📋 Windows Media 📄 Windows	
Software Modules	
Software Modules O two finally - D two finally - D badmit (0) - Co To Le Parente - A	Startighter Africa Alignida 7 htp IBM.
Firefulne on the Ub depiriyment zervet was mage1CARHSSHEEprop	
Destination path on the client: clinetall/setupmsi	
Command line to execute: MSIEXEC /gb // "eximatellaetupma/tetup.mai"	
Somvare application order: stage 3 (when the US is installed)	
opros. Hone	
Comment By IBM Corporation	
Edit software module files	
MSI Info	
Additional information about the MSI to install.	
Product hams: IBM Twoli Provisioning Hanager for DS Deployment	
Product version: 7.1.08078	
Manufacture: IBM Corporation	
Misi Tolehame: izatup.mai	
Software binding rules	
The following binding rules implicitly bind this software module to any deployment object	
matching all criteria of any single rule.	

Figure 14-31 Adding software binding rules

2. Click **New rule** and select the rules you want to be applied to target systems deploying the current software module, as shown in Figure 14-32.

escription:	-				
eployment scheme	v	(any)	System categ 0	۷	(anv)
vstem Profile	~	Setup : Windows Server 2003, Ent	System categ 1	¥	(any)
urrent OS	-	(apy)	System categ 2	Y	(anv)
onfiguration		(aii)	System categ 3	¥	(any)
roup	*	(anv)	User categ 0	¥	(anv)
S type	۷	(any)	User categ 1	¥	(any)
S version	۷	(anv)	User categ 2	¥	(anv)
S language	*	(any)	User categ 3	Y	(anv)
S architecture	~	(any)	User categ 4	¥	(anv)
odel	*	(any)	User cated 5	Y	(any)
IOS version	۷	(anv)	User cateo 6	*	(any)
CI device	¥	(any)	User categ 7	*	(any)
ase board	¥	(anv)	User categ 8	v	(any)
ultiChassi	¥	(any)	User categ 9	¥	(any)
	_				((carty)

Figure 14-32 Binding rules definition

For example, if you specify a rule based on "System Profile", the software module will be deployed any time the specific system profile is deployed to a target system. As another example, to create a binding based on the operating system type of the target, choose an operating system value for the "OS type" so that the software module will be installed on any target deployed with that specific operating system type. You can also enter a free-text condition following the Rembo-C syntax (this is for advanced users).

After you have built your automatic binding rules for software modules, you can view them in the Software bindings view by selecting **Go To** \rightarrow **Deployment** \rightarrow **Provisioning Computers**, selecting the appropriate computer in the list, and selecting the **Bindings** tab inside Deployment Properties. To add automatic binding rules for OS configurations, select Go To → Deployment → OS Management → Images, click the specific image profile, select Properties, and then select the Bindings tab, as shown in Figure 14-33.

Elle <u>E</u> dit <u>Vi</u> ew History <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp	. 0
C X 🚯 Tome.com https://tpm.rome.com:9443/maximo/ui/login	습 • [
🙍 Most Visited 📋 Customize Links 📋 Free Hotmail 📋 Windows Marketplace 📋 Windows Media 📋 Windows	
🗋 Images 🔅	
Images 🖉 Web Replay 📍 Bulletins: (0) 🎓 Go To 👫 Reports 🂠 Start Center 🎜	Profile
🗸 🗸 Find: 💦 🖓 Select Action 🔽 🎽 🛃 🧶 🖗 💠	
List Image Variables Provisioning Workflows Credentials Properties	
Image * Setup : Windows Server 2003, Enterprise Editi	
OS configuration details General Disks The following binding rule automatically bind this OS configuration to any target matching	
all criteria of any single rule.	
Innerit parameters New rule	

Figure 14-33 OS configuration bindings

4. Click **New rule** and set the rules you want to be matched, as shown in Figure 14-34.

OS configuration bi	ndings
By entering an autor this OS configuration criteria.	matic binding rule, you will implicitly bind n to any target matching the selected
Description:	
Deployment scheme	♥ (any)
Administrative group	(anv)
Model	✓ (anv)
User categ O	✓ (anv)
User categ 1	✓ (anv)
User categ 2	✓ (anv)
User categ 3	(anv)
free-text condition	
	OK Cancel

Figure 14-34 OS configuration bindings

You can, for example, select a specific target model to be matched.

After you have built your automatic binding rules for the OS configuration, you can see the rules by selecting **Go To** \rightarrow **Deployment** \rightarrow **Provisioning Computers**, select the appropriate computer in the list, select the **Bindings** tab inside Deployment Properties, and look in the "OS configuration bindings" section. The specific binding is reported as "by rule":

Eile Edit View History Bookmarks Tools Help			<i>"</i> "
C X 🏠 🔽 http://www.com/	s://tpm.rome.com:9443/maximo/ui/login		☆ • Koogle
🙍 Most Visited 📋 Customize Links 📄 Free Hotmail 📗) Windows Marketplace 📄 Windows Media 📗	Windows	
Provisioning Computers			
Provisioning Computers	🕑 Web Replay 🤚 Bulletins:	(0) 🖗 <u>G</u> o To 🔟 <u>R</u> eports 👫 Star	t <u>C</u> enter [▲] Profile [★] Sign Out ? Help ፲물
💌 Find: 🛃 💏	Select Action 🛛 🕑 🚯 🍃	.] 💠 🧼 🧀	
List Computer Hardware Software	Compliance Recommendations	Credentials Workflows	Variables Deployment Properties
Computer pc-005056963AD2	Management IP Address 10.1.2.34		Operating System
Target details for bmtl- Target Bindings OS configuration bindings The list below shows OS configuration decision whether or not to annly a ne	00:50:56:96:3A:D2	Task history	
on properties that are only available a	at deployment time.		
Setup : Linux RHELS Setup Setup : Windows Server 2003, Enterp	explicit prise Edition by rule	S.	
software bindings		Edit	
The list below shows software modu extra packages may apply according t	les bound to the selected target. No o the actual configuration deployed.	lote that	
Wake on LAN			

Figure 14-35 OS configuration bindings

Manual bindings

You can explicitly bind software modules/OS configurations to targets in order to enable their automatic deployment. This can be done by selecting **Go To** \rightarrow **Deployment** \rightarrow **Provisioning Computers**, selecting the appropriate computer in the list, clicking the **Deployment Properties** tab, and clicking the **Bindings** tab. You can either select **Edit** for the "OS Configuration bindings" or the "Software bindings" and select the OS configuration/software module to associate with this computer. The binding will be reported as "explicit".

Note: When you deploy a system profile to a target system, the related OS configuration chosen for the deployment is automatically bound to the target computer. The configuration will be shown on the boot menu every time the target PXE boots so that the user can manually restart the deployment of the already deployed OS configuration. You can remove or modify that OS configuration bound to the target by selecting **Go To** \rightarrow **Deployment** \rightarrow **Provisioning Computers**, selecting the appropriate computer in the list, clicking the **Deployment Properties** tab, and clicking the **Bindings** tab.

14.4 Hardware configuration

You can create hardware configuration tasks for:

- RAID Configuration: To create a RAID configuration regardless of the vendor
- BIOS Update: To update the BIOS firmware on the target
- BIOS Settings: To update the BIOS and Baseboard Management Controller (BMC) through an initialization file
- Custom Configuration: To perform your own configuration based on tools and a command to be applied to them

To use this feature, you need to create a hardware environment for each hardware vendor (for example, IBM, HP, Dell, and so on) you want t as a target. Therefore, you need to:

- 1. Create a hardware environment specific to each hardware vendor.
- 2. Create a hardware configuration task through the Tivoli Provisioning Server WEBUI to run the specific operation (for example, a RAID configuration) on a target host. During task creation, you have to specify the hardware environment to be used.

A hardware environment is the place where the hardware configuration task runs. It is composed of:

- An operating system that can be, for example, WInPE or DOS
- A vendor specific scripting toolkit

Both run in a ramdisk to access the host machine. The following operating systems are supported:

- DOS (only for older hardware)
- WinPE 1.x and WinPE 2.x

The following scripting toolkit tools are supported (for the various hardware vendors):

- For IBM: ServerGuide[™] Scripting Toolkit (SGST) running in DOS, WinPE 1.x, and WinPE 2.x
- ► For Dell: Dell Scripting Toolkit running in WinPE 1.x.
- ► For HP: HP SmartStartTM Scripting Toolkit running in WinPE 1.x.

Here is the step-by-step procedure to create a hardware environment based on the IBM ServerGuide Scripting Toolkit (SGST) running on WinPE 2.x:

- 1. Ensure that you are using a computer with a 32-bit architecture running the Web Interface Extension under Windows XP, 2003, Vista, or 2008. Windows 2000 is not supported. If your Tivoli Provisioning Server does not satisfy these requirements, you must use a computer with those characteristics. Ensure that the Web Interface Extension has been started with local administrator privileges on that machine.
- 2. Because the hardware environment leverages the Windows Imaging Format (WIM), you need to install Microsoft Windows Automated Installation Kit (WAIK) 32-bit on the machine with the Web Interface Extension. WAIK is licensed to you by a third-party vendor and not by IBM. You must reboot the computer after completing the WAIK installation.
- 3. Download the latest IBM ServerGuide Scripting Toolkit WinPE 2.x, which can be found at the following address:

http://www-947.ibm.com/systems/support/supportsite.wss/docdisplay?ln docid=SERV-TOOLKIT&brandind=5000008

- 4. Extract the software package to a folder (for example, C:\SGST_WINPE2) on the machine where you installed WAIK and where the Web Interface Extension is running.
- 5. Run the script SGTKWinPE.cmd from C:\SGST_WINPE2\sgdep1oy\SGTKWinPE with the following arguments (refer to the IBM ServerGuide documentation for more information):

SGTKWinPE.cmd /Image ScenarioINIs\Local\Raid_Config_Only.ini

Press Enter when prompted to continue the execution.

 After SGST is installed, select Go To → Deployment → OS Management → Hardware Configuration Image. Select any option (for example, RAID Configuration) and click Next. The panel shown in Figure 14-36 opens.

Now you have to choose the	targeted computer model and matching
environment required to run	hardware configuration on this specifi
model. Model name can contair	wildcards.
Model: Environment:	
No preboot environment,	please create a preboot environmen
before continuing. Click here to create a new preb	poot environment.

Figure 14-36 HW configuration wizard

7. Click **here** to create a new preboot environment. The panel shown in Figure 14-37 is displayed.

Hardwafe Environment wizard	
This wizard will help you to create a configuration utilities	new environment to run hardware
	Next > Cancel

Figure 14-37 Hardware environment wizard

8. Click **Next** and specify the 32-bit machine where you placed SGST and where WAIK is installed and the Web Interface Extension is running. In the next panel, shown in Figure 14-38, specify the directory where the scripting toolkit is installed. Generally, it is the directory named ISO.

Hardware Environment Wizard	
Choose the folder where the vendor s	specific scripting toolkit is installed
Toolkit: gdeploy/WinPE_ScenarioOutpu	tt\Local_Raid_Config_Only\ISO
	Browse local disk.

Figure 14-38 Scripting toolkit folder

9. Click **Next** and specify the folder where WinPE is located, as shown in Figure 14-39. Generally, it is the same ISO directory specified in the panel shown in Figure 14-38 on page 464.

Hardware Environment Wizard	
Choose the folder where WinPE material can be found	
WinPE: ksgdeploy/WinPE_ScenarioOutput\Local_Raid_Config_Only\ISO Browse local disk.	
< Prev Next > Cancel	

Figure 14-39 WinPE folder

10. When you click **Next**, the hardware environment software module is created, as shown in Figure 14-40.

Hardware Environment Wizard
Hardware configuration environment creation successful !
The new hardware environment has been successfully created, you can now use it to run a hardware configuration within a deployment on a target.
Be aware that the hardware environment has been created as a software module and visible also in 'Hardware Configuration Environments' folder.
Click finish to close this wizard.
Finish

Figure 14-40 Successful hardware environment creation

11. To view the hardware environment software module, select **Go To** \rightarrow **Deployment** \rightarrow **OS Management** \rightarrow **Software Modules**, and the panel shown in Figure 14-41 opens, where you can see the module.



Figure 14-41 Hardware environment software module

A similar sequence of steps is necessary to create hardware environments for other hardware vendors (such as HP, Dell, and so on). However, for further details, refer to the Tivoli Provisioning Server for OS Deployment documentation:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp

Now that you have created the hardware environment (specifically for IBM computers in the above example), select Go To → Deployment → OS Management → Hardware Configuration Image and select the hardware configuration you want to execute (for example, a RAID configuration).

2. In the next panel, shown in Figure 14-42, you have to specify the hardware environment to use and the target machine models for which the hardware configuration must be run (wildcards are supported).

Now you have environment re model. Model na	to choose the targeted computer model and matchin equired to run hardware configuration on this specif ame can contain wildcards.
Model: Environment:	 ✓ [↑] Hardware Config. Environment: WinPE 2.x (IBM)
Click bara to err	aste a new prehoot environment
	sate a new probate chartenine inc.

Figure 14-42 Computer model specification

The wizard will guide you through the specific hardware configuration configuration.

3. After the hardware configuration task has been created, you can edit it by selecting **Go To** → **Deployment** → **OS Management** → **Images** and making your changes there.

14.5 Unattended setup

In this section, we show some step-by-step scenarios about how to create Windows and Linux unattended profiles. More specifically, we show how to create Windows 2003, Windows Vista, and Linux Red Hat 5 unattended profiles. Notice that these scenarios can be easily generalized because the same procedure that we use for Windows 2003 applies also to Windows 2000 and XP, the one that we use for Windows Vista applies to Windows 2008, and the procedures for the various Linux versions are quite similar. We also provide the basic requirements and steps to create and deploy unattended profiles for AIX, Solaris, and Linux on PPC.

Now we discuss in detail how the unattended image profiles are created.

14.5.1 Windows

Here we discuss the creation of unattended image profiles for the various supported versions of the Windows operating system.

Windows 2003

Basically, you need to have the Windows 2003 source image available on a machine running the Web Interface Extension:

 After selecting Go To → Deployment → OS Management → Unattended Setup Image, choose Unattended setup (scripted install) and then A Windows 2000/2003/XP system profile. The wizard prompts you to specify the computer where the material to create your profile can be found (it can be the boot server itself or another computer with the Web Interface Extension running) and the directory where the image is located. 2. Notice that the folder you specify must be the one containing the I386 or AMD64 subdirectory, as shown in Figure 14-43.

Specify the folder where Windo either the root directory of a st another folder in which you have	ws setup files can be found. It can andard Windows installation CD-ROM, copied the I386 (or AMD64) directory
Folder: C:\repos\images\Win200	► Brow

Figure 14-43 Windows image folder

3. After clicking **Next**, if the folder is the correct one, the wizard recognizes the specific Windows operating system contained in the source image, as shown in Figure 14-44.

Profile Wizard
The following operating system was detected in the installation folder that you selected. To continue, click Next.
Setup : Windows Server 2003, Enterprise Edition
< Prev Next > Cancel

Figure 14-44 Windows operating system detection

4. You will be prompted to specify the partition size (in percentage of total disk space or MB) in panels shown in Figure 14-45 and Figure 14-46.

The wizard helps you creat this profile to install Windov sizes.	te a partition layout for computers that use vs. Choose how you want to specify partition
 O Specify partition sizes in ● Specify partition sizes as 	MB a percentage of total disk space
	< Prev Next > Cancel

Figure 14-45 Windows partition layout

Profile Wizard
FAT 16 FAT 32 INFS
Size: 100 % (100% remaining free)
Note: FAT16 partition size is limited to 2048 MB.
< Prev Next > Cancel

Figure 14-46 Windows partition size

5. In the next panel, you can enter a product key. If you specify an incorrect key, a new one will be requested during the deployment. If you do not specify the product key, you can set it on the target computer properties. This might be the case if you need separate product keys per computer.

After specifying the product key and clicking **Next**, the panel shown in Figure 14-47 is displayed.

Profile Wizard	
You may specify a you deploy this sy be set individually interactively.	additional fixed properties to use for all machines that ystem profile on. If left blank, these properties have to for each target or Windows setup might ask for them
Registered owner:	IBM
Organization:	IBM
Admin password:	•••••• Confirm: ••••••
Time zone:	✓ (GMT+01:00) Amsterdam, Berlin, Vienna
Language:	✓ Italian (Italy)
Note: You will be editing the Details > O	able to customize additional properties later on by newly created OS configuration (under Profiles > View S configuration).
	< Prev Next > Cancel

Figure 14-47 Windows details specification

- 6. Here you can specify additional fixed properties for all the deployed machines. If you do not specify them, you have to edit the properties of each computer to be deployed; otherwise, the Windows setup might ask for them during the deployment.
- In the next panel, shown in Figure 14-48, you can choose a configuration file (unattend.txt) with additional settings that will be merged with the host-specific settings.

Profile Wizard	
You can specifiy a custom con settings that you want to Provisioning Manager for OS file with host-specific setting:	nfiguration file (unattend.txt) with advanced o use in your system profile. IBM Tivoli Deployment server automatically merge this s.
□Use a custom setup config File:	uration file. Browse
	< Prev Next > Cancel

Figure 14-48 Windows custom configuration file specification

Enter a meaningful name and description for your unattended image and click **Next**.

8. The profile creation is now complete, as shown in Figure 14-49.



Figure 14-49 Windows profile creation

Optionally, you can customize the profile's properties by selecting **Go To** \rightarrow **Deployment** \rightarrow **OS Management** \rightarrow **Images**, clicking the image, and selecting the **Properties** tab.

Windows Vista/2008

Windows Vista/2008 (32-bit or 64-bit) deployment leverages WinPE2. When you create a Windows Vista/2008 unattended profile, a WINPE software module is automatically created and you can display it by selecting **Go To** \rightarrow **Deployment** \rightarrow **OS Management** \rightarrow **Software Modules**. This software package is automatically bound to the Vista/2008 image deployment.

To create an unattended Vista/2008 image profile:

- 1. Select Go To \rightarrow Deployment \rightarrow OS Management \rightarrow Unattended Setup Image and follow the instructions in the wizard.
- 2. After selecting the machine (running the Web Interface Extension) where the CD/DVD image is available, specify the path containing the install.wim file and click **Next**. All the various configurations available in the CD/DVD will be displayed, as shown in Figure 14-50.

folder you pr profile (each profile).	ovided. Select	t the ones ored as a	that you v different co	vant to indu nfiguration o	ide in you f the sam
Setup	: Windows Vis		SS (en-US)		-
🗆 Setup	: Windows Vis	ta HOMER	ASIC (en-US		
Setup	: Windows Vis	ta HOMEBA	ASICN (en-U	JS)	
🗌 Setup	: Windows Vis	sta HOMEPP	REMIUM (en	-US)	
🗆 Setup	: Windows Vis	sta STARTE	R (en-US)		
🗌 Setup	: Windows Vis	sta ULTIMA	TE (en-US)		
					7

Figure 14-50 Vista configuration selection

- 3. You can choose one or multiple configurations and click Next.
- 4. After specifying the partition sizes (MB or percentage of the total disk), you can choose whether you will use Microsoft BitLocker[™] Drive Encryption, as shown in Figure 14-51. This is a security tool that protects data by encrypting it, rendering the contents of a hard disk unreadable if it is stolen.

Profile Wizard
IBM Tivoli Provisioning Manager for OS Deployment has detected that your system is not compatible with Microsoft BitLocker Drive Encryption, do you want to prepare the disk layout to be compatible with this program or with other encryption programs? Microsoft BitLocker Drive Encryption allows you to encrypt your operating system but needs an extra partition to be usable.
Prepare the disk for Microsoft BitLocker Drive Encryption.
< Prev Next > Cancel

Figure 14-51 Microsoft BitLocker Drive Encryption selection
- 5. To operate, BitLocker requires at least two partitions: a boot partition containing the BitLocker tool, which must have a size of at least 1.5 GB, and an operating system partition that can be encrypted. This option is also available for Vista/2008 clone profiles.
- 6. You will be prompted to enter the product key or to use a volume licensing scheme. You can then specify some fixed properties that will be applied to all machines deployed through the current profile, as shown in Figure 14-52. If left blank, you have to enter them for your machine or they will be requested by the target during the installation.

You may specify you deploy this s be set individuall interactively.	additional fixed properties to use for all machines that ystem profile on. If left blank, these properties have to y for each target or Windows setup might ask for them
Registered owner:	IBM
Organization:	IBM
Admin password	: Confirm:
Time zone:	 (GMT+01:00) Brussels, Madrid, Paris
Language:	✓ Italian (Italy)
Note: You will be editing the Details > C	able to customize additional properties later on by newly created OS configuration (under Profiles > View OS configuration).

Figure 14-52 Windows installation details

7. If you want the Windows Vista/2008 deployment to use a custom configuration file (unattend.xml) with advanced settings, check Use a custom setup configuration file and specify its location, as shown in Figure 14-53. IBM Tivoli Provisioning Manager for OS Deployment server will automatically merge the setting in the unattend.xml file with host-specific settings.

You can specifiy a custom configuration file (unattend.xml) with advanced settings that you want to use in your system profile. IBM Tivoli Provisioning Manager for OS Deployment server automatically merge this file with host-specific settings. Use a custom setup configuration file. File:	Profile Wizard	
Use a custom setup configuration file. File: Browse_	You can specifiy a custom configu advanced settings that you want to us Provisioning Manager for OS Deployme file with host-specific settings.	ration file (unattend.xml) with e in your system profile. IBM Tivoli nt server automatically merge this
	Use a custom setup configuration file File:	Browse

Figure 14-53 Windows custom configuration file selection

- 8. Provide a name and description for the image profile and click **Next** to finish the creation of the profile.
- After the profile has been created, verify that a WINPE software module has been created by selecting Go To → Deployment → OS Management → Software Modules, as shown in Figure 14-54.



Figure 14-54 WinPE2 software module automatically created

10.Also, verify that the WinPE is bound by rule to the unattended Vista/2008 profile that has been created, as shown in Figure 14-55.

	https://tpm.rome.com:9443/maximo/ui/login	M . 🛃 . eee
ost Visited 📋 Customize Links 📋 Free Hotmail	🕒 Windows Marketplace 📄 Windows Media 📄 Windows	
Software Modules 🔶		
Software Modules	C Web Replay 🔮 Builstinis (0) 🔌 Qo To 🗽 Beparits 🖉 Start Cont	er 🌲 Profile 🔭 Sign Out
Software module type: ,	A WinPE2 virtual disk image	
Compatible OS: 1	Windows Vista	
Required OS Build: 6	5.0.6000	
Filename on the OS deployment server:	stowndw2963366 oko	
Destination path on the client:		
Software application order:	Stage 3 (When the OS is installed)	
Options:	none	
Comment:	Version 6.0 build 6000	
	Edit virtual disk image	
	Update drivers	
oftware binding rules		
The following binding rules implicitly t	bind this software module to any deployment object	
matching all criteria of any single rule.		
Rule name + Criteria		
Profile='Set	tup : Windows Vista BUSINESS'	
Now rule Back		

Figure 14-55 WinPE2 binding to the Vista profile

This rule means that the WinPE2 software module will be always deployed with the newly created image profile.

14.5.2 Linux

For an unattended profile creation on Linux, a wizard guides you through the task. All you need is a source image for one of the supported Linux versions:

- 1. Select Go To → Deployment → OS Management → Unattended Setup Image, click Unattended setup (scripted install), and then click A Linux system profile.
- 2. Specify the machine on which the Web Interface Extension is running and where the source CD/DVD images are located, and then specify the installation folder, as shown in Figure 14-56.

Profile Wizard	
Select where your Linux distribution CD-ROM/DVD-ROM file is	located.
Folder: E:\repos\RHEL5i386	▶ Browse.
< Prev Next >	Cancel

Figure 14-56 Linux setup location

3. By default, the Linux partition layout is created with three basic partitions: a swap partition, /boot, and the root partition. You can specify the size of the partitions, as shown in Figure 14-57.

install Linux. the suggeste	If you do not know the answers to these questions, ke ed settings.
How much a	disk space do you want to allocate for paging?
swap	size: 1024 MB
How much a	disk space do you want to allocate for the system?
root si	ize: 100 v percent
⊠Use a sej	parate partition for /boot.
/hoot	size: 256 MB

Figure 14-57 Linux partition layout

Notice that Tivoli Provisioning Server for OS Deployment needs a swap partition with enough size to store the temporary image. We suggest setting the swap size to be twice the unattended image size.

4. You can then choose to include additional Linux software in the image, as shown in Figure 14-58.

You may select additional software grou	ps to install:
 Applications Authoring and Publishing Editors Engineering and Scientific Games and Entertainment Graphical Internet Graphics Graphics Office/Productivity Sound and Video Text-based Internet Base System Deskton Environments 	

Figure 14-58 Linux additional software specification

5. The wizard will prompt you to specify deployment properties (for example, the root password), which you can decide to set now (and will be used for deployment on any target computer) or leave them blank, as shown in Figure 14-59. In the latter case, you can specify those settings individually for each target by selecting Go To → Deployment → Provisioning Computers, selecting the specific computer, and then selecting the Deployment Properties tab.

Profile Wizard
You may specify additional fixed properties applying on all machines that you deploy this system profile on. If left blank, these properties can be set individually for each target. If you do not specify a root password, you might not be able to log on to the deployed target.
Root password: •••••••• Confirm: ••••••••
Time zone: 🛛 🖂 (GMT+01:00) Amsterdam, Berlin, Vienna
Language: 🔽 Italian (Italy)
Note: You will be able to customize additional properties later by editing the newly created OS configuration (under Profiles > View Details > OS configuration).
< Prev Next > Cancel

Figure 14-59 Linux setup details

6. Optionally, you can specify a configuration file with advanced settings that will be merged with the host-specific settings, as shown in Figure 14-60.

Profile Wizard	
You can specifiy a custom co settings that you want to u Provisioning Manager for OS De file with host-specific settings.	onfiguration file (ks.cfg) with advanced ise in your system profile. IBM Tivoli ployment server automatically merge this
Use a custom setup configura	tion file.

Figure 14-60 Linux custom configuration file specification

14.5.3 AIX, Solaris, and Linux on PPC

In this section, we show the main steps to create an unattended profile for AIX, Solaris, and Linux on PPC and the prerequisites to deploy them on target computers.

AIX unattended profile creation

To create an AIX unattended system profile, you must be using a machine that has an AIX operating system that is the same version as the profile you want to create. That machine must have the Web Interface Extension running. The main steps are:

- 1. Copy the content of the AIX installation DVD to disk.
- 2. Export the path of the folder where you copied the installation files by using NFS.

3. Create the OS profile by way of the Tivoli Provisioning Server WEBUI by selecting Go To → Deployment → OS Management → Unattended Setup Image.

After your profile has been created, check that the following prerequisites are satisfied:

- The target computer has firmware that works for a network boot with your BOOTP/DHCP server.
- DHCP option 66 is set to the IP address of the OS deployment server and DHCP option 67 is set to rembo.fcode.
- You have registered manually the target computer in the OS deployment server, indicating at least its IP address and host name
- Start a deployment task on the target. Without a task bound to it, the target cannot boot on the OS deployment server.

After these conditions are satisfied, you can network boot your target machine to start the scheduled deployment task.

Solaris unattended profile creation

Tivoli Provisioning Server for OS Deployment does not require a full Solaris installation environment (with JumpStart[™]) to be able to provision Solaris. The only requirement is to have the corresponding operating system image files available by of an NFS share to create the Solaris unattended setup profile. The Solaris installation server can be configured on any standard Solaris computer using the following steps:

- 1. Set up a Solaris installation server.
- 2. Configure a network share. (If you creating an unattended profile from a Solaris flash archive, the network share need to be for Solaris Flash Archives.)
- 3. Load the installation content of the Solaris operating system into the network share directory.
- 4. Download and start the Web interface extension on the Solaris install server.
- 5. Create the profile through the Tivoli Provisioning Server WEBUI by selecting Go To \rightarrow Deployment \rightarrow OS Management \rightarrow Unattended Setup Image.

After your Solaris unattended profile has been created, you can deploy it on a target computer after verifying that the following prerequisites are met:

► The target system has a sun4u (SUN Ultra[™]) or sun4v (SPARC T1 / T2) architecture.

- DHCP option 66 is set to the IP address of the OS deployment server and DHCP option 67 is set to rembo.fcode.
- To network boot with Tivoli Provisioning Manager for OS Deployment, the SUN SPARC target must support WAN boot. The Open Boot version of the SPARC target must be equal or greater than 4.17.1. A minimum of 1 GB RAM is required (this is a WANBoot requirement).
- You must register your SPARC target on the OS deployment server by indicating at least its IP address and its host name before it can boot on it.
- A network boot (boot net:dhcp or boot net) on the OS deployment server for Solaris is accepted only when a deployment task is scheduled on that target.

After ensuring that you performed all the indicated steps, you can network boot your target so that the scheduled Solaris deployment starts.

Linux on PPC unattended profile

A Linux unattended profile creation for a PPC target is the same as for Intel platforms. You create the profile by simply following the wizard (which you start by selecting **Go To** \rightarrow **Deployment** \rightarrow **OS Management** \rightarrow **Unattended Setup Image**) and providing the installation DVD image (RHEL5 / SLES10).

What is different for Linux on PPC targets is the unattended deployment phase. Before starting the deployment, ensure that the following requirements are satisfied:

- 1. The target system firmware works for network boot with your BOOTP/DHCP server.
- 2. You registered the target computer by IP address and host name. You do not require bare-metal discovery. You have only to network boot the target machine.
- 3. Use the boot parameters and commands that you use for AIX.

14.6 Cloning computers

You can clone computers in two different ways:

- By creating a *golden master image* profile built on a prepared computer by running a specific tool (for example, Sysprep on Windows) or by performing some specific operations (Linux).
- By taking a *point-in-time snapshot image*, which is a Windows snapshot that can be restored on to the same computer from which the snapshot has been taken.

14.6.1 Golden master image

In this section, we show how to create Windows XP and Linux RHEL 5 clone profiles. Notice that the scenarios can be easily applied to other platforms because the procedure that applies to Windows XP also applies to Windows 2000 and 2003 (with only some changes made to the options used when running the Sysprep tool on the reference machine, if you do it manually) and the procedure for the various Linux versions is quite similar. After your golden master image profile has been created, you can deploy it by selecting Go To \rightarrow Deployment \rightarrow OS Management \rightarrow Image Deployment.

Windows XP

In order to clone an already installed Windows XP machine, you need a Sysprep version aligned to the XP Service Pack level. Generally, Sysprep for Windows XP is included on the Windows XP CD-ROM and archived in the \Support\Tools\Deploy.cab file. The Sysprep tool will prepare your system to be cloned.

Note that:

- Sysprep cannot be used on targets that are part of a domain. If you run the tool on a computer that is part of a domain, Sysprep removes it from the domain.
- ► Before running Sysprep, you must configure your target to use DHCP. Select Go To → Deployment → Provisioning Computers, click the specific computer, open the Deployment Properties panel, and check the settings in the "Common networking info" section. If the target uses a static IP address, you have a high risk of IP conflicts when the target boots for the first time and it has not yet applied all the Sysprep settings.
- Log on to the computer as an administrator.

Tivoli Provisioning Server provides two possibilities for cloning on Windows XP:

- Run Sysprep manually on the computer to be cloned.
- ► Let Tivoli Provisioning Server run Sysprep on the computer to be cloned.

Run Sysprep manually

Perform the following steps:

- 1. Copy the Sysprep executable files into a folder named C:\sysprep.
- 2. Close all your applications.

Select Start → Run and run the C:\sysprep\sysprep.exe -mini
 -forceshutdown -reseal command. Alternatively, you can start Sysprep in a
 graphical user interface by double-clicking its icon. Make sure that Mini
 Setup is checked and click Reseal. Your system shuts down automatically
 after a few seconds.

Notice that the Sysprep options to be used depend on the specific operating system to be cloned. For more details, refer to the Tivoli Provisioning Server Information Center at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp

The options that we just reported are specifically for Windows XP/2003. If you planned to run Sysprep manually, uncheck the option **Run Sysprep?** in the image capture panel.

Let Tivoli Provisioning Server run Sysprep

If the Windows operating system type is known to Tivoli Provisioning Server (this can be forced by running a Tivoli Provisioning Manager initial discovery on the computer), you can have the capture image provisioning workflow copy and run the Sysprep files to prepare the computer for cloning. To use this feature for all Windows platforms other than Vista and 2008, you have to make the Sysprep files available in the Tivoli Provisioning Manager repository by performing the following steps:

 Access the Sysprep tool from the CD/DVD for you specific Windows version. Usually, it is packaged as deploy.cab in the Support\Tools folder. Alternatively, you can download it for free from the Microsoft Web site at:

http://www.microsoft.com/downloads/en/default.aspx>

- If available, use the Sysprep tool for the latest Service Pack level of the operating system release you are using. For example, to clone Windows 2003 SP1 and SP2 computers, use Sysprep fro Windows 2003 SP2 if available from Microsoft.
- 3. Unpack the deploy.cab file and copy the extracted **sysprep.exe** and **setupcl.exe** files into the provisioning server directory:

%TIO_HOME%/repository/windows-operating-system/Windows_subdirectory

Where *Windows_subdirectory* can have the following values, depending on the specific operating system:

- win2k/32-bit: Windows 2000 32-bit
- win2k/64-bit: Windows 2000 64-bit
- win2k3/32-bit: Windows 2003 32-bit
- win2k3/64-bit: Windows 2003 64-bit
- winxp/32-bit: Windows XP 32-bit
- winxp/64-bit: Windows XP 64-bit

Make sure that you copy the correct **sysprep.exe** and **setupcl.exe** files under the provisioning server repository for each Windows operating system type because Sysprep will fail during the image capture if the incorrect files are used. If you plan to have Tivoli Provisioning Server run Sysprep on the target computer, check the **Run Sysprep?** check box in the image capture panel.

A golden master image creation can be started either from the Tivoli Provisioning Server WEBUI by selecting **Go To** \rightarrow **Deployment** \rightarrow **OS Management** \rightarrow **Image Capture** or by selecting **Select Action** \rightarrow **Capture Image** after selecting the computer in the Provisioning Computers panel.

In the panel shown in Figure 14-61, specify TPMfOSd as the Boot Server Type, Golden Master as the Image Type, and then click **Submit**, or **Schedule** if you want to run it at a later time.

🚱 🗹 C 🗙 🔞	Mtps://tpm.r	ome.com:9443/naximo/uj/h	ogin		<u>े</u> • 🛃• 🚥	igle 🚽
🙍 Most Visited 🧻 Customize Lin	nks 📄 Free Hotmal 📄 Window	is Marketplace 📋 Window	vs Media 📄 Windows			
Image Capture						
🔣 Image Capture		C wes Repty	Balance (D) Provide To 1	A Beports Off Start Center	A Donie 🗶 Sign Out	'dee IBM.
Task • Inop Source Computer • pc-C Boot Server Type • TRM	ye Capture 1043 105050967a/70 mOSil		Tineout (sec) 21600		
Image Details Image * Golden Master Window	ve XP SP3			Inage T	ype × Golden Master	٩
Scheduling Click Schedule to change options.	Scheduled: Now					Schedule Submit

Figure 14-61 Image capture

If the Windows operating system is not known to Tivoli Provisioning Server (which could be the case if you PXE-booted the machine without discovering it), you must run Sysprep manually before submitting an image capture.

If the Windows operating system type is known to Tivoli Provisioning Server (because you performed an initial discovery of the computer), you also see the Run Sysprep? check box in Figure 14-61. You have to select that option if you already copied the Sysprep files into the provisioning server repository. You have to uncheck it if you executed Sysprep manually on the computer.

Linux

In order to build a Linux golden master image, you have to prepare the source Linux image as follows:

- Check and see if the temporary cache partition has enough space. The sum of the space in the last partition and the unpartitioned space must be large enough to hold all the partition images. Ensure that the swap partition is not at the end of the disk.
- Tivoli Provisioning Manager for OS Deployment supports only Linux Grand Unified Bootloader (GRUB). You can install GRUB on the bootsector of the Linux /boot partition or in the root partition. To start your system correctly with GRUB, ensure that you have a standard MBR on the disk, with the boot partition flagged as bootable.
- The Xen virtualization package part of RHEL5 is not supported and must be removed from the reference computer before the clone operation is started.

Notice that Tivoli Provisioning Server for OS Deployment automatically installs and runs its own system preparation tool named LinPrep.

A golden master image creation can be started either from the Tivoli Provisioning Server WEBUI by selecting **Go To** \rightarrow **Deployment** \rightarrow **OS Management** \rightarrow **Image Capture** or by selecting **Select Action** \rightarrow **Capture Image** after selecting the computer in the Provisioning Computers panel.

14.6.2 Point-in-time snapshot image

The point-in-time snapshot image is supported only for a Windows platform. You are not required to prepare the source machine through the Sysprep tool. Capturing a snapshot should not be used as a backup solution: It is useful to make a quick snapshot of a Windows computer, but it is not reliable if your computer has an extremely large amount of data.

Before starting the image creation, ensure that the following requirements are satisfied for the computer where you are capturing the image:

- If the network interface on the computer is set with a dynamic IP address, ensure that the computer name is in the DNS so that Tivoli Provisioning Manager can detect the machine's IP from by inquiring the DNS server.
- The BIOS startup sequence on the computer must have the network as the first and hard disk.

The point-in-time snapshot can be started in two ways:

 Select Go To → Deployment → OS Management → Image Capture. Complete the Source Computer field, set the Boot Server Type to TPMfOSd, specify a meaningful image name in the Image field, and in the Image Type menu, click Point-in-Time Snapshot[™].

Elle Edit Yew Higtory Bookmarks Iools Help				
🚱 🖂 🕑 🗶 🏠 🗋 romancen https://tom.m	ome.com:9443/maxima/utiliogin		र्द्ध • 🚮 • Google	P
🙍 Most Visited 🗋 Customize Links 🍈 Free Hotmail 👌 Window	is Marketplace 📄 Windows Media 👔	Windows		
👌 Image Capture 🔷 🔶				
[A] Image Capture	C Vielo Replay P Quietno:	(0) 🕈 Qo To 🔤 Beports 🕈 Start (Center #Boule #Silvi Cut 7Heb	IBM
Tisck = Intege Capture 1812 Source Computer = pc-000505641te6 Boot Server Tuese - DistanCol		Tineout (sec) 21600		
Image Details Image * Snapshot for pc-0050559541a6	F		nage Type * Point-In-Time Snapshot	ا
Scheduling Click Schedule to change options. Scheduled: Now				Schedule Submit

Figure 14-62 Point-in-time snapshot from image capture selection

2. Click Submit.

 Select a computer and select Go To → Deployment → Provisioning Computers. The panel shown in Figure 14-63 opens.

🍠 🖸 🕐 🟠 🗋 🛄 🚾	e.com https://tpm.rome.com:9443/maximo/uijh	ngin	公・ 😽 Google	
Most Visited 📄 Customize Links 📄 Free P	Hotmail 📑 Windows Marketplace 📄 Window	vs Media 📄 Windows		
Provisioning Computers				
Provisioning Computers	Contractor Contractor	P(julietins (I) P⊙o To la Megacoriti I I	Start Gerter A Profile K Sign Out ? Help	11
✓ Find:	n 🗸 🗸 Select Action 🛛 🗸 🚯] 🔒 🧶 🍦 🍦		
List Computer Handware	Software Compliance Recomm	endations Credentials Workf	own Variables Deployment Properties	99)
Giobally Unique Identifier Configuration Item]0	
afiguration		Last Known Status		
Management IP Address Operating System Computer Templete Localit	10.1.2.22 Windows Server 2003 En	Operations Framework Agent Agent Status	Deployment engine	
tals Model Type Anchitecture Serial Number Manufacture		Compliance Security Software Patches	Configuration required Configuration required Configuration required	
latic Provisioning Groups 🖓 🖉 Filter 🖓	21441ee		🛈 Seetlas	17
ntic Provisioning Group		Description	Туре	
anamic Group Association		owe to explore	Assign to Static G	iroup

Figure 14-63 Point-in-time snapshot from provisioning computers selection

 Click Select Action → Capture Image. In the next panel, shown in Figure 14-64, set the Boot Server Type to TPMfOSd, specify a meaningful image name in the Image field, and in the Image Type menu, select the value Point-in-Time Snapshot.

🛛 Capture Image				
Task *	Image Capture 1813	 Timen d (ann)	04000	
Boot Server Type *	TPMfOSd	 Timeout (sec)	21600	
Image Details				
Image • Snapshot for ;	c-005056964fa6			Image Type · Point-in-Time Snapshot
Scheduling Click Schedule to chang	e options. Scheduled: Now			Schedule
				suomit

Figure 14-64 Point in time snapshot details

- 5. Click Submit.
- 6. After the Point-in-Time snapshot image has been created, you can view it by selecting Go To → Deployment → OS Management → Images. It can be restored on to the same computer by selecting Go To → Deployment → OS Management → Image Deployment.

15

The IBM Tivoli Monitoring Agent for Tivoli Provisioning Manager

In this chapter we provide an overview of the IBM Tivoli Monitoring Agent for Tivoli Provisioning Manager.

This agent can be installed as part of the core components installation if selected at installation time, or manually after the installation.

The agent must be installed on the same system as the Tivoli Provisioning Manager Version 7.1.1 provisioning server and must be installed as tioadmin user. The scripts used to retrieve the data to fill the workspaces make use of Tivoli Provisioning Manager Version 7.1.1 variables, therefore the tioadmin user must start the agent process.

We cover the following topics:

- "IBM Tivoli monitoring agent software" on page 498
- "Installing support files" on page 502
- "Predefined workspaces" on page 503
- "Sample workspaces data" on page 503

15.1 IBM Tivoli monitoring agent software

The IBM Tivoli Monitoring Agent for Tivoli Provisioning Manager software can identify and notify you of common problems with the Tivoli Provisioning Manager Version 7.1.1.

15.1.1 Features and functions of the monitoring agent

The software includes the following features:

- Monitoring
- Data gathering
- Event management

The IBM Tivoli Monitoring Agent for Tivoli Provisioning Manager provides the following functions:

- Availability Monitoring: Provides Tivoli Provisioning Manager server availability information. Also provides the information about Tivoli Provisioning Manager server dependent components.
- Task Monitoring: Collects information about tasks which were executed in the last few days (number of days is decided by using *Tasks Information Time Range* parameter provided in the agent's configuration as detailed in Example 15-1) and tasks which are scheduled for the current day.

15.1.2 Configuring the agent

The Tivoli Provisioning Manager Version 7.1.1 installer allows you to install the agent, but a separate step is needed to direct the agent to the appropriate monitoring server and configure the options for collecting provisioning server data.

To configure the IBM Tivoli Monitoring Agent for Tivoli Provisioning Manager on a UNIX or Linux computer, follow these steps:

- Make sure that you are logged in as the tioadmin user.
- Run the following command to start the agent configuration:
 \$CANDLEHOME/bin/itmcmd config -A pe

Example 15-1 shows the sample output of the agent configuration command:

Example 15-1 IBM Tivoli Monitoring Agent for Tivoli Provisioning Manager configuration

```
[tioadmin@risc40pa][/opt/IBM/tivoli/ITM/bin]> itmcmd config -A pe
Agent configuration started...
Edit "Monitoring Agent for Tivoli Provisioning Manager" settings? [
1=Yes, 2=No ] (default is: 1): 1
Edit 'Agent Configuration' settings? [ 1=Yes, 2=No ] (default is: 1): 1
WAS Administrator User Name (default is: wasadmin):
WAS Administrator Password (default is: *******):
Type password:
Tasks Information Time Range [ 1=1 Day, 2=2 Days, 3=3 Days ] (default
is: 1):
CPC Port (default is: 2093):
CPC Log Level [ 1=None, 2=Minimum, 3=Maximum ] (default is: 2):
Will this agent connect to a TEMS? [1=YES, 2=N0] (Default is: 1):
TEMS Host Name (Default is: risc550a): vmachine1.rot.it.ibm.com
Network Protocol [ip, sna, ip.pipe or ip.spipe] (Default is: ip.pipe):
     Now choose the next protocol number from one of these:
     - ip
     - sna
     - ip.spipe
     - 0 for none
Network Protocol 2 (Default is: 0): ip
     Now choose the next protocol number from one of these:
     - sna
     - ip.spipe
     - 0 for none
Network Protocol 3 (Default is: 0): ip.spipe
IP Port Number (Default is: 1918):
IP.PIPE Port Number (Default is: 1918):
Enter name of KDC PARTITION (Default is: null):
IP.SPIPE Port Number (Default is: 3660):
Configure connection for a secondary TEMS? [1=YES, 2=N0] (Default is:
2):
Enter Optional Primary Network Name or O for "none" (Default is: 0):
Info - TO update auto restart script, you have to enter root password:
Tried to run authorized
Agent configuration completed...
[root@risc40pa][/opt/IBM/tivoli/ITM/bin]> itmcmd agent stop pe
```

Stopping Monitoring Agent for Provisioning ...
Product Monitoring Agent for Provisioning was stopped gracefully.
Agent stopped...
[tioadmin@risc40pa][/opt/IBM/tivoli/ITM/bin]> itmcmd agent start pe
Starting Monitoring Agent for Provisioning ...
Monitoring Agent for Provisioning started

The Tasks Information Time Range represents the time range in number of days. The agent will send back data for the tasks performed in the last days as specified by this value. For example, if you select 1 day, the agent will send the tasks executed in the last day and the tasks scheduled for today.

The CPC port number is the port number on which the Custom Provider Client and Custom Provider Server will communicate. This information is used internally by the monitoring agent. Make sure that the port number is not already in use.

The CPC Log Level can be configured with one of the following options:

None means that no information will be logged Minimum means that only errors will be logged Maximum means that both information and errors will be logged.

The installation creates a startup file on /etc that is used to automatically restart the agent at system reboot. This file is then executed at reboot time by the /etc/inittab file.

In our environment the startup file is named /etc/rc.itm2 as shown in Example 15-2.

Example 15-2 automatic agent startup

```
Startup agent file created at installation time:
[tioadmin@risc40pa][/etc]> cat rc.itm2
#!/bin/ksh
# (C) COPYRIGHT IBM, Inc. 2007
# Unpublished Work
# All Rights Reserved
# IBM/Tivoli Monitoring Version 6.2.0
# Added by install utility to start instance <#> of the
# IBM/Tivoli Monitoring agents
# start all()
```

The file is then automatically executed at system restart by this line in the /etc/inittab file (added at installation time):

```
[tioadmin@risc40pa][/etc]> grep rc.itm2 inittab
rcitm2:2:once:/etc/rc.itm2 > /dev/console 2>&1
```

Important: If the installation of the agent is performed at the core components installation time, the IBM Tivoli Monitoring Agent for Tivoli Provisioning Manager installation script (install.sh) is invoked by the root user. A group called i tmusers is then created and the tioadmin user added as its member to be granted the required permissions to use the agent files.

During the agent configuration described in Example 15-1 on page 499, a script to update the auto restart script is executed, **UpdateAutoRun.sh**. This script updates the /etc/rc.itmx file created by the installation, therefore it needs root access to perform this operation on the /etc filesystem. The following message is displayed at the end of the configuration command:

Info - TO update auto restart script, you have to enter root
password:
Tried to run authorized
Agent configuration completed...

Make sure the /etc/rc.itmx updated at this stage contains this line to startup the agent:

```
/usr/bin/su - tioadmin -c " /opt/IBM/tivoli/ITM/bin/itmcmd agent
start pe >/dev/null 2>&1"
```

If the **su** command is followed by any other user name, change the name to match tioadmin and restart the agent by running these commands. (They assume the default installation path for the IBM Tivoli Monitoring Agent for Tivoli Provisioning Manager.):

/opt/IBM/tivoli/ITM/bin/itmcmd agent stop pe
/opt/IBM/tivoli/ITM/bin/itmcmd agent start pe

15.2 Installing support files

To be able to use the agent, you have to install the support files on your IBM Tivoli Monitoring infrastructure that includes:

- Tivoli Enterprise Monitoring Server (the value that you specify for the Tivoli Enterprise Monitoring Server Host Name property during the agent configuration).
- Tivoli Enterprise Portal Server
- ► Tivoli Enterprise Portal Server desktop client

These support files can be found in the IBM Tivoli Monitoring Agent for Tivoli Provisioning Manager installation image contained in the core components media.

The monitoring infrastructure used to connect to our provisioning server is based on Windows 32-bit, therefore we used the ITM_Agent_V711_Windows.zip file taken from this core components installation image: TPM_V711_CoreComp_Win32.zip.

For details about the support files installation, refer to the IBM Tivoli Monitoring documentation at:

http://www.ibm.com/developerworks/wikis/display/tivolidoccentral/Tivoli
+Monitoring

15.3 Predefined workspaces

The IBM Tivoli Monitoring Agent for Tivoli Provisioning Manager provides the following predefined workspaces, which are organized by Navigator items.

Agent level Navigator item

Tivoli Provisioning Manager workspace

Availability Navigator item

Availability workspace

Tasks Navigator items

- Tasks workspace
- Task Details workspace

For details about these workspaces, the attributes and the situations reference, refer to *Tivoli Monitoring Agent for Tivoli Provisioning Manager User's Guide*, SC23-9998 at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ibm.t ivoli.tpm.ref.doc/monitoring_agent_user_guide.pdf

15.4 Sample workspaces data

Next we show some typical data collected by the IBM Tivoli Monitoring Agent for Tivoli Provisioning Manager in the environment that we used for this Redbooks publication.

Agent level Navigator item

Figure 15-1 shows a sample view of the Tivoli Provisioning Manager default workspaces.

This workspace contains three views:

► Situation Console:

Represents the classic Situation Event Console filtered for **Tivoli Provisioning Manager**.

Availability:

Displays the Tivoli Provisioning Manager Version 7.1.1 provisioning server and its dependent components availability.

► Performance Object Status:

Displays the information about all component objects of the agent.



Figure 15-1 Tivoli Provisioning Manager workspace

Availability Navigator item

Next we describe a sample view of the Availability Navigator item workspaces.

The workspace shown in Figure 15-2 uses a script called **tioStatusWrapper.sh** that invokes the **tioStatus.sh** command to return the availability information. The **tioStatus.sh** requires the wasadmin user and password to complete; the agent uses the value specified at agent configuration time as detailed in Example 15-1 on page 499.

It contains two views:

Situation Console:

Represents the classic Situation Event Console filtered for Availability.

► Availability:

Displays the Tivoli Provisioning Manager Version 7.1.1 provisioning server and its dependent components' availability.

Availability - WAACHINE 1 - SYSADMIN Jie Edit View Heip Jie Edit View Heip Jie Struation Event Console View Prysica Struation Event Console View Prysica Struation Event Console View Prysica Struation Event Console Struation Name Display Item Source Impact Opened Age Local Timestamp Type Severity Status Owner Situation Name Display Item Source Impact Opened Age Local Timestamp Type Taka: Windows Systems Availability Treestamp Application Component Status Type Functionality Test Status Provisioning server is running. Availability Timestamp Application Component Status Type Functionality Test Status Provisioning server is running. Availability					
File Edit Yew File File File File <tr< th=""><th>Availability - VMACHINE1 - SYSADMIN</th><th></th><th></th><th></th><th></th></tr<>	Availability - VMACHINE1 - SYSADMIN				
Comparison C	File Edit View Help				
Newigator Image: Studion Event Console Vew Physical Enterprice Image: Studion Event Console Image: Studion Event Console <th>🗢 • 🔿 • 🗂 🗔 🛛 🖽 🗞 🚸</th> <th>A 🖸 🔘 🔾 🎘 🚳 🍕</th> <th>🔄 🖉 🛄 🐼</th> <th>😂 🛄 🖪 🗎 📓 🖓 🧕</th> <th>17 🐚 🖸 🔥 🎫</th>	🗢 • 🔿 • 🗂 🗔 🛛 🖽 🗞 🚸	A 🖸 🔘 🔾 🎘 🚳 🍕	🔄 🖉 🛄 🐼	😂 🛄 🖪 🗎 📓 🖓 🧕	17 🐚 🖸 🔥 🎫
View Physical Vi	📲 Navigator 🌲 🗉 🖯	Situation Event Console			
Severity Status Owner Situation Name Display Item Source Impact Opened Age Local Timestamp Type Severity Status Owner Situation Name Display Item Source Impact Opened Age Local Timestamp Type Severity Status Owner Situation Name Display Item Source Impact Opened Age Local Timestamp Type Severity Status Owner Situation Name Display Item Source Impact Opened Age Local Timestamp Type Severity Status Owner Situation Name Display Item Source Impact Opened Age Local Timestamp Type Severity Status Owner Situation Name Display Item Source Impact Opened Age Local Timestamp Type Severity Status Owner Situation Name Display Item Source Impact Opened Age Local Timestamp Type Severity Status Owner Situation Name Display Item Source Impact Opened Age Local Timestamp Type Severity Status Owner Situation Name Display Item Source Impact Opened Age Local Timestamp Type Severity Status Owner Status Owner Situation Name Display Item Source Impact Opened Age Local Timestamp Type Severity Status Owner Status Owner Status Owner Status Opened St	🔘 🍪 View: Physical 📃	😣 🔕 🛕 🛕 💽 🚯	🕐 🏤 🟫 🕅 🕅	🕕 🛈 (Active) 🛛 Total Events: 0	Item Filter: Availability
Availability Availability Availability Availability Availability Availability Availability Availability Availability VMACHINE1 - SYSADMIN	Enterprise E	Severity Status Owmer &	Situation Name Display It	em Source Impact Opened A	ge Local Timestamp Type
Availability - VMACHINE1 - SYSADMIN	Physical				
Immestamp Application Component Status Type Functionality Test Status Functionality Test Message 09/01/09 17:39:15 Status Check PASSED FUNCTIONALITY TEST SUCCESS PROVISIONING SERVER RUNNING: Provisioning server is running. 1					
Infrestanting Replication Component Status PASSED FUNCTIONALITY TEST SUCCESS PROVISIONING SERVER RUNNING: Provisioning server is running Provisioning Server Available Availability - VMACHINE1 - SYSADMIN	Timestern Augustion Component	Ctatua Tuna	Functionality Test Otatus	Functionality	Test Magazara
Hub Time: Tue, 09/01/2009 08:40 AM Server Availability - VMACHINE 1 - SYSADMIN	09/01/09 17:39:15 Status Check	PASSED FUNCTIONALITY TEST	SUCCESS	PROVISIONING SERVER RUNNIT	NG: Provisioning server is running.
La C Hub Time: Tue, 09/01/2009 08:40 AM Server Available Availability - VMACHINE1 - SYSADMIN					
🕒 🕒 Hub Time: Tue, 09/01/2009 08:40 AM 🛛 🔮 Server Available 🔹 Availability - VMACHINE1 - SYSADMIN				10	<u> </u>

Figure 15-2 Availability workspace

Tasks Navigator item

Here we discuss a sample view of the Tasks Navigator item workspaces.

Tasks workspace

The Task workspace shown in Figure 15-3 shows the completed and scheduled tasks within the current day in the Task view. This is because we instructed the IBM Tivoli Monitoring Agent for Tivoli Provisioning Manager to show only 1 day of data for the tasks during its configuration as detailed in Example 15-1 on page 499.

The Situation Console view represents the classic Situation Event Console filtered for **Tasks**.

ile <u>E</u> dit <u>V</u> iew <u>H</u>	ACT - STSADMIN				
	lelp				
5 • 🖦 • 🔭 (. 🚸 🕂 🖂 🖽	81 🗖 🔘 🍙) 22 46 47 🗸 🎟 🚱 🗊 🖂 🐟 🗔 🗟 의 💭 🤅	🌒 :/7 🖻 🧿 🖌	3. 🗐
Ravigator		Situation Even	nt Console		
🎒 🖑 Viev	w: Physical	🛛 🙆 🔼 🛆	, 🔽 🛈 🚸 🐏 🏤 🙀 🖄 🔘 (Active) 🛛 Total Events:	0 Item Filter: Tas	ks
Enterprise		Severity St	tatus Owner Situation Name Display Item Source Impact Opened		tamn Tyne
🗄 🛅 Linux Systems	3		and of owner of one and of the most of order of an part of opened	Trige Ebtar Times	Marrie 1366
🗄 🛅 UNIX System:	s				
😑 🚂 risc40pa					
🖻 😓 Tivoli	i Provisioning Manager				
	Availability				
····· 🕞	asks				
🗄 😤 Windows Sys	tems				
C Physical					
Tasko				1 1	
III Tasks				/ 1	
Tasks				/ 1	
Tasks	Timestamp	TaskiD	TaskName	/ 1	TaskStatus
Tasks	Timestamp 03/01/09 17:41:45	▼ TaskiD 3005	TaskName Run provisioning workflow TCA_PingAgentManager submitted at S	TaskSubmitter MAXADMIN	TaskStatus
Tasks Tosks Node risc40pa:PE risc40pa:PE	Timestamp 09/01/09 17:41:45 09/01/09 17:41:45	▼ TaskID 3005 3003	TaskName Run provisioning workdow TCA_PingAgentManager submitted at S Run provisioning workdow TCA_PingAgentManager submitted at S	TaskSubmitter MAXADMIN MAXADMIN	TaskStatus SCHEDULED SUCCESS
Tasks Tasks Node risc40pa:PE risc40pa:PE risc40pa:PE	Timestamp 09/01/09 17:41:45 09/01/09 17:41:45 09/01/09 17:41:45	▼ TaskID 3005 3003 3002	TaskName Run provisioning workflow TCA_PingAgentManager submitted at 8 Run provisioning workflow TCA_PingAgent Submitted at August 24	TaskSubmitter MAXADMIN MAXADMIN MAXADMIN	TaskStatus SCHEDULED SUCCESS SUCCESS
Tasks Tosks Node risc40pa:PE risc40pa:PE risc40pa:PE risc40pa:PE	Timestamp 09/01/09 17:41:45 09/01/09 17:41:45 09/01/09 17:41:45 09/01/09 17:41:45	▼ TaskID 3005 3003 3002 3001	TaskName Run provisioning workflow TCA, PingAgentManager submitted at 5 Run provisioning workflow TCA, PingAgentManager submitted at August 24 Run provisioning workflow TCA, PingAgent submitted at August 24	TaskSubmitter MAXADMIN MAXADMIN MAXADMIN MAXADMIN	TaskStatus SCHEDULED SUCCESS SUCCESS SUCCESS

Figure 15-3 Tasks workspace

Task Details workspace

The Task Details workspace shown in Figure 15-4 contains a browser view that is used to launch the Tivoli Provisioning Manager Version 7.1.1 Provisioning Tasks Tracking from that workspace.

The Tivoli Provisioning Manager application is launched using a URL that uses 9045 as a default SSL port. If the Tivoli Provisioning Manager application is using a different SSL port number, then you need to modify the URL.

The following steps describe the process for modifying the default Tivoli Provisioning Manager SSL port number:

- 1. Log in to Tivoli Enterprise Portal.
- In the TEP navigation tree, click <*TPM Server*> → Tivoli Provisioning Manager → Task. Then right-click Workspace → Task Details.
- 3. With your Task Details Workspace selected, click Edit \rightarrow Properties.
- 4. In the Task Details Properties window, select the Browser view.
- 5. Select **Use Provided Location** and replace 9045 with the desired port number.

https://\$TPMServer\$.DomainName:9443/maximo/ui/?event=loadapp&value=t
ptask&uniqueid=\$TPMTaskID\$

6. Save the changes.

Task Details - VM	ACHINE1 - SYSADMIN				
⇔ • ⇒ - 🛅 🖟		8 💿 () 🗘 🌮 🕼 🌗 📓 🎟 🗞 🖬 🖉 🖾 🛄 📓	🖓 🧕 🖅 📴 🖸	1 🔥 🗉
🝓 Navigator	* 🗆 🖯	Provisioni	ng Task Tracking	,	* = = = >
🌒 🦑 🛛 View:	Physical 💌	¢ • 0	🈂 👫 📇 🕅 Location: 💽 https://risc40pa.rot.it.ibm.com:9443/maximo/ui	i/?event=loadapp&value=	tptask&uisessionid=125
Enterprise Linux Systems Linux Systems	Provisioning Manager valiability ems	Provisioning Technology Advanced Provisioning Te Provisioning Te Run provision Run provision TCA_Provision TCA_Provision	oning Task Tracking Web Replay Builetins: (0) © 00 Find: East Search Save Query Bookmarks Task D Status Find: Task D Status Status	ûn Reports P Start <u>C</u> er	ter Aprolie A
📢 Physical	1	Done			
III Tasks	1			4	
Node	▲ Timestamp	TaskID	TaskName	TaskSubmitter	TaskStatus
🙁 risc40pa:PE	09/01/09 17:41:45	3000	Run provisioning workflow TCA_PingAgentManager submitted at Se	MAXADMIN	SUCCESS
🙁 risc40pa:PE	09/01/09 17:41:45	3001	Run provisioning workflow TCA_PingAgent submitted at August 24, 2	MAXADMIN	SUCCESS
🙁 risc40pa:PE	09/01/09 17:41:45	3002 Run provisioning workflow TCA_PingAgent submitted at August 24, 2		MAXADMIN	SUCCESS
🙁 risc40pa:PE	09/01/09 17:41:45	3003 Run provisioning workflow TCA_PingAgentManager submitted at Se		MAXADMIN	SUCCESS
🙁 risc40pa:PE	09/01/09 17:41:45	3005	Run provisioning workflow TCA_PingAgentManager submitted at Se	MAXADMIN	SCHEDULED
•				·	
(🕒 Hub Time: Tue, 09/0)1/2009 08:44	AM 🚺 Server Available Task Details - V	MACHINE1 - SYSADN	11N

Figure 15-4 Task Details workspace

508 IBM Tivoli Provisioning Manager V7.1.1: Deployment and IBM Service Management Integration Guide

Part 5

Troubleshooting and migration from Tivoli Provisioning Manager V5.1.2

In this final part of the book, we first cover troubleshooting of Tivoli Provisioning Manager components. We also provide a step by step scenario of what happens "under the hood" when a software distribution is initiated using the scalable distribution, to help you diagnose real life software distribution problems.

With Tivoli Provisioning Manager V7.1.1, a migration path from Tivoli Provisioning Manager V5.1.2 is now available. In the final chapter, we discuss a migration scenario from Tivoli Provisioning Manager V5.1.2 to Tivoli Provisioning Manager V7.1.1.

510 IBM Tivoli Provisioning Manager V7.1.1: Deployment and IBM Service Management Integration Guide

16

Troubleshooting

In this chapter we discuss troubleshooting, best practices, and frequently asked questions for Tivoli Provisioning Manager V7.1.1. We cover the basics of troubleshooting, where to find logs, what the error messages mean, and which solutions exist for some of the most common questions.

Included in the chapter is a step by step scenario of what happens "under the hood" when a software distribution is initiated using the scalable distribution and deployment engine infrastructure. We believe that this information will help you diagnose real life software distribution problems.

We cover the following topics:

- "Troubleshooting basics" on page 513
- "Installation troubleshooting" on page 515
- "Runtime troubleshooting" on page 520
- Collecting logs from Tivoli Provisioning Manager server" on page 523
- "Displaying and exporting provisioning workflow logs" on page 524
- "Verifying if the Tivoli Common Agent is working" on page 526
- "Setting up the Tivoli common agent log levels" on page 527
- "Collecting a log file from the Tivoli common agent" on page 528
- "Verifying if the depot has been successfully installed" on page 529
- "Collecting a log file from the depot server" on page 531
- "Troubleshooting the software distribution" on page 531
- "Troubleshooting operating system provisioning" on page 540

For more information about Tivoli Provisioning Manager V7.1.1 troubleshooting, you can refer to the *Tivoli Provisioning Manager V7.1.1 Problem Determination and Troubleshooting Guide* at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ibm.s
upport.tpm.doc/tpm_pd_guide.pdf

You can also find some troubleshooting tips on the Tivoli Provisioning Manager External Wiki at:

https://www.ibm.com/developerworks/wikis/display/tivoliprovisioningmana
ger/Home

16.1 Troubleshooting basics

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and explain how to resolve the problem. The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM Support person know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, and that is the best way to start down the path of problem resolution.

16.1.1 What are the symptoms of the problem?

When starting to describe a problem, the most obvious question is, What is the problem? This might seem like a straightforward question; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, performance degradation, or incorrect result?
- What is the business impact of the problem?

16.1.2 Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems. The following questions can help you to focus on where the problem occurs to isolate the problem layer:

Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems? Are the current environment and configuration supported?

Remember that even if one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration; many problems can be traced back to incompatible levels of software that are not intended to run together or have not been fully tested together.

16.1.3 When does the problem occur?

Develop a detailed timeline of events leading up to a failure, especially for those cases that are one-time occurrences. You can most easily do this by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward using the available logs and information. Typically, you need to look only as far as the first suspicious event that you find in a diagnostic log; however, this is not always easy to do and takes practice. Knowing when to stop looking is especially difficult when multiple layers of technology are involved, and when each has its own diagnostic information. To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware? Responding to questions like this helps to provide you with a frame of reference in which to investigate the problem.

16.1.4 Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur when the same task is being performed?
- Does a certain sequence of events need to occur for the problem to surface?
- Do any other applications fail at the same time? Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might have occurred around the same time, the problems are not necessarily related.
16.1.5 Can the problem be reproduced?

From a troubleshooting standpoint, the *ideal* problem is one that can be reproduced. Typically, problems that can be reproduced have a larger set of tools or procedures at your disposal to help you investigate. Consequently, problems that you can reproduce are often easier to debug and solve. However, such problems can also have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation. Can the problem be recreated on a test system?

- Are multiple users or applications encountering the same type of problem?
- Can the problem be recreated by running a single command, a set of commands, or a particular application, or a stand-alone application?

16.2 Installation troubleshooting

We start our troubleshooting discussion with installation troubleshooting.

16.2.1 Troubleshooting the provisioning server

Tivoli Provisioning Manager 7.1.1 installation consists of the following steps:

- 1. Install the middleware.
- 2. Run Base Services install (only Web Replay is installed).
- 3. Install the Tivoli Provisioning Manager core components.
- 4. Install Tivoli Provisioning Manager Web components.

In this section we discuss the troubleshooting of these steps.

Middleware installation

Refer to the following link for a list of middleware prerequisite log files:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp?nav=/
0_8_1_2_3_3

Also, the following link lists possible middleware installation problems and how to diagnose and resolve these errors:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp?topic =/com.ibm.support.tpm.doc/limitations/rtrb_mw.html

Base Services install (Web Replay)

Web Replay installation is performed by the Base Services Installer (BSI).

For further details about the installation of BSI, refer to 4.3.2, "Base Services install" on page 70.

When an error occurs, the install error panel will display failure messages from the configuration execution. These messages are generally brief, and help narrow down the problem to a database, WebSphere, or PSI package problem.

The Install trace logs can be searched for the message seen on the panel, and can be useful in getting more diagnostic information about why the error occurred.

Trace logs

If the problem is in a PSI package, then the solution install logs provide in depth information about what exceptions and errors were seen during an install.:

- Deployment Engine Runtime Trace: This log can be found in <Maximo_HOME>\logs\si_inst.logPackage.
- Specific Action log: These files contain the StdOut and StdErr output of external commands launched by the package as it is processed by the deployment engine. These log files are typically vital to the proper debugging of package issues. The logs can be found in <Maximo_HOME>\solutions\logs\<PACKAGE_NAME>\.

For example, if PSI encounters an error in the Web replay, and Tivoli Provisioning Manager is installed to C:\IBM\SMP, then the logs for the Change Package would be found in: C:\ibm\SMP\solutions\logs\Toolbox WebReplay.

- Base Services: Install logs can be found in a temporary location before the install button is selected. This is usually C:\Documents and Settings\Administrator. After selecting the Install button, the logs can be found in <INSTALL_HOME>\logs.
- CTGInstallTrace*.log: These logs have all of the trace statements from the installer and the configuration code, including the embedded calls to PSI. These logs will be appended to when you run PSI, or run the base services installer a second time.
- CTGInstallMessage*.log: These logs have message statements from the installer, configuration code, and PSI.

Refer to the following link for information about how to diagnose and resolve base services installation errors:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp?topic =/com.ibm.support.tpm.doc/limitations/rtrb_base.html

16.2.2 Tivoli Provisioning Manager core components

Tivoli Provisioning Manager core components are installed by using Tivoli Provision Manager Core Components Installer.

For further details about the installation of this component, refer to 4.3.3, "Tivoli Provisioning Manager core components" on page 75.

When an error occurs during the Installation of the Core Component, the logs can be found in the following locations:

- Windows:
 - %TMP%\tclog_wrapper\tcinstall.log
- ► UNIX:
 - tmp/tclog_wrapper/tcinstall.log

Refer to the following link for information about how to diagnose and resolve core components installation errors:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp?topic =/com.ibm.support.tpm.doc/limitations/rtrb_corecomponents.html

16.2.3 Tivoli Provisioning Manager Web components

During this stage of installation, Change PMP, Change PMP fix packs, Base Services and Common PMP fix packs, Ifixes and Hot Fixes, Tivoli Provision Manager PMP, are deployed. For further details, refer to 4.3.4, "Tivoli Provisioning Manager Web components" on page 89.

When an error occurs during the Installation of the Web component, the logs can be found under the following directory:

Windows:

%TMP%\tclog_wrapper\tcinstall.log

► UNIX:

tmp/tclog_wrapper/tcinstall.log

Refer to the following link for information about how to diagnose and resolve Web components installation errors:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp?topic =/com.ibm.support.tpm.doc/limitations/rtrb_webcomponent.html

16.2.4 Tivoli Provisioning Manager installation logs

Next we discuss other useful logs for troubleshooting of Tivoli Provisioning Manager V7.1.1 Installation.

Agent Manager:

- AM_HOME/logs/AMReturnValues.log
- ► AM_HOME/logs/am_upgrade.log

Dynamic Content Delivery:

Tivoli_common_dir/ctgde/logs

Device Manager Federator:

- ► Windows:
 - %TIO_HOME%\DeviceManager\log\DMS_install.log
 - %TIO_HOME%\DeviceManager\dms_config_trace.log
- ► UNIX:
 - \$TIO_HOME/DeviceManager/log/DMS_install.log
 - \$TIO_HOME/DeviceManager/dms_config_trace.log

Tivoli Provisioning Manager for OS Deployment:

- Windows:
 - %TMP%\tclog_wrapper\tpmfosd-installation.log
 - %TMP%\tclog_wrapper\tpmfosd.log
- UNIX:
 - tmp/tclog_wrapper/tpmfosd.log

ITM_Agent:

- ► Windows:
 - %CANDLE_HOME%\InstallITM\IBM Tivoli Monitoring for Provisioning....log
- ► UNIX:
 - \$CANDLE_HOME/InstallITM/IBM Tivoli Monitoring for Provisioning....log

16.2.5 Troubleshooting the infrastructure components installation

After Tivoli Provisioning Manager V.7.1.1 has been installed, in order to run an Inventory scan or deploy software packages to a large number of targets, the scalable distribution infrastructure (SDI) has to be installed.

Refer to 5.2, "Implementing the scalable distribution infrastructure" on page 107" for an overview of this topic.

In this section we discuss troubleshooting techniques for installation of the two SDI components, Tivoli common agent and the depot.

When you install the common agent from the Web interface, a task called *Install common agent* is run. It invokes the workflow *Install_Agent* that will execute the agent installation. So the first check to do is to see if the task status is successful.

If the task should fail, perform the following checks:

- Access the workflow execution log: from Tivoli Provisioning Manager V7.1.1 WEBUI, click Go to → Task Management → Provisioning Task Tracking and search for Install Common Agent task and view the details of the workflow object id. You should see a panel similar to Figure 16-1.
 - a. If the failure is due to a Tivoli Provisioning Manager server problem, continue the troubleshooting and refer to "Runtime troubleshooting" on page 520.
 - b. If the failure is due to a target machine issue, check the following three files in the folder <tca install dir>/runtime/agent/logs/install:
 - i. epInstall.log Contains all the processing during the Agent install.
 - ii. **epInstallStatus.log** Contains the return code for the installation of the common agent.
 - iii. **epPreinstall.log** Contains the pre-check logging prior to the agent install starting.
 - c. On a Windows target computer, you can open the Windows Services control panel and look for a service called IBM Tivoli Common Agent. Make sure that the service is started.
 - d. If these checks do not help, refer to 16.6, "Verifying if the Tivoli Common Agent is working" on page 526.
- 2. When you install the Tivoli common agent with standalone method, you can check the *install.log* in the common agent installation directory for any installer output information and error messages.

00	Provisioning Workflow	/ Status			[™] <u>R</u> eturn <u>T</u> E∏E
	Find:	n 🔁 💎 Selec	t Action 🛛 🖌 🍦 🚯		
List	Execution Logs				
	Workflow Name	Install_Agent	8	Dealeyment Deauest	11 200
	Status	Success	8	Deployment Request	11,250
Para	meters 🛛 💗 Filter > 🕅 🗍 💈	🛭 🛊 🍦 🔶 1 - 2 of 2 🥪			Download
Param	neters		Input Values	Output Values	
Devie			0022		
Softw	vareModuleID		5154		
Execu	ution Logs 🔄 💌 Filter 🖂 🕮	ini 🔶 🌲 🖕 1 - 25 of 681 📣			Developed 1210
Enote	Start Date	Seconds.Milliseconds	Text		Log Level
•	2009-07-21 01:32:56	56.584	Start workflow: 'Install_Agent'		debug
•	2009-07-21 01:32:58	58.646	Start workflow: 'Get_DCM_Property'		debug
•	2009-07-21 01:32:58	58.818	End workflow: 'Get_DCM_Property'	End workflow: 'Get_DCM_Property'	
•	2009-07-21 01:32:59	59.537	Start workflow: 'TCA_Check_Platform_Resources'		debug
2009-07-21 01:33:01 01.209 End workflow: 'TCA_Check_Platform_Resources'				debug	
•	2009-07-21 01:33:01 01.302 Start workflow: 'Set_Server_In_Maintenance'			debug	
•	2009-07-21 01:33:02	02.365	End workflow: 'Set_Server_In_Maintenance'		debug
•	2009-07-21 01:33:04	04.974	Start logical operation: 'SoftwareModule.Install'		debug
•	2009-07-21 01:33:05	05.615	Start workflow: TCA_SoftwareModule_Install		
•	2009-07-21 01:33:05	05.755	Start workflow: 'Get DCM Property'		

Figure 16-1 Workflow execution log of Install_Agent

16.3 Runtime troubleshooting

In this section we discuss how to troubleshoot the Tivoli Provisioning Manager V7.1.1 at runtime. We also cover troubleshooting in the software distribution infrastructure (SDI) and deployment engine (DE) scenarios.

16.3.1 Configuring logging levels

Log data in Tivoli Provisioning Manager is managed by log4j, an open source logging tool. This section details the default log4j settings and how you can modify settings dynamically. For complete log4j documentation, go to:

http://logging.apache.org/log4j/docs/documentation.html

The data from the console.log, msg.log, trace.log, and cbe.log files are recorded based on the default logging levels and configuration parameters set in the *log4j.prop* file or in the *log4j-util.prop* file. Use the log4j-util.prop file to configure

the logging for all scripts located in the %TIO_HOME%\tools directory. Some scripts in automation packages also use the logging settings in log4j-util.prop.

By default, the initial log4j.log level configuration for each log file is set to *info*. As defined in the log4j.prop file, each log file is set to a unique log level for Tivoli Provisioning Manager using the log4j.appender.<filename>.threshold= parameter, where the most common values for <filename> are consolefile, errorfile, and messagefile.

16.3.2 Setting logging levels

Logging levels can be set for each logger within the Web interface or dynamically by editing directly the configuration file. In order to change the logging level of a logger from the Web interface, you can follow these steps:

$\label{eq:Click Go To} \textbf{Click Go To} \rightarrow \textbf{System Configuration} \rightarrow \textbf{Platform Configuration} \rightarrow \textbf{Logging}.$

Logging			Web Replay 👎 <u>B</u> ulletins: (0)	ile × Sign Out	? Неф 🔢 🕅
Select Action					
Root Loggers ⊮ Filter⇒da ≒ + ∳ + 1 - 5 of 18 →					B ¹ Download
Logger	Log Level		Key	Active	
		P		P	
crontaskmgr	ERROR	۹.	log4j.logger.maximo.crontaskmgr	V	Û
crontaskmgr	ERROR	P	log4j.logger.maximo.sql.crontaskmgr	V	Û
exception	ERROR	P	log4j.logger.maximo.exception	V	Û
> security	ERROR	P	log4j.logger.maximo.security	V	Û
) sql	ERROR	P	log4j.logger.maximo.sql	V	Û
					New Row
Loggers 🖌 Filter > 🖧 📜 🛊 🐳 🐟					📴 <u>Coviniasa</u> i ? i 🖻
Logger	Log Level		Key	Active	
		P		P	1
			lo rows to display		
					New Row

The window in Figure 16-2 will be displayed.

Figure 16-2 Configuring logging from Tivoli Provisioning Manager 7.1.1 Start Center

- 3. Within the **Log Level** column, click the **Select Value** button for the logger to be configured. A dialog for selecting the log level is displayed. The example is for the crontaskmgr logger provided by Tivoli process automation engine.
- 4. Within the Select Value dialog, select the logging level to use for the logger.
- 5. Click the **Save Logger** button within the Action Menu bar. This change does not occur immediately and will require a restart of the provisioning server.

If you want to customize the logging level dynamically (without the need to restart the provisioning server), you have change the log4j files manually. You can use the following steps:

- 1. Look on your Tivoli Provisioning Manager server for the log4j files: they are in the following locations by default:
 - Windows %TIO_HOME%\config
 - UNIXLinux \$TIO_HOME/config
- 2. To change the log4j.prop or log4j-util.prop files, open the properties file in a text editor.
- 3. Edit the settings as required. For example, in the lines in Example 16-1, you can change the INFO variable into WARNING, ERROR, or DEBUG, depending on the type of logging information needed.

Example 16-1 config file

```
log4j.category.com.thinkdynamics=INFO, console, file
log4j.category.com.ibm.tivoli=INFO, console, file
log4j.appender.consolefile.threshold=info
```

For example, DEBUG has a higher threshold than INFO.

4. Save the file; the provisioning server automatically reloads the log4j configurations 60 seconds after you save the properties file. You do not need to restart the provisioning server. The updated log4j configuration will implement after 60 seconds.

To enable the automation package manager to append to its log file located in the TIO_LOGS\tcdrivermanager directory, complete these steps:

- 1. Open log4j-util.prop in a text editor.
- Change the default log4j.appender.file.append=false to log4j.appender.file.append=true.
- 3. Save the file.

Note: To understand which log level can be set up, look for the "Logging levels" section in the Tivoli Provisioning Manager 7.1.1. InfoCenter.

16.4 Collecting logs from Tivoli Provisioning Manager server

Tivoli Provisioning Manager records system activity and events in message logs and trace logs. You can use the configuration examiner to view system environment variables, Java properties, product versions, Tivoli Provisioning Manager configuration files, agent manager and device manager service status, runtime logs (Tivoli Provisioning Manager, IBM WebSphere Application Server, dynamic content delivery), and installation logs (Tivoli Provisioning Manager core components, Tivoli Provisioning Manager Web components, middleware installer, and base services installer).

You can also use the configuration examiner to package installation or runtime logs together with system properties and Tivoli Provisioning Manager product information.

For a discussion of the configuration examiner tool, refer to:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp?topic =/com.ibm.support.tpm.doc/logs/rtrb_builtInTroubleshoot.html

Another tool that you can use is the packageLogs tool, a command line utility that packages Tivoli Provisioning Manager logs into a single compressed file that you can send to the IBM Tivoli Software Support team.

You need to launch the packageLogs tool using the following syntax:

Windows

packageLogs.cmd

UNIX

packageLogs.sh

From the following location:

- ► Windows: %TIO_HOME%\tools
- UNIX: \$TIO_HOME/tools

Where TIO_HOME is in the Tivoli Provisioning Manager home directory.

The *packageLogs* tools automatically determines the default location of the logs. The tool produces a compressed file *LogPackagetimestamp.zip*, located in the current directory, where *timestamp* is a time stamp assigned by the system when the packageLogs tool completes the compressed file. See the following link for more information about the packageLogs tool:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp?topic =/com.ibm.support.tpm.doc/general/rtrb_ziptool.html

Tip: To reduce the package size, you can use the two optional date flags:

Syntax:

packageLogs [-start start_date] [-end end_date]

Options:

-start

Excludes log files that were modified before this date. Log entries dated before this date will also be excluded. All configuration files will be included.

Date format is yyyy-MM-dd. For example: 2009-01-01.

-end

Excludes log entries that were dated after this date. All configuration files will be included. Date format is yyyy-MM-dd. For example: 2009-01-30.

For instance, packageLogs.cmd -start 2009-07-30 -end 2009-07-31.

16.5 Displaying and exporting provisioning workflow logs

You can view the history of provisioning workflows recorded in the provisioning workflow logs. You can also export the log files of your provisioning workflow history.

To view provisioning workflow run history:

- 1. Open the provisioning workflow palette if it is not displayed.
- 2. From the Eclipse menu, click **Window** \rightarrow **Show** View \rightarrow Other.
- 3. Expand Automation Package and click Workflow Execution Logs.
- 4. Click OK.
- 5. If you want to clear the logs, right-click in the list and then click **Clear messages**.

To export the logs using the Command Line Interface (CLI), change to the TIO_HOME\tools directory and then run the following command:

Windows

```
workflowLogExport.cmd (-n <workflow_name>* | -r <request_id>) [-f
<export_filename>] [-i <input_filename>]
```

UNIX Linux

```
workflowLogExport.sh (-n <workflow_name>* | -r <request_id>) [-f
<export_filename>] [-i <input_filename>]
```

Where:

[-n <workflow_r< th=""><th> specifies the name of the provisioning workflow whose run history you want to export to a log file. The asterisk (*) indicates that you can include multiple provisioning workflow names in this variable. If you do not specify </th></workflow_r<>	 specifies the name of the provisioning workflow whose run history you want to export to a log file. The asterisk (*) indicates that you can include multiple provisioning workflow names in this variable. If you do not specify
	one or more provisioning workflow names, workflowLogExport will include the provisioning workflow run history for all provisioning workflows.
[-r <request_id></request_id>	Indicates the workflow execution identifier.

- [-f <export_filename>] Specifies the fully qualified path and file name of the provisioning workflow log. By default, the file format for the exported log file is XML, and the default file name is workflowLogExport.xml. If you do not specify a different file format, the log file will be exported by default to XML. Also, if no file location is specified, the log file will be exported by default to the TIO_LOGS directory.
- [-i <input_filename>] Specifies the name of the file that lists the names of all provisioning workflows whose run history you want to export to the same log file.

Note: There is a limit of 4000 characters for workflow output. If this limit is exceeded, the output is truncated.

While if you want to export the workflow log from the Web Interface, run these steps:

- 1. Click Go To \rightarrow Task Management \rightarrow Provisioning Tasks \rightarrow Provisioning Workflow Status.
- 2. To export a provisioning workflow log:
 - a. Search for the workflow execution and select the *workflow name* in the search results.

- b. Click the Execution Logs tab.
- c. Click Select Action \rightarrow Export.
- 3. The Save window for the Web browser is displayed. Specify the location where you want to save the file.

16.6 Verifying if the Tivoli Common Agent is working

After installing the Tivoli common agent, you can verify if this is running properly.

On a Windows computer, you can open the Windows Services control panel and look for a service called *IBM Tivoli common agent*. Make sure that the service is started.

There is also a workflow called *TCA_PingAgent* that can be used to check the Tivoli common agent status. Furthermore there is a tool called **agentcli.cmd** that can be used to verify the agent health. It is located in *\$LWI_DIR/runtime/agent/bin*, where *\$LWI_DIR* is:

► WINDOWS:

C:\Program Files\tivoli\ep\runtime\agent\bin

► UNIX:

/tivoli/ep/runtime/agent/bin

You can use this command in the following way:

agentcli <service_name>, where:

service_name

Is the name of the service you want contact. A complete list of all valid services can be obtained by running: agentcli.cli list.

command

The actual command you want to run against the service specified before. All available commands for a specific service and the usage of it are listed when using: agentcli <service-name> help.

To verify if the agent is running you can use the following command:

agentcli connector alive

If the agent is running, the message, The agent is alive, is displayed. If the agent is not running, the message CLI command failed. A communication error occurred. Verify that the agent is registered and active on port agent_port as indicated.

Another useful option of agentcli is:

```
agentcli deployer list bundles state
```

This will show you all installed bundles for this agent, so you can verify, not only if the agent is running, but also if all necessary bundles are available.

Note: If The Tivoli Common Agent installation fails before it completes, you can review the logs that have been created under the following directory:

- ► For Windows: C:\Program Files\tivoli\ep
- ► For UNIX: /opt/tivoli/ep
- For AIX and Solaris: /usr/tivoli/ep

16.7 Setting up the Tivoli common agent log levels

Follow these instructions to change the log level for Tivoli common agent:

Edit the CA_HOME $\$ for the CA_HOME $\$

com.ibm.tivoli.cas.level=<value>

Where the possible values for <value> are FINE, FINER, and FINEST.

Restart the agent service, or run the following command:

```
CA_HOME/bin/lwilog.sh[bat] -refresh
```

Use the trace command on the managed server. Here is the syntax for this command:

CA_HOME/runtime/agent/bin/agentcli.bat trace <command> <level>

Where <*command*> is either getlevel or setlevel.

The **getlevel** command returns the current trace level. The **setlevel** command changes the current trace level. The available values for level are: off, low, medium, and high.

For example, entering the following line gives information about the trace command:

C:\ep\runtime\agent>agentcli.bat trace help

This line sets the log levels to low:

C:\ep\runtime\agent>agentcli.bat trace setlevel low

16.8 Collecting a log file from the Tivoli common agent

It is possible to collect Tivoli common agent logs using a workflow from Tivoli Provisioning Manager or directly on Tivoli common agent using a local script.

In order to collect the Tivoli common agent's log from Tivoli Provisioning Manager server, you can use the Tivoli common agent log file collector.

This is a workflow that collects logs from the common agents. The device ID of the computer is passed to the workflow. It runs a service command on the target computer and brings the common agent logs back to the folder, %TI0_L0GS%/tivolicommonagent.

The workflow uses the default service access point to run the service command and copy the resulting file back to Tivoli Provisioning Manager.

To use the log file collector, run the workflow, TCA Collect Logs (< DeviceID>).

The logs are returned to the Tivoli Provisioning Manager server.

If you want to collect the Tivoli common agent's log, locally at the Tivoli common agent, you can follow these steps:

- Open a command window.
- Change to the Tivoli common agent install directory.
- Run the script for your operating system:
 - Windows service
 - UNIX Linux service.sh

The script creates an archive file named *CASservice.zip* file in the Install directory.

Note: If you have more than one common agent on a managed system, run the tool in the Install directory of the common agent for which you want to capture diagnostic information.

16.9 Verifying if the depot has been successfully installed

When a distribution fails, the first step consists of verifying if the depot is active and checking its configuration: for example, a good test is to verify if enough space is free in the depot directory for the package.

This can be done by selecting:

Go To \rightarrow Administration \rightarrow Provisioning \rightarrow Dynamic Content Delivery Configuration, as shown in Figure 16-3.

Dynamic Content Delivery Configuration - Microso	It Internet Explorer		
File Edit View Pavorites Tools Help			
🕒 Back + 🐑 - 💌 📓 🏠 🔎 Search	📌 Favorites 😧 🍰 🌺	🗉 - 🔜 🚯 😐	Links 🌒
Address 📳 https://nc117218.romelab.it.iom.com:9443/ine	ximo/ui/login		. 🔁 🔂 👀
Dynamic Content Delivery Configuration	C Web Replay	🖲 Buletina: (0) 🔮 Go To 🔛 Beports 🏛 Start Cent	er *Bolle * Sign Out ? Help IBM.
Select Action 💌 📓 🌞 😓			
List Depots Regions Zones			
Depote S Filter (1, 1, 2, 4, 4, 1, 1 of 1 +	AND DESCRIPTION OF THE OWNER	Tableton, Nation, Veterinteriore	Download 17
Depat	Description	Computer	Status
▶ net17175	depot Rome region	nc117175 romelab.it.ibm.co	m Active 🧃
			New Row

Figure 16-3 Dynamic Content Delivery console

The record of the depot will show either active or inactive. In case it is inactive, make sure that the Tivoli common agent is running on the depot server.

Alternatively, you can try to connect to the depot directly using telnet:

telnet <depot-server-hostname> 2100

Then run command syst, where <depot-server-hostname> is the fully qualified domain name (FQDN) of the computer hosting the depot. and 2100 is the default depot listening port.

A properly working depot will answer as shown in Example 16-2.

Example 16-2 A properly working depot

```
DS: <depot-server-hostname>=2.1.0.1(20090626D)
MC=<depot-server-hostname>=:9046 CONN=0 OS=Windows Server 2003
ARCH=x86_32
```

To verify the depot configuration, you need to select the **Details** button. See Figure 16-4.

Pie Edit Ver Peroriter Total Help Back + Or Resolution Stack + Or Resolution Dynamic Context Delivery Configuration Depois Regions Zones Depois Depois Regions Depois Regions <t< th=""><th>Dynamic Content Delivery Configura</th><th>ation - Micro</th><th>soft Internet Explorer</th><th></th><th></th><th></th><th></th><th>80 S</th><th>فلد</th></t<>	Dynamic Content Delivery Configura	ation - Micro	soft Internet Explorer					80 S	فلد	
	File Edit View Favorites Tools	Help								
doress https://rc11228.com/sb/b.tbm.com/s493/maxima/u/login Image: Content Delivery Configuration Image: Content De	🌀 Back + 🕤 - 💌 😰 🐔	Seard	h 🧙 Favorites 🔗 🔝	· 🕹 🗔 🛄 🚯 (()				Links 😹	
Dynamic Content Delivery Configuration Owe Resist Openantic Content Delivery Configuration Openantic Configuration Delivery Configuration <th>ddress 1 https://nc117218.romelab.it.i</th> <th>bm.com:9443/i</th> <th>maximo/ui/login</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>- 🛃</th>	ddress 1 https://nc117218.romelab.it.i	bm.com:9443/i	maximo/ui/login						- 🛃	
leiect Action leiect Action leiect Action Regions Zones Computer net17175 Computer net17175 Computer net17175 Computer Region Region Regi	Dynamic Content Delivery Conf	iguration	internet and a state 🗈 Web	Replay 👯 Bulieties: (0) 🥖	Go To 🛄 Вер	orta 🕈 Start	i Center 🔮 Brofile	s 🗶 Sign Out 🤉 Help	IR	
Lat Depots Regions Zones Patter Patt	elect Action 🛛 💌 🔒 🗼									
Computer Computer nc117175 dept Rome region Depot Computer Depot Patterss Demain Zone Served Patt Patt 2,100 Nax connections 30 Preferred upbad server? Computer Data Directory Link (HS)* 2,000 Uaid Space (HS) 182 Depot Statistics Mes Date Depot Files Pending Nercereetrander Rate Since Ye	List Depots Regions	Zones								
Description Description Computer nc117175 depot Rome region nc117175 : romelab. I.lom.com Description depot Rome region P Address * 8 106.117.175 Region * Fully qualified host name * nc117175 : romelab. I.lom.com Status Description Description Status Description P Address * 8 106.117.175 Status Region * Fully qualified host name * nc117175 : romelab. I.lom.com Status Demain Zone Served P Bandwidth centrol Demain Zone Served P Status Patierred upload server? Status KB/s Data Directory Link (HB) * 2.000 Used space (HB) 182 Depot Statistics Files On Depot Files Pending Average Transfer Rate Since Yesterday (WB) 64 Inside Zone (WB) 0.0 Last 70 Days (WB) 2002.98 Outside Region (WB) 0.0		1.414								
Inclif7175 Jepot Rome region Depot details Depot	Depots Preser Para (2) (T. V (+ 1)	- 1 01 1 -9	Description		<u> </u>	Cor	outer			
Depot Entropy Entropy <thentropy< th=""> <thentropy< th=""> <thent< td=""><td>- nc117175</td><td></td><td>depat Rome re</td><td>gion</td><td></td><td>not</td><td>17175.romelab.t.lb</td><td>m.com</td><td></td></thent<></thentropy<></thentropy<>	- nc117175		depat Rome re	gion		not	17175.romelab.t.lb	m.com		
Depot				Depot det	als					
Description P Address * 8 166.117.175 Status Active Region * Region 1 P Fully qualified host name * Inc117175 romelab.t.ibm com Distribution Configuration Description Description Distribution Configuration Description Port * 2,100 C Adaptive. High promty Max connections 30 C Static KB/is Preferred upload server? C None C None Data Directory * data Depot Statistics and Files Depot Statistics Files On Depot Piles Pending Since Yeaterday (MB) 640 Inside Zone (MB) 0.0 Last 70 Days (MB) 2002.96 Outside Region (MB) 0.0	Depot • pe117175		Computer *	nc117175.romelab.it.ibm.com	1	1				
Region* Region1 P Fully qualified host name* Incl1717E.romelab.t.Bm.com Distribution Configuration Domain Zone Served P Bandwidth control Port* 2.100 C Adapte: High prority M Max connections 30 C Static 0 KB/a Preferred upload server? C Static 0 KB/a Data Directory & data C None C None Data Directory & data C None C None Data Directory & data C None C None Data Directory Limit (HB) * 2.000 Used space (HB) 182 Depot Statistics and Files Server Traffic Average Transfer Rate Since Yeaterday (HB) 0.0 Last 70 Days (HB) 2002.96 Outside Region (NB) 0.0 Last 70 Days (HB) 2002.96 Outside	Description depot Rome region		P Address *	9.168.117.175		Status	Active			
Distribution Configuration Demain Zone Served Port * 2,100 Port * 2,100 C Adaptive. High priority Max connections 30 Preferred upload server? C Static Data Directory & data C None Data Directory Link (HS) * 2,000 Depot Statistics and Files Depot Statistics Files On Depot Server Traffic Average Transfer Rate Total 2002.98 Since Yestenday (MB) 6.46 Last 70 Days (MB) 2002.98 Outside Region (MB) 0.0	Region * Region1		P Fully qualified host name*	nc117175.romelab.t.ibm.com	•					
Demain Zone Served Bandwidth control Part 2,100 C Adaptive Hgs priority Me Max connections 30 C Static B KB/s Preferred uplad server? Image: Served Image: S				Distribution Con	figuration					
Port* 2,100 C Adaptive. High priority Me Max connections 30 C Static 0 KB/s Preferred upload server? Image: Connections 0 C Static 0 Data Directory. data Image: Connections 0 C Static 0 Data Directory. data Image: Connections 0 C Static 0 Data Directory. data Image: Connections 0 C Static 0 Data Directory. Image: Connections Image: Connections C Static 0 C Static Data Directory. Image: Connections Image: Connections C Static C Static C Static C Static Depot Statistics Files Dr. Depot Pres Prending C Static C Stati	Domain Zone Served		P		Bandwidth centre	01				
Max connections 30 C Static 0 KB/is Preferred upload server? Image: Connections Image: Connections Image: Connections Image: Connections Data Directory (and a Data Directory (and (and a Data Directory (and (and a Data Directory (and Directory (and a Data Director	Port.*	2,100			C Adaptive.	High priority		¥		
Preferred uplaad server? Preferred uplaad server? Data Directory data Directory data Data Directory data Director	Max connections	30			C Static	0 K	08/s			
Data Directory & data Data Directory Link (HB) * 2,000 Used space (HB) * 182 Depoi Statistics and Files Depoi Statistics and Files Cepoi Statistics and Files Depoi Statistics and Files Depoi Statistics and Files Depoi Statistics and Files Depoi Statistics and Files Output Statistics and Files Depoi Statistics and Files <th c<="" td=""><td>Preferred upload server?</td><td>2</td><td></td><td></td><td>None</td><td></td><td></td><td></td><td></td></th>	<td>Preferred upload server?</td> <td>2</td> <td></td> <td></td> <td>None</td> <td></td> <td></td> <td></td> <td></td>	Preferred upload server?	2			None				
Data Directory Linit (HB)* 2.000 Depot Statistics and Files Server Traffic Average Transfer Rate Total 2002.98 Inside Zone (MB) 0.0 Last 7 Days (MB) 2002.96 Outside Region (MB) 0.0	Data Directory*	data								
Used space (HB) 182 Depot Statistics and Files Depot Statistics Files On Depot Files Pending Server Traffic Average Transfer Rate Total 2802.96 Inside Zone (MB) 0.0 Since Yesterday (MB) 6.40 Inside Region (MB) 0.0 Last 70 Days (MB) 2902.96 Outside Region (MB) 0.0	Data Directory Limit (MB)*	2,000								
Depot Statistics and Files Depot Statistics and Files Depot Statistics and Files Depot Statistics and Files Server Traffic Average Transfer Rate Total 2002.98 Inside Zone (MB) 0.0 Since Yestenday (MB) 6.40 Inside Region (MB) 0.0 Last 7 Days (MB) 2002.98 Outside Region (MB) 0.0	Used space (MB)	182								
Depot Statistics Files Dn Depot Files Pending Server Trattic Average Tratsfer Rate Total 2002.98 Inside Zone (MB) 0.0 Since Yesterday (MB) 6.40 Inside Region (MB) 0.0 Last 7 Daya (MB) 2002.98 Outside Region (MB) 0.0				Depot Statistics	and Files					
Server Traffic Average Transfer Rate Total 2002.96 Inside Zone (MB) 0.0 Since Yesterday (MB) 6.40 Inside Region (MB) 0.0 Last 7 Days (MB) 2002.96 Outside Region (MB) 0.0 Last 70 Days (MB) 2002.96 Outside Region (MB) 0.0	Depot Statistics Files On Depot	Piles P	ending					<u>an an an an</u>		
Total 2802.98 Inside Zone (MB) 0.0 Since Yesterday (MB) 6.40 Inside Region (MB) 0.0 Last 7 Days (MB) 2802.98 Outside Region (MB) 0.0		Serv	ver Traffic				Averag	e Transfer Rate		
Since Yesterday (MB) 6.40 Inside Region (MB) 0.0 Last 70 Days (MB) 2002.96 Outside Region (MB) 0.0	Total 200	02.98			Insid	a Zana (UR)	0.0			
Last 70 Days (MB) 2002.96 Outside Region (MB) 0.0	Since Yesterday (MB) 6.4	0	Section and Section		Inside	Region (MR)	0.0			
Last 30 Days (MB) 2002.98	Last 7 Days (MB) 2002.98				Outside	Region (MB)	0.0	tinio inici monocom	-	
	Last 30 Days (MB) 200	02.98			1. 1. 1.					
					Yananaanaa					

Figure 16-4 Depot details

In case the depot is not working correctly, you should make sure that the Tivoli common Agent is running on the target box.

16.10 Collecting a log file from the depot server

Because the Depot is a special Common Agent, you can troubleshoot it in the same way. So if you need to set and collect trace logs, you can refer to the previous sections about debugging of a Tivoli common agent.

For further information about the Dynamic Content Delivery (DCD) logging and tracing, refer to the online InfoCenter.

16.11 Troubleshooting the software distribution

Tivoli Provisioning Manager uses the scalable distribution infrastructure for software and patch distribution and installation, discovery, and compliance management. Unlike the deployment engine infrastructure, which is typically used for automating operations on smaller sets of managed targets, the scalable distribution infrastructure ensures a fast and reliable software distribution to large numbers of target computers (tens of thousands) in a variety of topologies.

For a detailed review of software distribution infrastructure, see 5.2, "Implementing the scalable distribution infrastructure" on page 107"

16.11.1 Debugging the software distribution in a scalable distribution infrastructure (SDI)

In this section we review, step by step, what happens when you distribute a software package in an SDI environment.

A software package distribution is initiated to one or more targets:

- 1. Tivoli Provisioning Manager contacts the dynamic content delivery service Management Center and performs a publish operation.
- 2. From Tivoli Provisioning Manager WEBUI, under Provisioning Task Tracking, the following window is displayed, as shown in Figure 16-5.

Provisioning Task Tracking	⊙ We	eb Replay 👎 <u>B</u> ulletins	: (0) 🎤 <u>G</u> o To 🔟 <u>R</u> eports 🕈	Start <u>C</u> enter ^{&} <u>P</u> rofile	X Sign Out ? <u>H</u> elp III
🔽 Find: 🕅 🕅 💙 S	elect Action 🛛 🖌 🍾	3 1 🗔 🧶 1 💠 🕴			
List Task					
Provisioning Task Install Software 2212			Definit	on Install Software 221	2
Type Software Installation			Start D	ate 2009-08-07 19:07:2	1
Created By MAXADMIN			End U	Eailed	9
Changed By			Base Services Ta	isk	1
Provisioning Workflows > Filter > 🚳 🗊 + 🐳 🔶 1	- 1 of 1 🧇				Download ? =
Provisioning Workflow Status		Start Date	End Date	Concurrency Level	Subtask
SoftwareModule.Install Failed	1	2009-08-07 19:07:	24 2009-08-07 19:12:19	5	Install Software 10647
		Details			
Targets Workflow Parameters					
≽ Filter > ﷺ ∰ ⊕ ⊕ 1 - 1 of 1 ⇒					🖾 <u>Download</u> 🖓 📼
Target	Status Message				Provisioning Workflow Log
 nc117177.romelab.it.ibm.com 	Failed COPINF050E	Failed to install softwar	e product 🚀		1
Download Plans > Filter > A 🗇 + + + 1 - 1 of	l 🦗				Download ? =
Plans	Status Start Time		End T	ime	
1249665011732	1 2009-08-07	19:10:15	2009-	08-07 19:10:16	
Depots ▶ Filter > ₩ 🗊 ♦ 🔶 ⇔ 1 - 1 of 1 ↔					🖾 <u>Download</u> ? 🗖
Depot/Peer	Status	Speed (Kb/s) Sta	rt Time	Duration (seconds)	Is Peer
nc117175.romelab.it.ibm.com	0	67 200	9-08-07 19:10:15	0.017	

Figure 16-5 Provisioning Task Tracking

The Tivoli Provisioning Manager server Console.log reports the information shown in Example 16-3.

Example 16-3 console.log

```
2009-08-07 19:07:39,804 DEBUG [Install Software 10647(10659) from
com.ibm.tivoli.tpm.infrastructure.soa.OSGiSdiTaskDispatcher]
(FileManager.java:294) cds.FileManager: PackageId for new file
published is 1249664853724
2009-08-07 19:07:40,445 DEBUG [Install Software 10647(10659) from
com.ibm.tivoli.tpm.infrastructure.soa.OSGiSdiTaskDispatcher]
(FileManager.java:317) cds.FileManager: Published file C:/Program
Files/IBM/tivoli/tpm/repository/\/test_redbk.1.0.spb with taskId 10659
to CDS depots: nc117175.romelab.it.ibm.com,
```

3. The Management Center validates the request and sends an upload plan to the designated upload depot server specifying what file is to be uploaded (for download plan details, see point 6 below).

 The upload depot server retrieves the file from the file repository and stores it in the depot directory. Example 16-4 shows an extract from the Depot Trace-log.xml file.

Example 16-4 Depot Trace-log.xml

```
<CommonBaseEvent creationTime="2009-08-07T11:07:32.593+02:00"
globalInstanceId="EL09a875af000122eb23dd01000221da"
msg="ENTER^^o^{{1249664853724,1249664853724-1,C:\Program
Files\tivoli\ep\runtime\agent\subagents\cds\depot\data\files\1\12496648
53724-1,test_redbk.1.0.spb,1136,cache_controller_1247769173069,}}"
severity="10" version="1.0.1">
<extendedDataElements name="CommonBaseEventLogRecord:level"
type="noValue">
```

5. At the same time Tivoli Provisioning Manager contacts the Device Management Service and submits an installation job to be sent to the target list. Looking at the Tivoli Provisioning Manager server console log you will see the following lines (Example 16-4).

Example 16-5 Console.log

```
... (JobManagementServiceClient.java:521)
client.JobManagementServiceClient: Submitting JDML job
2009-08-07 19:07:40,976 INF0 [Install Software 10647(10659) from
com.ibm.tivoli.tpm.infrastructure.soa.OSGiSdiTaskDispatcher]
(JobManagementServiceClient.java:523)
client.JobManagementServiceClient: job.requestId =
d0c5c300837411de810c000c2916ae22
2009-08-07 19:07:40,976 INFO [Install Software 10647(10659) from
com.ibm.tivoli.tpm.infrastructure.soa.OSGiSdiTaskDispatcher]
(JobManagementServiceClient.java:524)
client.JobManagementServiceClient: job.applicationData =
SoftwareModule.Install
2009-08-07 19:07:41,445 INF0 [Install Software 10647(10659) from
com.ibm.tivoli.tpm.infrastructure.soa.OSGiSdiTaskDispatcher]
(JobManagementServiceClient.java:542)
client.JobManagementServiceClient: Submitted job to the job management
server. Job id is: [124966486117979313]
```

 Target computers continually poll the device manager service server to see if there are any jobs for them to run (polling interval is set in jes.properties file). Device manager passes all pending jobs to the Tivoli common agent. See Example 16-6.

Example 16-6 Agent Trace-log.xml

- 7. The Device Manager client subagent passes the download instruction to the content delivery system subagent.
- 8. The Content Delivery System subagent contacts the management center distribution agent and requests a download plan. Example 16-7 shows the Agent Trace-log.xml.

Example 16-7 Agent Trace-log.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<OptimizedPlan AllPrivileges="false"</pre>
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="OptimizedPlan.xsd">
  <PlanID>1249665011732</PlanID>
  <FileID>1249664853724-1</FileID>
  <PackageID>1249664853724</PackageID>
  <FileName>test redbk.1.0.spb</FileName>
  <FingerPrint>19869CECA54E95DAF1C112B464E5E471</FingerPrint>
  <FileSize>1136</FileSize>
  <DepotServerList DepotServerNumber="1">
    <DepotServer>
      <ServerName>nc117175.romelab.it.ibm.com</ServerName>
      <ServerIP>9.168.117.175</ServerIP>
      <Region>Region1</Region>
      <ServerPort>2100</ServerPort>
      <MaxDownloadRate>0</MaxDownloadRate>
      <DownloadRateHasConstraint>false</DownloadRateHasConstraint>
      <NumberOfRetries>3</NumberOfRetries>
      <RequestDelayMs>0</RequestDelayMs>
      <FileStatus>1</FileStatus>
    </DepotServer>
  </DepotServerList>
  <PeerServerList PeerServerNumber="0"></PeerServerList>
  <EncryptKey>U9sKmCu4KAIYZj0TR8gGJcPwYMn94nHHymDp6Rc/qwM=</EncryptKey>
  <EncryptMode>0</EncryptMode>
  <MIN TOTAL PEER SPEED KBPS>600</MIN TOTAL PEER SPEED KBPS>
  <MIN_PEER_SPEED_KBPS>30</MIN_PEER_SPEED_KBPS>
```

```
<LIMIT_SERVER_SPEED>false</LIMIT_SERVER_SPEED>
<CONN_WAIT_TIME_SEC>5</CONN_WAIT_TIME_SEC>
<MIN_CHUNK_SIZE_MB>1</MIN_CHUNK_SIZE_MB>
<MAX_CHUNK_SIZE_MB>200</MAX_CHUNK_SIZE_MB>
<INITIAL_NUM_OF_CONNS>3</INITIAL_NUM_OF_CONNS>
<CONN_INCREASE_PCNT>75</CONN_INCREASE_PCNT>
<LOOP_SLEEP_TIME_MS>150</LOOP_SLEEP_TIME_MS>
<TRANSFER RATE HISTORY_SEC>2</TRANSFER RATE HISTORY_SEC>
```

<servers_speed_update_interval_sec>3</servers_speed_update_interval_sec</pre>

>

```
<HANDSHAKE_TIMEOUT_SEC>30</HANDSHAKE_TIMEOUT_SEC>
<MAX_HANG_TIME_SEC>30</MAX_HANG_TIME_SEC>
<wireEncryptMode>0</wireEncryptMode>
<GlobalNumberOfRetries>0</GlobalNumberOfRetries>
<DownloadType>0</DownloadType>
<MAX_DEPOT_CONNS>1</MAX_DEPOT_CONNS>
<MAX_CONNS>0</MAX_CONNS>
<ProxyUsage>0</ProxyUsage>
```

```
</OptimizedPlan>
```

The download plan returned to the agent includes a list of depots or peers from which to download the file.

9. When all parts of the file have been downloaded from the various depots and peers, the subagent re-assembles the file and notifies the Management Center that the download is complete.

If peering is enabled, the file is copied into the Tivoli common agent's cache directory. This system can now act as a peer download server for other local agents.

10.DMS updates results into Tivoli Provisioning Manager. The device manager client subagent starts the appropriate subagent to start the unpacking and installation of the file, this instruction is actually passed by the JES subagent. See Example 16-8.

Note: For software package block software packages, the SPBHandler subagent is used.

```
</extendedDataElements>
<extendedDataElements
name="CommonBaseEventLogRecord:sourceClassName" type="string">
<values>com.ibm.tivoli.orchestrator.endpoint.tca.handlers.spb.impl.SPBH
andler</values>
</extendedDataElements>
<extendedDataElements
name="CommonBaseEventLogRecord:sourceMethodName" type="string">
<values>installPackage</values>
</extendedDataElements>
```

Return results

The following results are returned:

- 1. Results of the distribution (success or failure) are passed from the SPB Handler to the DMS sub agent.
- 2. The DDMS sub agent passes results back to the remote federating agent.
- 3. Remote federating agent periodically sends back all results to the device management server.
- 4. The results finally get passed back to Tivoli Provisioning Manager.
- 5. In our case, the result is a failure because we have installed the package twice on the same target machine without setting the *FORCE* option. In the Agent Trace-log.xml you can see the following error:

DSM0003E Error while attempting to install package [9]: rc test_redbk,

Tivoli Provisioning Manager WEBUI shows the same error (Figure 16-6).



Figure 16-6 Error message pop-up

16.11.2 Debugging the software distribution in a deployment engine infrastructure

In this case, only a deployment engine is involved.

Here are the main steps:

1. The logical operation *SoftwareModule.Install* is started. The workflow execution export log will report the lines shown in Example 16-9.

Example 16-9 Workflow log extract

The corresponding Tivoli Provisioning Manager server console.log is shown in Example 16-10.

Example 16-10 Workflow name and ID

```
2009-08-07 22:39:47,976 INFO [Deployment Request 11610]
(DeploymentWorker.java:257) engine.DeploymentWorker: Executing
workflow: Name='SoftwareModule.Install', id=1025
```

2. The workflow SPB_TCA_Install is executed, as shown in Example 16-11.

Example 16-11 Workflow execution log

3. The logical operation *FileRepository.GetFile* is started to copy the software package from file repository to the target machine (by using RXA protocol). Example 16-12 shows the workflow execution log.

Example 16-12 Workflow execution log extract

```
<execution-log workflow-name="FileRepository.GetFile" id="10920"</pre>
date="Aug 7, 2009 10:39:59 PM" position="320" call-stack-level="4"
log-text="Start logical operation:
'FileRepository.GetFile'">
      <log-details position="0"
name="FileRepositoryID">1450</log-details>
      <log-details position="1" name="SourcePath">\</log-details>
      <log-details position="2"
name="SourceFileName">test redbk.1.0.spb</log-details>
      <log-details position="3" name="DestinationId">8857</log-details>
      <log-details position="4"
name="DestinationPath">C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp</log-details>
      <log-details position="5"
name="DestinationFileName">test redbk.1.0.spb</log-details>
      <log-details position="6"
name="TimeoutInSeconds">600</log-details>
    </execution-log>
```

Example 16-13 shows the Tivoli Provisioning Manager server console.log.

Example 16-13 Tivoli Provisioning Manager server console.log

2009-08-07 22:40:01,632 DEBUG [Deployment Request 11610] (TCACopyFile.java:85) javaplugin.TCACopyFile: source path after normalizing: C:/Program Files/IBM/tivoli/tpm/repository\ 2009-08-07 22:40:01,632 DEBUG [Deployment Request 11610] (TCACopyFile.java:89) javaplugin.TCACopyFile: dest path before normalizing: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp 2009-08-07 22:40:01,632 DEBUG [Deployment Request 11610] (TCACopyFile.java:92) javaplugin.TCACopyFile: dest path after normalizing: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp 2009-08-07 22:40:01,632 DEBUG [Deployment Request 11610] (TCACopyFile.java:106) javaplugin.TCACopyFile: copyHostSapId=9067 2009-08-07 22:40:01,632 DEBUG [Deployment Request 11610] (TCACopyFile.java:107) javaplugin.TCACopyFile: copyHostDeviceId=8857 2009-08-07 22:40:01,632 DEBUG [Deployment Request 11610] (TCACopyFile.java:108) javaplugin.TCACopyFile: hostIPAddress=9.168.117.177 2009-08-07 22:40:01,632 DEBUG [Deployment Request 11610] (TCACopyFile.java:109) javaplugin.TCACopyFile: sourceFilePath=C:/Program Files/IBM/tivoli/tpm/repository/test redbk.1.0.spb 2009-08-07 22:40:01,632 DEBUG [Deployment Request 11610] (TCACopyFile.java:110) javaplugin.TCACopyFile:

4. The workflow *SPB_Synch_Install* is executed to run the TASK (Install Software 10647) that performs the SPB installation. See Example 16-14.

Note: An activity plan is run to accomplish the task.

Example 16-14 Workflow execution log

```
<execution-log workflow-name="SPB Synch Install" id="10939" date="Aug</pre>
7, 2009 10:40:06 PM" position="339" call-stack-level="4"
log-text="Start workflow: 'SPB Synch Install'">
      <log-details position="0" name="DeviceID">8857</log-details>
      <log-details position="1"
name="OperationalParameters">-spbclean</log-details>
      <log-details position="2"
name="OperationalParameters">-n</log-details>
      <log-details position="3"
name="OperationalParameters">"test redbk".1.0</log-de</pre>
tails>
      <log-details position="4"
name="OperationalParameters">C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\test re
dbk.1.0.spb</log-details>
      <log-details position="5" name="keys" />
      <log-details position="6" name="values">*******</log-details>
    </execution-log>
```

The console.log, shown in Example 16-15 reports the following information.

Example 16-15 Console.log

2009-08-07 22:40:06,913 DEBUG [Status Updater]
(StatusUpdateProcessor.java:78) manager.StatusUpdateProcessor: Start
processing for task instance id=10674, name=Install Software 10647
2009-08-07 22:40:06,913 DEBUG [Status Updater]
(StatusUpdateProcessor.java:83) manager.StatusUpdateProcessor: Trying
to lock task instance id=10674, name=Install Software 10647
2009-08-07 22:40:06,929 DEBUG [Status Updater]
(StatusUpdateProcessor.java:85) manager.StatusUpdateProcessor: Locked
task instance id=10674, name=Install Software 10647
2009-08-07 22:40:06,929 DEBUG [Status Updater]
(StatusUpdateProcessor.java:99) manager.StatusUpdateProcessor: Task
instance status is PROGRESS
current status for plan: Install Software 2219(2219) is IN_PROGRESS

Return results

In our case the result is a failure because we have installed the package twice on the same target machine without flagging the FORCE option:

```
(Current software package status is 'IC---).
```

The console.log, seen in Example 16-16 will report this kind of failure:

Example 16-16 Console.log

16.12 Troubleshooting operating system provisioning

You can also collect the Tivoli Provisioning Manager for OS Deployment logs from the Tivoli Provisioning Manager user interface. Follow these steps:

- 1. In Tivoli Provisioning Manager user interface, go to the computer that the activity was run against. (For example, click **Provisioning computers** on the Start Center main page, then find the target computer in question.
- 2. Click the **Deployment Properties** tab for the computer. This will launch a view that shows you properties on the Tivoli Provisioning Manager for OS Deployment server for that target computer.
- 3. On that page, click the tab Task History.
- 4. There will be a list of tpmfosd tasks for that target computer. You can right-click the task and select **Export debug data**. This will start a wizard to save a .cab file that has the logs.

17

Migrating from Tivoli Provisioning Manager Version 5.1.1.2 to Tivoli Provisioning Manager Version 7.1.1

In this chapter, we provide the necessary steps for a successful migration of a Tivoli Provisioning Manager Version 5.1.1.2 data and artifacts to a Tivoli Provisioning Manager Version 7.1.1 environment.

A migration allows you to maintain the investment made in Tivoli Provisioning Manager Version 5.1.1.2 and leverage the new functionalities introduced by Tivoli Provisioning Manager Version 7.1.1.

Here, we only describe the migration from Tivoli Provisioning Manager Version 5.1.1.2. The Tivoli Intelligent Orchestrator and Tivoli Provisioning Manager for Software can also be migrated to Tivoli Provisioning Manager Version 7.1.1. Refer to Table 17-3 on page 551 for the upgrade path.

We cover the following topics:

- "Migration objectives" on page 543
- ► "Environment used for the migration" on page 545
- "Migration overview" on page 548
- "Tivoli Provisioning Manager Version 5.1.1.2 pre-migration tasks" on page 550
- "Tivoli Provisioning Manager Version 7.1.1 pre-installation tasks" on page 558
- "Tivoli Provisioning Manager Version 7.1.1 installation" on page 559
- "Completing the property file" on page 577
- "Migrating Tivoli Provisioning Manager" on page 591
- "Post-migration tasks" on page 655

17.1 Migration objectives

By *migration*, we mean the process of migrating your existing 5.1.1.2 provisioning environment to a newly created Tivoli Provisioning Manager Version 7.1.1 provisioning environment.

By *upgrade*, we mean the process of upgrading your existing Tivoli Provisioning Manager Version 7.1 provisioning environment to Tivoli Provisioning Manager Version 7.1.1.

For the scope of this chapter, we detail all the steps required for a successful migration.

The migration uses a gradual and phased migration for agents and depots and respects the N-1 principle of backward version compatibility (operational support of older agents down to version 5.1.0.2).

The switch to version 7.1.1 provisioning server is a one-step operation and the existing agent certificates works with the new Agent Manager.

17.1.1 Gradual phased migration process approach

You can use a phased migration process approach that leverages the existing infrastructure, minimizes disruption, and accommodates failures. Here we list an outline of the phases:

1. Preparing for migration on the current 5.1.1.2 provisioning server:

Refer to section "Tivoli Provisioning Manager Version 5.1.1.2 pre-migration tasks" on page 550.

2. Preparing a 7.1.1 server in parallel:

Refer to sections "Tivoli Provisioning Manager Version 7.1.1 pre-installation tasks" on page 558 and "Tivoli Provisioning Manager Version 7.1.1 installation" on page 559.

3. Big switch to 7.1.1 provisioning server in a maintenance window:

Refer to "Migrating Tivoli Provisioning Manager" on page 591 and "Post-migration tasks" on page 655.

At the completion of this phase, the 7.1.1 provisioning server is operational and you can continue the migration process with the phases listed next:

- 4. Migrate depots and federate DMS.
- 5. Upgrade agents to 7.1.1 level.

17.1.2 Artifacts migration

Most artifacts are automatically migrated during the migration scripts execution. The rest require some manual steps to be performed.

Table 17-1 details the artifacts migrated during the migration scripts execution.

7.1.1 provisioning server 5.1.1.2 provisioning server **Tivoli Provisioning Manager Workflows** Preserved in Tivoli Provisioning Manager 7.1.1 Activity Plans Preserved in Tivoli Provisioning Manager 7.1.1 SPB Definitions Preserved in Tivoli Provisioning Manager 7.1.1 Users, Roles, user/resource groups and Part of them migrated by the migration Security Policies toolkit; some manual mapping to new roles and permissions **Tivoli Provisioning Manager Compliance** Preserved in Tivoli Provisioning Manager Checks 7.1.1 Static Resource Groups Covered by schema and data migration DCM contents and Customer extensions Schema migration and database data migration in 7.1.1 Default file repositories (for example SPB Migrated with database in 7.1.1. storage) Note that the file repository contents, (i.e. actual SPBs files) need to be manually copied over from the 5.1.1.2 LocalFileRepository to the 7.1.1 LocalFileRepository. Discovery/Inventory scan schedules Migrated with database in 7.1.1 (Tivoli Provisioning Manager)

Table 17-1 Artifacts migrated during the migration scripts execution

As shown in this table, most of the tools already in use at version 5.1.1.2 have been preserved in version 7.1.1 (for example, SPE and APDE). Preserving the tools preserves skill investment made on version 5.1.1.2 that can be reused.

Table 17-2 details the artifacts that need manual effort to be migrated.

5.1.1.2 provisioning server	7.1.1 provisioning server		
Out of the box Reports and Customer Reports	Manual rebuild using BIRT (you can start with current SQL queries)		
Customer code leveraging Tivoli Provisioning Manager Web service interface	Minor changes needed		
Dynamic Group Definitions in Tivoli Provisioning Manager 5.1.1.2	Manually create the queries in 7.1.1 (you can start with current SQL queries). Refer to "Migrating dynamic groups" on page 652		
Web Replay Scenarios from Tivoli Provisioning Manager 5.1.1.2	Manually recreated in 7.1.1		
Tivoli Provisioning Manager for OS Deployment Embedded Edition images from Tivoli Provisioning Manager 5.1.1.2	Need to deploy and recapture the images in 7.1.1		
Favorite Tasks in Tivoli Provisioning Manager 5.1.1.2	Migrated automatically during the migration process. Tasks will be displayed under Provisioning Task Definitions when logged in as the user who saved the task in 5.1.1.2		

 Table 17-2
 Artifacts that required manual intervention for their migration

17.2 Environment used for the migration

This section describes the environment used for this chapter.

We used just one of the possible topology configuration, single computer deployment configuration for both the 5.1.1.2 and 7.1.1 provisioning servers.

For details about the supported topologies, refer to *Tivoli Provisioning Manager Version 7.1.1 Migration Guide* at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ibm.t ivoli.tpm.ins.doc/tpm_migrate_guide.pdf **Important:** It is mandatory to have the 5.1.1.2 provisioning server and the Tivoli Provisioning Manager version 7.1.1 systems belonging to the same VLAN because during the migration process, it is required to configure the 5.1.1.2 provisioning server IP address and hostname on the Tivoli Provisioning Manager version 7.1.1 system.

Moreover, the two systems must be of the same platform type; you cannot mix Windows and UNIX systems.

17.2.1 Tivoli Provisioning Manager Version 5.1.1.2 system

The system used for the Tivoli Provisioning Manager Version 5.1.1.2 installation consists of an AIX 5.3 64-bit processor, with the characteristics described in Example 17-1.

Example 17-1 AIX 5.3 system characteristics

System Model: IBM,9115-505 Machine Serial Number: 65084AA Processor Type: PowerPC POWER5 Processor Implementation Mode: POWER 5 Processor Version: PV 5 Number Of Processors: 2 Processor Clock Speed: 1650 MHz CPU Type: 64-bit Kernel Type: 64-bit LPAR Info: 1 65-084AA Memory Size: 3936 MB Good Memory Size: 3936 MB Platform Firmware level: SF235 180 Firmware Version: IBM, SF235 180 Console Login: enable Auto Restart: true Full Core: false Network Information Host Name: risc40pa IP Address: 9.168.47.12 Sub Netmask: 255.255.255.128 Gateway: 9.168.47.1 Name Server: 9.64.162.21 Domain Name: rot.it.ibm.com

Paging Space Information

Both the IBM Tivoli Directory Server and the IBM DB2 Universal Database are installed on the local system.

17.2.2 Tivoli Provisioning Manager Version 7.1.1 system

The system used for the Tivoli Provisioning Manager Version 7.1.1 installation consists of an AIX 6.1 64-bit processor, with the characteristics described in Example 17-2.

Example 17-2 AIX 6.1 system characteristics

System Model: IBM,9111-520 Machine Serial Number: 6556F5D Processor Type: PowerPC POWER5 Processor Implementation Mode: POWER 5 Processor Version: PV 5 Number Of Processors: 2 Processor Clock Speed: 1500 MHz CPU Type: 64-bit Kernel Type: 64-bit LPAR Info: 1 65-56F5D Memory Size: 7808 MB Good Memory Size: Not Available Platform Firmware level: SF225 096 Firmware Version: IBM, SF225 096 Console Login: enable Auto Restart: true Full Core: false Network Information Host Name: risc550a IP Address: 9.168.47.14 Sub Netmask: 255.255.255.128 Gateway: 9.168.47.1 Name Server: 9.64.162.21 Domain Name: rot.it.ibm.com Paging Space Information Total Paging Space: 8192MB Percent Used: 1%

Both the IBM Tivoli Directory Server and the IBM DB2 Universal Database are installed on the local system.

17.3 Migration overview

The migration is composed of several steps that must be performed in the following order:

1. Upgrade the provisioning server to version 5.1.1.2.

The supported migration path to version 7.1.1 is from a 5.1.1.2 provisioning server. The Tivoli Intelligent Orchestrator and Tivoli Provisioning Manager for Software products must also be upgraded to the 5.1.1.2 version. The migration can be completed from any level of interim fix on 5.1.1.2, for example 5.1.1.2 with interim fix 3, but there is no requirement to install any interim fixes before you migrate.

2. Upgrade the common agents.

The Tivoli Common Agent should be upgraded to the 5.1.1.2 level; version 1.3.2.29, or version 1.3.2.30 if you have installed 5.1.1.2 interim fixes. The upgrade must be done on both the depot servers and the endpoints that are participating in the software distribution process.

3. Install Tivoli Provisioning Manager version 7.1.1.

On a new computer, install version 7.1.1.

Important: The installation steps for the migration are different from the typical installation, so follow the documentation in the migration guide.

For example, when you install the core components, you will not install the following components:

- Agent Manager
- Tivoli Provisioning Manager for Dynamic Content Delivery
- Tivoli Provisioning Manager Job Management Service

These components skipped during core components installation will be installed during the migration step. There are also migration steps to perform before installing the base services and Web components. 4. Complete the property file.

The migration involves a series of scripts that automate the process. One property file is provided so that you can enter all of the required information at the beginning of the migration. During the migration, the scripts will retrieve the values from the property file. It is very important that the correct values are added to the property file.

Incorrect values will cause errors and delays in the migration process.

Tip: Some of the information that you enter during the installation is required for configuring the property file, the next step in the migration.

Have the property file open so that you can complete the two tasks concurrently.

Before you restore the 5.1.1.2 data, you need to edit the property file again to ensure that the values are still correct for your 7.1.1 provisioning environment.

5. Back up the 5.1.1.2 data.

There are two backup tasks to run to retrieve the information that you will migrate to version 7.1.1.

- Configuration backup of the 5.1.1.2 provisioning server
- Provisioning database backup

Depending on your environment, these backups will be done in either one or two steps. If you use a local database server for 5.1.1.2, it will be a one-step backup; the configuration and the local database backup is completed at the same time. If you have a remote database server for 5.1.1.2, two steps will be done; you will back up the remote database server and then you will back up the 5.1.1.2 configuration on the provisioning server.

6. Restore and migrate the 5.1.1.2 data.

Restore the 5.1.1.2 backup data to the 7.1.1 provisioning server and the database server. If you have a remote database server, you will restore the database information to the remote database and then restore the provisioning server configuration information on the 7.1.1 provisioning server. If you have a local database for 7.1.1, the restore is completed in one step. The data migration also installs the components that were skipped during the 7.1.1 installation:

- Common Agent Services
- Tivoli Provisioning Manager for Dynamic Content Delivery
- Tivoli Provisioning Manager Job Management Service

7. Complete the 7.1.1 installation.

Install the base services and Tivoli Provisioning Manager Web components.

8. Assigning the 5.1.1.2 server host name to the 7.1.1 server.

Your 7.1.1 provisioning server will take the host name and IP address of your 5.1.1.2 provisioning server. You will also update the host names for the directory server, WebSphere Application Server, software distribution infrastructure, and Tivoli Provisioning Manager for OS Deployment.

9. Start the 7.1.1 provisioning server.

Start the provisioning server for the first time since the data migration. At startup, the automation package migration begins.

Attention: It can take some time for the provisioning server to fully start this first time. Before you begin any tasks, or shut down the provisioning server, ensure that it has fully started.

10. Restore the LDAP.

All of the 5.1.1.2 users and roles were migrated and need to be restored to the 7.1.1 LDAP server. During the 5.1.1.2 backup, an LDIF file was created to store all of the information, and to map the 5.1.1.2 roles to the 7.1.1 roles so that they will work in your new provisioning environment. Restore this LDIF file to the 7.1.1 LDAP server. After the LDAP is restored, you can also migrate the access groups that you used in version 5.1.1.2.

11. Recreate and upgrade additional 5.1.1.2 data objects.

After the migration, additional tasks can be completed outside of the migration maintenance window. Tasks like recreating images for Tivoli Provisioning Manager for OS Deployment, recreating custom automation packages and reports, and migrating the TADDM GUID. If your 5.1.1.2 provisioning operations used these data objects, you can add them to your 7.1.1 provisioning environment.

17.4 Tivoli Provisioning Manager Version 5.1.1.2 pre-migration tasks

In this section we describe the pre-migration tasks and checks to be performed on the Tivoli Provisioning Manager Version 5.1.1.2 system to prepare it for the migration.
For the scope of this chapter, we installed a fresh 5.1.1 provisioning server, then installed the fix packs to raise the level to the minimum required by the migration, 5.1.1.2.

We then created some resources for the scalable distribution infrastructure, but we did not perform other customizations, therefore some of the tasks detailed next were not needed.

17.4.1 Upgrading the provisioning server to version 5.1.1.2

Prerequisite for the migration is the version of the provisioning server that must be 5.1.1.2 level. If your provisioning server is lower than version 5.1.1.2, you must upgrade it before you begin the migration.

The Tivoli Intelligent Orchestrator and Tivoli Provisioning Manager for Software products must also be upgraded to 5.1.1.2. The migration can be completed from any level of interim fix on 5.1.1.2, for example 5.1.1.2 with interim fix 3, but there is no requirement to install any interim fixes before you migrate.

Table 17-3 shows the upgrade path to 5.1.1.2 version:

► 5.1 to 5.1.1.1 through 5.1.0.2-TIV-TPM-FP0003 Fix Pack installation

Note: Tivoli Provisioning Manager 5.1 cannot be upgraded to 5.1.1. You can either install a fresh 5.1.1 system or upgrade to 5.1.1.1 installing the above-mentioned Fix Pack on top of a 5.1.0.2 installation.

- ► 5.1.1 to 5.1.1.1 through 5.1.1-TIV-TPM-FP0001 Fix Pack installation
- ► 5.1.1.1 to 5.1.1.2 through 5.1.1.1-TIV-TPM-FP0002 Fix Pack installation

Table 17-3 Upgrade path to 5.1.1.2 versions

Current Version	Target Version	Reference
5.1.0.2	5.1.1.1	5.1.0.2-TIV-TPM-FP0003 can be downloaded from this link: http://www-01.ibm.com/support/docview.wss?uid=swg24018333
		5.1.0.2-TIV-TIO-FP0003 can be downloaded from this link: http://www-01.ibm.com/support/docview.wss?uid=swg24018345
		5.1.0.2-TIV-TPMFSW-FP0003 can be downloaded from this link: http://www-01.ibm.com/support/docview.wss?uid=swg24018402

Current Version	Target Version	Reference
5.1.1	5.1.1.1	5.1.1-TIV-TPM-FP0001 can be downloaded from this link: http://www-01.ibm.com/support/docview.wss?uid=swg24018403 5.1.1-TIV-TIO-FP0001 can be downloaded from this link: http://www-01.ibm.com/support/docview.wss?uid=swg24018404 5.1.1-TIV-TPMFSW-FP0001 can be downloaded from this link: http://www-01.ibm.com/support/docview.wss?uid=swg24018346
5.1.1.1	5.1.1.2	5.1.1.1-TIV-TPM-FP0002 can be downloaded from this link: http://www-01.ibm.com/support/docview.wss?&uid=swg24021726 5.1.1.1-TIV-TIO-FP0002 can be downloaded from this link: http://www-01.ibm.com/support/docview.wss?uid=swg24021708 5.1.1.1-TIV-TPMFSW-FP0002 can be downloaded from this link: http://www-01.ibm.com/support/docview.wss?uid=swg24021756

17.4.2 Upgrading the common agent to version 1.3.2.29

Another prerequisite for the migration is the upgrade of the common agent to version 1.3.2.29 on both the depot servers and the endpoints that are participating in the software distribution process.

The depot servers must be upgraded before you upgrade the target computers, so do not upgrade them at the same time.

For the configuration of the systems used for this chapter, this operation was not required because there were no common agent installation at a previous version.

17.4.3 Copying the files for the scalable distribution infrastructure (SDI) installation

During the migration, the scalable distribution infrastructure will be installed:

- ► Agent Manager
- ► Tivoli Provisioning Manager for Dynamic Content Delivery
- ► Tivoli Provisioning Manager Job Management Service

Before you run the migration scripts, prepare for the installations by creating the appropriate directories and copying the images to the directories as detailed in Example 17-3.

Example 17-3 Preparing the files for the SDI infrastructure installation

The files needed for the scalable distribution infrastructure installation are contained in the Core Components installation file called, for an AIX at 64-bit, TPM_V711_CoreComp_AIXPPC64.tar.

With the below commands you create the directory sctructure required by the migration scripts to locate the installation files for the SDI components.

In the /tpm_images/U2823 we placed the TPM_V711_CoreComp_AIXPPC64.tar
file.

[root@risc550a][/tpm_images/U2823]> mkdir CASInstaller DCDInstaller
DMSInstaller

```
[root@risc550a][/tpm_images/U2823]> cd CASInstaller
[root@risc550a][/tpm_images/U2823/CASInstaller]> tar xvf
../AM_V142_AIXPPC64.tar
```

```
[root@risc550a][/tpm_images/U2823/CASInstaller]> cd ../DCDInstaller
[root@risc550a][/tpm_images/U2823/DCDInstaller]> tar xvf
../DCD_V21_AIXPPC64.tar
```

```
[root@risc550a] [/tpm_images/U2823/DCDInstaller]> cd ../DMSInstaller
[root@risc550a] [/tpm_images/U2823/DMSInstaller]> gunzip
../DMS_V20_multiplatf.tar.gz
[root@risc550a] [/tpm_images/U2823/DMSInstaller]> tar xvf
../DMS_V20_multiplatf.tar
```

The images are now ready to be used by the migration scripts.

17.4.4 Copying the backup tools to the 5.1.1.2 provisioning server

The backup tool is the tool that contains the script for the migration. You can obtain it from the Tivoli Provisioning manager installation media or image (TPM_V711_Install_UNIX.tar for a UNIX installation).

The file is called tpm5112migration.zip and must be extracted to the *\$TIO_HOME* directory on the Tivoli Provisioning Manager Version 5.1.1.2 system as detailed in Example 17-4 on page 554.

Note: You might want to back up the original *\$TIO_HOME*/migration directory before running the **unzip** command of the migration tool.

Example 17-4 Extracting the backup tools on the Tivoli Provisioning Manager Version 5.1.1.2 system

Once taken the tpm5112migration.zip file from TPM_V711_Install_UNIX.tar, copy it to the *\$TI0_HOME* directory on the Tivoli Provisioning Manager Version 5.1.1.2 system and run this command to unzip it:

[tioadmin@risc40pa][/opt/ibm/tivoli/tpm]> unzip tpm5112migration.zip

replace migration/sql/db2/reportViews.sql? [y]es, [n]o, [A]11, [N]one, [r]ename: y replace migration/sql/oracle/reportViews.sql? [y]es, [n]o, [A]11, [N]one, [r]ename: y

replace the existing files.

17.4.5 Backing up the LDAP server

If you are going to use your existing LDAP server when you migrate to version 7.1.1, we strongly recommend to create a backup of your LDAP server so that it can be restored if necessary.

For the scope of this chapter, we used a new LDAP server (Tivoli Directory Server), therefore the execution of this task was not required.

17.4.6 Pre-migration tasks for Tivoli Directory Server

WebSphere Application Server 6.1 is installed with Tivoli Provisioning Manager Version 7.1.1. This task configures the users in your existing Tivoli Directory server so that they are compatible with the latest application server version.

This task is only required if you are using your existing Tivoli Directory Server for your 7.1.1 provisioning environment.

For the scope of this chapter, we used a new LDAP server, therefore the execution of this task was not required.

17.4.7 Prerequisites for migrating automation packages

There are changes to the automation packages in 7.1.1. Before you begin the migration, backup your custom automation packages, ensure that all of the installed automation packages are at the correct version level, and list the 5.1.1.2 automation packages that you use in your provisioning operations.

These version 5.1.1.2 automation packages are being deprecated in version 7.1.1, but some of them are available on the Open Process Automation Library (OPAL) Web site:

http://www-01.ibm.com/software/tivoli/features/opal/

When the migration is complete, you can download the 5.1.1.2 automation packages from OPAL and restore your 5.1.1.2 custom automation packages. It is also recommended to uninstall any of the deprecated automation packages that you do not use in your provisioning operations. Uninstalling the automation packages will remove their record from your provisioning database.

To verify the automation packages version you can run the **tc-driver-manager.sh** command as shown in Example 17-5.

Example 17-5 tc-driver-manager.sh execution

```
The below command, with the "1" option, lists all the automation packages in the
provisioning database, their version and status.
The ouptut is just a sample output, so not all the packages returned in the output
are listed in this section:
[tioadmin@risc40pa][/opt/ibm/tivoli/tpm/tools]> tc-driver-manager.sh 1
2009-08-04 15:32:16,244 INFO log4j configureAndWatch is started with configuration
file: /opt/ibm/tivoli/tpm/config/log4j-util.prop
2009-08-04 15:32:16,630 INFO COPTDM004I Config directory:
"file:/opt/ibm/tivoli/tpm/config/".
2009-08-04 15:32:17,488 INFO COPTDM004I Config directory:
"file:/opt/ibm/tivoli/tpm/config/".
2009-08-04 15:32:17,506 INFO COPTDM002I Driver directory: "Driver directory:
"/opt/ibm/tivoli/tpm/drivers/".".
2009-08-04 15:32:29,382 INFO COPTDM004I Config directory:
"file:/opt/ibm/tivoli/tpm/config/".
2009-08-04 15:32:34,035 INFO
```

TC Driver Name	Version	Status
AIX-LVM	5.1.1.2.2395.870.33.100	installed
AIX-Operating-System	5.1.1.2.2395.870.33.100	installed

AIX_PATCH	5.1.1.2.2395.870.33.100	installed
Apache-Web-Server-Windows	5.1.1.2.2395.870.33.100	installed
Blade-Center-4p-Gb-Eth	5.1.1.2.2395.870.33.100	installed
CDS	5.1.1.2.2395.870.33.100	installed
CHAMPS	5.1.1.2.2395.870.33.100	installed
CIMClient	5.1.1.2.2395.870.33.100	installed
CSM-Linux-Install	5.1.1.2.2395.870.33.100	installed
CiscoSwitchDiscovery	5.1.1.2.2395.870.33.100	installed
CitScannerAgent	5.1.1.2.2395.870.33.100	installed
Cygwin	5.1.1.2.2395.870.33.100	installed
OUTPUT TRUNCATED		
vmware-4	5.1.1.2.2395.870.33.100	installed
weblogic	5.1.1.2.2395.870.33.100	installed
windows-operating-system	5.1.1.2.2395.870.33.100	installed
yast	5.1.1.2.2395.870.33.100	installed
zVM_Server	5.1.1.2.2395.870.33.100	installed

17.4.8 Exporting the 5.1.1.2 report query

Before you migrate the 5.1.1.2 data to the 7.1.1 provisioning server, export the 5.1.1.2 report query.

Use an SQL query to export the report query. The customized query in the output will be used to migrate your custom reports using the BIRT development environment in version 7.1.1.

For the scope of this chapter, we did not perform this task, not having custom reports created in the 5.1.1.2 provisioning server.

17.4.9 Migrating file repositories

Software binaries that are located in local file repositories in version 5.1.1.2 will not be migrated to version 7.1.1 because the location of the file repositories can change.

Manually back up the software binaries and note the directories for the file repositories, so that you can recreate them on the 7.1.1. provisioning server after the migration.

17.4.10 Migrating images created using Tivoli Provisioning for OS Deployment

There is no migration for the images created with Tivoli Provisioning Manager for OS Deployment Embedded Edition 5.1.1.2. The version 5.1.1.2 images are formatted differently than the images that are created with Tivoli Provisioning Manager for OS Deployment, the product that is integrated in Tivoli Provisioning Manager Version 7.1.1.

To recreate the images, you can:

- 1. Recreate your images in the 7.1.1. provisioning environment after the migration.
- 2. Use a test 7.1.1 provisioning environment to recapture the images held on the 5.1.1.2 provisioning environment. After the full data migration of your 7.1.1 production environment is complete, you will run a provisioning workflow on the 7.1.1. provisioning server to clone the images of your test environment and move them to your (migrated) production environment.

For the scope of this chapter, we did not perform this task. We installed the Tivoli Provisioning Manager for OS Deployment as part of the Core Components installation, but we did not have any image created with the Tivoli Provisioning Manager for OS Deployment Embedded Edition 5.1.1.2.

17.4.11 Removing nicknames and views

Migration is not supported for Tivoli Configuration Manager gateway coexistence that is configured and integrated with Tivoli Provisioning Manager or Tivoli Provisioning Manager for Software. Before you can migrate to version 7.1.1, all gateways and Tivoli Monitoring Framework endpoints must be upgraded to the scalable distribution infrastructure (SDI) endpoint and the nicknames and views that were created by the Tivoli Configuration Manager coexistence must be removed.

For the scope of this chapter, we did not perform this task, not having configured the coexistence with Tivoli Configuration Manager in our Tivoli Provisioning Manager Version 5.1.1.2 environment.

For details about this task, refer to *Tivoli Provisioning Manager Version 7.1.1 Migration Guide* at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ibm.t ivoli.tpm.ins.doc/tpm_migrate_guide.pdf

17.5 Tivoli Provisioning Manager Version 7.1.1 pre-installation tasks

In this section we describe the pre-installation tasks and checks to be performed on the Tivoli Provisioning Manager Version 7.1.1 system.

Before installing Tivoli Provisioning Manager Version 7.1.1, the system has been prepared with the prerequisite software. Customizations of the systems are described in the *Tivoli Provisioning Manager Version 7.1.1 Migration Guide* at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ibm.t ivoli.tpm.ins.doc/tpm_migrate_guide.pdf)

Here is a summary of the checks and the related order of execution:

- 1. Check the prerequisite RPMs installation for the Tivoli Provisioning Manager Version 7.1.1 installation.
- 2. Set the PATH variable to include the GNU tar at first place.
- 3. Install openssl and openssh packages.
- 4. Verify 64-bit cpu/kernel configuration.
- 5. Verify the automount daemon status.
- 6. Check the required Paging Space.
- Check the required maxuproc setting.
- 8. Check the required ulimit settings.
- 9. Check the /tmp permission.
- 10. Check disk space availability for the installation.

Note: For this scenario we pre-allocated the hardware by creating a separate volume group to be used by Tivoli Provisioning Manager Version 7.1.1, and we created all the filesystems and mount points matching the default installation location of the Middleware, Core Components and Web services components.

- 11.Check umask setting.
- 12. Check the environment configuration:
 - a. Host name requirements
 - a. /etc/hosts file requirements
 - a. sshd_config configuration
- 13. Prepare the installation media.

For details about these tasks, refer to the *Tivoli Provisioning Manager Version 7.1.1 Migration Guide* at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ibm.t ivoli.tpm.ins.doc/tpm_migrate_guide.pdf

Details of the foregoing checks for the system used for this installation, can be found in Appendix B, "Tivoli Provisioning Manager Version 7.1.1 pre-installation checks" on page 685.

17.6 Tivoli Provisioning Manager Version 7.1.1 installation

You can start the launchpad after verifying that all the prerequisites for the installation as detailed in *Tivoli Provisioning Manager Version 7.1.1 Migration Guide* at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ibm.t ivoli.tpm.ins.doc/tpm_migrate_guide.pdf

The launchpad is used by Tivoli Provisioning Manager Version 7.1.1 to install all the components. It requires a Web Browser to be installed on the system when you are running it. We require to use VNC as X session to run a remote installation on an AIX system.

For the scope of this chapter, we tested a single server installation on AIX 6.1. New in Tivoli Provisioning Manager Version 7.1.1 release is the possibility to install on AIX 6.1 and use a single server installation, having the administrative workstation on the same AIX 6.1 system as the provisioning server.

17.6.1 Starting the launchpad

The launchpad must be run each time you want to install any Tivoli Provisioning Manager component.

The script to invoke the launchpad on AIX is called launchpad.sh and it can be found in the installation location where the TPM_V711_Install_UNIX.tar was extracted.

After the launchpad is invoked, a Web Browser session is started and the Tivoli Provisioning Manager Version 7.1.1 welcome page is shown as detailed in Figure 17-1.



Figure 17-1 Tivoli Provisioning Manager Version 7.1.1 Welcome Page

17.6.2 Installing the middleware

The middleware consists of these applications:

- Application Server, in this case WebSphere Application Server Network Deployment 6.1.0.23.
- Database Server, in this case IBM DB2 9.5 FP3a.
- ► Directory Server, in this case IBM Tivoli Directory Server 6.2.0.2.
- Additional Software, installed by the Middleware installation.

The middleware installer is designed to record the options you select during the installation in a directory referred to as the "workspace", and then configure the components selected as a single deployed application. The recorded options can also be imported by other installers so that some fields can be filled automatically for you.

After a plan has been deployed, the middleware installer cannot subsequently deploy additional features and products onto the computer at a later time. The

existing plan must first be completely undeployed through the middleware installer before a different set of features and products can be deployed.

The composition and details of the deployment, as well as any logs generated by the middleware installer process are located in the workspace. For AIX the default directory is /ibm/tivoli/mwi/workspace. We kept this directory name to its default value; we just created a filesystem with that mount point before running the middleware installation.

The middleware installer generates several log files in the foregoing path.

For details about the log files location, refer to *Tivoli Provisioning Manager Version 7.1.1 Migration Guide* at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ibm.t ivoli.tpm.ins.doc/tpm_migrate_guide.pdf

For this chapter, we performed a custom installation, by selecting Custom Installation from the launchpad menu as shown in Figure 17-2.

) Mozilla Firefox		E
Tivoli Provisioning M	anager 7.1.1	
Welcome	Custom Installation	
Installation Planning		
Custom Installation	For a custom installation, you can choose the topology that you want to use and customize installation settings.	
Exit	1. Install the middleware	
	The middleware installer can install and configure IBM middleware or configure existing middleware. See the Installation Guide for details about supported middleware versions and installation and configuration options.	1
	1.1 & Verify middleware installation prerequisites	
	1.2 🖏 Install middleware	
	1.3 🚰 Back up WebSphere configuration	
	2. Install the base services	
	If your application server is installed on the following platforms: AIX 5.3, Red Hat Enterprise Linux, SUSE Linux Enterprise Server 10 SP2 (BM System z 64-bit), or Solaris 10, you must run the base services installer from a separate Windows computer.	
	2.1 Ger Verify base services installation prerequisites	
	2.2 🚵 Install the base services	
	2.3 💒 Install the language pack (required for non-English installation only)	
	2.4 💒 Back up base services home directory	
	3. Install Tivoli Provisioning Manager core components	
	This installer installs and configures core components and required software for the provisioning server. See the Installa Guide for details about the components that are installed.	tio
	3.1 & Verify core components installation prerequisites	
	3.2 🚵 Install core components	
	4. Install the Tivoli Provisioning Manager Web components	
	You must install the Web components from the same computer that you are using for the base services installation.	

Figure 17-2 Custom Installation selection from launchpad

Before installing any component, you have to first verify the installation prerequisites by clicking the corresponding link and selecting the check box at the bottom of the page you get. You are then redirected to the Custom Installation panel where you can select **Install Middleware**.

At the beginning of the Tivoli Provisioning Manager Version 7.1.1 we unpacked the installation files. The file used for the Middleware installation, for an AIX at 64-bit, is called TPM_V711_Midlwr_AIXPPC64.tar. The content of this archive is shown in Example 17-6.

Example 17-6 Content of TPM_V711_Midlwr_AIXPPC64.tar archive

Unpacking the TPM_V711_Midlwr_AIXPPC64.tar file you get these directories:

```
aix/DB2-ESE_9.5
aix/DB2-ESE_9.5_FP3a
aix/TIV-DirectoryServer_6.2.0
aix/WS-ESS_6.1_GA
aix/WS-WAS_IHS_6.1.0_FP23
aix/WS-WAS_ND_6.1.0_23_Custom_ISCAE71
aix/WS-WAS_ND_6.1.0_Supplemental_64bit
aix/WS-WAS_Plugins_6.1.0_FP23
aix/WS-WAS_UpdateInstaller 7.0.0.3
```

The first time the middleware installation is run on a system, the IBM Autonomic Deployment Engine is installed automatically as a first step.

The installer then searches for existing software instances to be reused. In case of a fresh system, such as the one we used for this scenario, nothing is found and the panel in Figure 17-3 is shown.

🙆 Tivoli Middleware Ir	staller
IBM.	Select the features to deploy on the local machine.
	🖌 Database Server
	The Database Server is used to store details about the attributes and history of each configuration item and the details about the relationships among configuration items.
	Z Directory Server
	The Directory Server is used to secure the J2EE Server. This feature should be selected to either install a new directory server locally or reuse a local directory server.
	✓ J2EE Server
	The J2EE Server is the application server used to serve and manage the application.
	Secure the J2EE Server using the Directory Server
InstallShield	
1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	
	< <u>Back</u> <u>Next</u> > <u>Cancel</u>

Figure 17-3 Features to deploy

In the next panels you must provide, in the order listed, the following configuration details:

- 1. Machine fully qualified host name
- 2. Password used during the installation (you can decide to use the same password for the subsequent selection by checking the "Use this password as the value for all subsequent passwords" check box
- 3. Configuration parameters for DB2 Enterprise Server Edition Version 9.5.0.3a
- 4. Configuration parameters for Database Instance (ctginst1)
- 5. Configuration parameters for the Default Database Instance (db2inst1)
- 6. Configuration parameters for IBM Tivoli Directory Server Version 6.2
- 7. Configuration parameters for IBM Tivoli Directory Server Database Instance (idsccmdb)
- 8. Configuration parameters for WebSphere Application Server security
- 9. Configuration parameters for WebSphere Application Server ND Version 6.1.0.23
- 10. Configuration parameters for IBM HTTP Server 6.1.0.23

11.Configuration parameters for WebSphere Application Server plug-in for the IBM HTTP Server

You can specify:

- The directory containing the middleware images (/tpm_images/U2823 in our installation)
- The temporary directory where the middleware will store temporary files and extract middleware images (/tmp/swrepos in our installation)

You can then select the option to deploy the plan. Before the actual installation starts, you get the detailed list of actions performed in the deployment plan.

A summary of the actions performed by the middleware installation is shown in Figure 17-4.

Oeployment Choices	
IBM.	The following plan has been generated. To enter configuration parameters for this plan, choose Next. DB2 Enterprise Server Edition Version 9.5.0.3a Configuration for DB2 Enterprise Server Edition Configuration of DB2 Enterprise Server Edition Configuration for BM Tivoli Directory Server WebSphere Application Server ND Version 6.1.0.23 Configuration for WAS ND IBM HTTP Server Version 6.1.0.23 Embedded Security Services
	< Back Next > Cancel

Figure 17-4 Deployment Plan summary

Tivoli Middleware Installer

IEM.

Configuration for IBM Tivoli Directory Server

WebSphere Application Server ND

Configuration for WAS ND

IBM HTTP Server

Embedded Security Services

InstallShield

Einish

On successful installation completion, you get the panel shown in Figure 17-5.

Figure 17-5 Successful middleware installation completion

17.6.3 Creating the database and database server user

After installing the middleware, you have to create the database and database server user.

Example 17-7 shows the detailed steps executed for the user and database creation.

Example 17-7 database server user and database creation

To create the maximo user, you can run these command line interface utilities:

[root@risc550a][/home]> useradd -d /home/maximo -m maximo

You can set the password of the user by running: [root@risc550a][/home]> passwd maximo Changing password for "maximo" maximo's New password: Enter the new password again: Run the following command to avoid changing the maximo password after the first login:

```
[root@risc550a][/home]> pwdadm -c maximo
```

Having pre-allocated the /home/maximo and /home/ctginst1 directories we run these commands to correctly set the home directory ownership:

```
chown -R maximo.staff /home/maximo
chown -R ctginst1.db2iadm1 /home/ctginst1
```

You can now create the database by running these commands:

```
su - ctginst1
set DB2INSTANCE=ctginst1
db2start
db2 create db maxdb71 using codeset UTF-8 territory US
```

To verify the database creation run the command:

db2 list database directory

The following output is listed:

System Database Directory

Number of entries in the directory = 1

Database 1 entry:

Database alias	= MAXDB71
Database name	= MAXDB71
Local database directory	= /home/ctginst1
Database release level	= c.00
Comment	=
Directory entry type	= Indirect
Catalog database partition number	= 0
Alternate server hostname	=
Alternate server port number	=

Note: This is a prerequisite step for the core components installation.

17.6.4 Core components installation

The core components must be installed on the provisioning server. They represents the core Tivoli Provisioning Manager Version 7.1.1 components.

Considering that we are describing a migration installation, it differs from a fresh installation in that not all the components are installed at the same time. You have to perform a custom installation, selecting only:

- Tivoli Provisioning Manager
- Tivoli Provisioning Manager for OS Deployment
- Tivoli Monitoring agent

Important: *Do not* select the following core components:

- Agent Manager
- Tivoli Provisioning Manager for Dynamic Content Delivery
- Tivoli Provisioning Manager Job Management Service

They will be installed as part of the migration process that is described later in this chapter.

As a prerequisite for this installation, make sure that the middleware just installed is up and running.

Starting the middleware

Example 17-8 shows the detailed steps to start the middleware or check its status.

Important: Until the Tivoli Provisioning Manager Version 7.1.1 installation is complete and the migration scripts executed, restart the WebSphere Application Server manually as detailed in Example 17-8 on page 568.

The automatic startup of the Tivoli Provisioning Manager Version 7.1.1 using the startup script (tio.sh) can only be performed after the completion of these tasks:

- Migration scripts execution
- Base Services and Web components installation
- Host name change script execution

Example 17-8 Starting the middleware

```
The middleware consist of a database server (below referenced as DB2),
a directory server (below referenced as ITDS) an HTTP server (below
referenced as HTTP) and an application server (below referenced as
WAS).
Follow these steps to start the middleware:
```

DB2

```
[root@risc550a] [/home]> su - ctginst1
[ctginst1@risc550a] [/home/ctginst1]> db2start
08/04/2009 17:58:12 0 0 SQL1063N DB2START processing was
successful.
SQL1063N DB2START processing was successful.
```

In case the database server is already running, the output will look like:

```
[ctginst1@risc40pa][/home/ctginst1]> db2start
08/26/2009 12:05:13 0 0 SQL1026N The database manager is
already active.
SQL1026N The database manager is already active.
```

ITDS

The directory server makes use of a database instance, therefore you have to check first that the database server instance for the directory server is running, by using these commands:

```
[root@risc550a][/home]> su - idsccmdb
[ctginst1@risc550a][/home/ctginst1]> db2start
```

The directory server administrative daemon can be started by running:

[root@risc550a][/opt/IBM/ldap/V6.2/sbin]> idsdiradm -I idsccmdb GLPADM056I Admin server starting. GLPCOM025I The audit plugin is successfully loaded from libldapaudit.a. GLPCOM022I The database plugin is successfully loaded from libback-config.a. GLPADM060I The admin server backup and restore server configuration entry is not enabled. GLPCOM024I The extended Operation plugin is successfully loaded from libloga.a. GLPCOM003I Non-SSL port initialized to 3538. Once the admin daemon is started, you can start the directory server instance process by running:

[root@risc550a][/opt/IBM/ldap/V6.2/sbin]> ibmslapd -I idsccmdb GLPSRV041I Server starting. GLPCTL113I Largest core file size creation limit for the process (in bytes): '1073741312'(Soft limit) and '-1'(Hard limit). GLPCTL119I Maximum Data Segment(Kbytes) soft ulimit for the process is -1 and the prescribed minimum is 262144. GLPCTL119I Maximum File Size(512 bytes block) soft ulimit for the process is -1 and the prescribed minimum is 2097151. GLPCTL122I Maximum Open Files soft ulimit for the process is 8192 and the prescribed minimum is 500. GLPCTL119I Maximum Physical Memory(Kbytes) soft ulimit for the process is -1 and the prescribed minimum is 262144. GLPCTL119I Maximum Stack Size(Kbytes) soft ulimit for the process is -1 and the prescribed minimum is 65536. GLPCTL119I Maximum Virtual Memory(Kbytes) soft ulimit for the process is -1 and the prescribed minimum is 1048576. GLPCOM024I The extended Operation plugin is successfully loaded from libevent.a. GLPCOM024I The extended Operation plugin is successfully loaded from libtranext.a. GLPCOM024I The extended Operation plugin is successfully loaded from libldaprepl.a. GLPSRV1551 The DIGEST-MD5 SASL Bind mechanism is enabled in the configuration file. GLPCOM021I The preoperation plugin is successfully loaded from libDigest.a. GLPCOM024I The extended Operation plugin is successfully loaded from libevent.a. GLPCOM024I The extended Operation plugin is successfully loaded from libtranext.a. GLPCOM023I The postoperation plugin is successfully loaded from libpsearch.a. GLPCOM024I The extended Operation plugin is successfully loaded from libpsearch.a. GLPCOM025I The audit plugin is successfully loaded from libldapaudit.a. GLPCOM024I The extended Operation plugin is successfully loaded from libevent.a. GLPCOM023I The postoperation plugin is successfully loaded from libpsearch.a. GLPCOM024I The extended Operation plugin is successfully loaded from libpsearch.a.

GLPCOM022I The database plugin is successfully loaded from libback-config.a. GLPCOM024I The extended Operation plugin is successfully loaded from libevent.a. GLPCOM024I The extended Operation plugin is successfully loaded from libtranext.a. GLPCOM023I The postoperation plugin is successfully loaded from libpsearch.a. GLPCOM024I The extended Operation plugin is successfully loaded from libpsearch.a. GLPCOM022I The database plugin is successfully loaded from libback-rdbm.a. GLPCOM010I Replication plugin is successfully loaded from libldaprepl.a. GLPSRV189I Virtual list view support is enabled. GLPCOM021I The preoperation plugin is successfully loaded from libpta.a. GLPSRV194I The Record Deleted Entries feature is disabled. Deleted entries are immediately removed from the database. GLPSRV207I Group conflict resolution during replication is disabled. GLPSRV200I Initializing primary database and its connections. GLPRDB126I The directory server will not use DB2 selectivity. GLPCOM024I The extended Operation plugin is successfully loaded from libloga.a. GLPCOM024I The extended Operation plugin is successfully loaded from libidsfget.a. GLPSRV180I Pass-through authentication is disabled. GLPCOM003I Non-SSL port initialized to 389.

To check the connection to the directory server you can run this command:

[root@risc550a][/opt/IBM/ldap/V6.2/bin]> ibmdirctl -D cn=root -w
<password> -h risc550a.rot.it.ibm.com status
Directory server is running.

HTTP

The command below checks the http server status.

[root@risc550a][/usr/IBM/HTTPServer/bin]> ps -ef|grep -i http root 438526 499798 0 19:46:37 pts/1 0:00 grep -i http root 512148 1 14 19:46:36 - 0:00 /usr/IBM/HTTPServer/bin/httpd -d /usr/IBM/HTTPServer -k start In case it is down, you can start the http server by running the command:

/usr/IBM/HTTPServer/bin/apachectl start

WAS

To completely startup the application server you have to start these processes:

Deployment Manager Node MXServer Application Server

You can check the status of these processes by running the **serverStatus.sh** script as shown below:

[root@risc550a][/usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/bin]>
serverStatus.sh MXServer -username maxadmin -password <password>

The output looks like:

ADMU0116I: Tool information is being logged in file

/usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/logs/MXServer/serverS
tatus.log
ADMU0128I: Starting tool with the ctgAppSrv01 profile
ADMU0500I: Retrieving server status for MXServer
ADMU0509I: The Application Server "MXServer" cannot be reached. It
appears to be stopped.

From the command output above you see that all the processes are stopped. To start the **Deployment Mananger**, use this command:

[root@risc550a][/usr/IBM/WebSphere/AppServer/profiles/ctgDmgr01/bin]>
startManager.sh
ADMU0116I: Tool information is being logged in file

/usr/IBM/WebSphere/AppServer/profiles/ctgDmgr01/logs/dmgr/startServer.l
og
ADMU0128I: Starting tool with the ctgDmgr01 profile
ADMU3100I: Reading configuration for server: dmgr
ADMU3200I: Server launched. Waiting for initialization status.
ADMU3000I: Server dmgr open for e-business; process id is 434406

To start the Node use this command:

[root@risc550a][/usr/IBM/WebSphere/AppServer/profiles/ctgDmgr01/bin]>
cd ../../ctgAppSrv01/bin
[root@risc550a][/usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/bin]>
startNode.sh
ADMU0116I: Tool information is being logged in file

/usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/logs/nodeagent/startS
erver.log
ADMU0128I: Starting tool with the ctgAppSrv01 profile
ADMU3100I: Reading configuration for server: nodeagent
ADMU3200I: Server launched. Waiting for initialization status.
ADMU3000I: Server nodeagent open for e-business; process id is 422104

To start the MXServer application server, use this command:

[root@risc550a][/usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/bin]>
startServer.sh MXServer
ADMU0116I: Tool information is being logged in file

/usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/logs/MXServer should contain failure information.

The core components installation makes use of the launchpad as all the other Tivoli Provisioning Manager Version 7.1.1 components.

Before installing the core component, you have to first verify the installation prerequisites by clicking the corresponding link and selecting the check box at the bottom of the page you get. You are then redirected to the Custom Installation panel where you can select **Install core components**. After selecting the language used for the wizard and accepting the license agreement, the Topology Configuration panel in Figure 17-6 is shown.

🗙 IBM Tivoli Provisioning	Manager	- D ×
TEW	Topology Configuration	
IBM.	Database Information Select the type of relational database available in your environment. Select remote database check box if you are using remote database Image: Image	.k
	LDAP Directory Server Information Select the type of LDAP directory available in your environment. Tivoli Directory Server Microsoft Active Directory The maxadmin user exists in the LDAP repository 	
InstallShield	< <u>B</u> ack <u>N</u> ext > <u>C</u> a	ncel

Figure 17-6 Topology Configuration panel for DB2 and ITDS

Note: By default, the check box The maxadmin user exists in the LDAP repository is checked.

The Middleware installer does not create the maxadmin user into the LDAP repository, therefore deselect this check box unless you manually added the user.

Scrolling down the Topology Configuration panel, you can specify to reuse the Middleware Installer Workspace Information by selecting the **Import data from middleware installer workspace** check box and specifying the workspace location as shown in Figure 17-7.

IBM.	
	The maxadmin user exists in the LDAP repository
	Middleware Installer Workspace Information
	Select the check box if you want to import data from Middleware Installer Workspace and enter the workspace location.
	Mimport data from Middleware Installer workspace
	Middleware Installer workspace directory
	/ibm/tivoli/mwi/workspace
	Browse
	Select this option if you are using service IP addresses and host names for the computers in your installation, for example, in an HADR environment. The host names that you specify in this installer must match the host names specified in the middleware installer.
	Use Service IP
station.	
etallShield	

Figure 17-7 Topology Configuration panel for Middleware installer workspace

You then get the Select Components panel.

Important: *Do not* make the following selections in the Select Component panel:

- Back up Database and WebSphere Application Configuration
- Agent Manager
- Tivoli Provisioning Manager for Dynamic Content Delivery
- Tivoli Provisioning Manager for Job Management Service

In the installation for this chapter, we selected the optional installation of Tivoli Provisioning Manager for OS Deployment, therefore we have been asked to accept the license agreements for its installation.

At the beginning of the Tivoli Provisioning Manager Version 7.1.1 we unpacked the installation files. The file used for the Core Components installation, for an AIX at 64-bit, is called TPM_V711_CoreComp_AIXPPC64.tar. The content of this archive is shown in Example 17-9.

Example 17-9 Content of TPM_V711_CoreComp_AIXPPC64.tar archive

Unpacking the TPM_V711_CoreComp_AIXPPC64.tar file you get these files:

AM_V142_AIXPPC64.tar DB2_CLIENT_V95_AIXPPC64.tar.gz DCD_V21_AIXPPC64.tar DMS_V20_multiplatf.tar.gz ITM_Agent_V711_AIX.tar.gz TPM_V711_Disk1_AIXPPC64.tar TPM_V711_Disk2_AIXPPC64.tar TPM_V711_Disk3_Unix.tar.gz TPMf0Sd-Full-7.1.0.0-build-080.96-aix.tar.gz

You do not need to further uncompress or unpack these files. The installer will manage them.

At this point the following actions take place:

- Installation file integrity check
- DB2 prerequisites check
- Disk space check
- WebSphere Network Deployment configuration check

You then get the Installation Preview panels without specifying any configuration details for the Middleware components, considering that we instructed the installer to reuse the Middleware Installer Workspace Information.

When the installation is complete you get the panel in Figure 17-8. Click **Finish** to complete the installation.



Figure 17-8 Core Components installation completed panel

As noted in the foregoing message, you cannot start the Tivoli Provisioning Manager at this stage. You have to first complete the migration, then install the Base Service, Web components and continue with the host name changes tasks before starting it.

To verify the successful Core Components installation, check for the existence of these directories:

- /opt/IBM/tivoli/tpm/xml
- /opt/IBM/tivoli/tpm/drivers

Also check for these files:

- \$TIO_HOME/config/dcm.xml
- \$TIO_HOME/config/user-factory.xml
- \$TIO_HOME/config/crypto.xml

The next step in the installation is to prepare for the migration, by completing the property file that will be used by the provisioning servers.

17.7 Completing the property file

The property file is packaged in the tpm5112migration.zip file on the Tivoli Provisioning Manager Version 7.1.1 installation media or image, TPM_V711_Install_UNIX.tar in our environment.

The tpm5112migration.zip file must be extracted to the Tivoli Provisioning Manager Version 5.1.1.2 server.

There is a single property file that manages all of the parameters required for the scripts to back up the Tivoli Provisioning Manager Version 5.1.1.2 server and complete the migration to the Tivoli Provisioning Manager Version 7.1.1 server. When you run the scripts during the migration, the scripts will pull the parameters values from this file.

These parameters are then used for the following scripts that are run on the Tivoli Provisioning Manager Version 7.1.1 server:

- ▶ tpm711restore.sh
- tpm711migrate.sh
- tpm711ChangeDBHost.sh
- tpm711ChangeOtherHost.sh

Important: All parameters that specify a value in brackets ([]) are example values and must be reviewed. If the example value is correct, just delete the brackets, otherwise delete the example value and the brackets and type the correct value.

The script will check that all brackets are removed for the required parameters.

In case you use DB2 as database server, remove or comment the Oracle-specific parameters from the tpmmigrate unix.properties file:

- 1. orclChangeWordSize
- 2. orclOSUser

Example 17-10 shows a sample tpmmigrate_unix.properties file filled with the values required by the migration.

You can use this file as a reference after you have completed the default with all the parameters that apply to your environment.

Each section in the file has a comment that provides details about its use and explanation about the parameter to configure.

Example 17-10 Sample tpmmigrate_unix.properties file filled in

```
******************
# This file defines all of the configuration parameters that are required
# for the migration.
# All parameter values must be reviewed and updated:
# - Values that are not in square brackets are generated values; no change
 is required.
#
# - Values that are in square brackets are default values or examples.
   Remove the square brackets so that the value is used.
#
# Lines that begin with a the pound sign (#) are commented out.
# All parameter values are listed in the following order:
# - The environment version that they are used in.
# - The components of the migration operation as listed here:
 - 5.1.1.2 and 7.1.1 Database configurations
#
 - 5.1.1.2 and 7.1.1 LDAP configurations
#
 - 5.1.1.2 and 7.1.1 WebSphere configurations
 - 5.1.1.2 Backup configurations
#
#
 - 5.1.1.2 LDAP configurations
#

    7.1.1 Restoration and migration configurations

 - 7.1.1 Installation configurations
#
 - 7.1.1 Services configurations
#
#
 - 7.1.1 Agent manager configurations
# - 7.1.1 Dynamic content delivery configurations
# - 7.1.1 Database Administration Server configurations
 - 7.1.1 Database configurations
  - 7.1.1 Deployment manager configurations
#
 - 7.1.1 WebSphere Application Server configurations
****
##
## Migration configurations for both the 5.1.1.2 and 7.1.1 environments
##
## 5.1.1.2 and 7.1.1 Database configurations
## dbIsRemote (5.1.1.2 and 7.1.1): Is database remote or local?
##
# yes = The database is a remote database.
# no = The database is a local database.
```

```
# This parameter is used by the tpm5112backup script.
# It is also used by the tpm711restore, tpm711migrate, tpm711ChangeDBHost,
# and tpm711ChangeOtherHost scripts.
# After you run the tpm5112backup script, change the value if it is different
# for your 7.1.1 system.
#-----
dbIsRemote=no
     _____
## orclOSUser (5.1.1.2 and 7.1.1): OS user name for Oracle Administrator
##
# This parameter is used by the tpm5112backup script.
# It is also used by the tpm711restore and tpm711migrate scripts.
# After you run the tpm5112backup script, change the value if it is different
# for your 7.1.1 system.
# This parameter is only used for Oracle configurations.
# If DB2 is used, remove this parameter.
#_____
#orclOSUser=[oracle]
## 5.1.1.2 and 7.1.1 WebSphere Application Server configurations
_____
## wasUser (5.1.1.2 and 7.1.1): WebSphere deployment manager administrator user
##
# This parameter is used by the tpm5112backup script.
# It is also used by the tpm711migrate and tpm711ChangeOtherHost scripts.
# After you run the tpm5112backup script, change the value if it is different
# for your 7.1.1 system.
#-----
wasUser=wasadmin
## 5.1.1.2 and 7.1.1 LDAP configurations
## ldapType (5.1.1.2 and 7.1.1): 7.1.1 LDAP type
##
# ITDS = IBM Tivoli Directory Server
```

```
****
##
## Migration configurations for the 5.1.1.2 environment
##
***********
## 5.1.1.2 Backup configurations
#-----
## outputDir (5.1.1.2): The directory where the backup files will be stored.
##
# This directory will be created if it is not yet created when the backup
# script is run on the 5.1.1.2 system.
# This parameter is used by the tpm5112backup script.
#_____
outputDir=/opt/ibm/tivoli/tpm/migration/backup
    _____
## removeAuditData (5.1.1.2): Remove the existing audit table entries
## before doing the backup? Note that removed entries are not recoverable.
##
# ves = Remove the entries.
# no = Do not remove the entries.
# This parameter is used by the tpm5112backup script.
#_____
removeAuditData=yes
#_____
## zipBackupFiles (5.1.1.2): Zip backup files after running tpm5112backup.sh?
##
# yes = zip backup files
# no = do not zip backup files
# This parameter is used by the tpm5112backup script.
#_____
                               -----
zipBackupFiles=no
```

```
## 5.1.1.2 LDAP configurations
_____
## ldapUseNew (5.1.1.2): Do you want to use a new or existing LDAP?
## [new or exist]
##
# This parameter is used by the tpm5112backup script.
#_____
ldapUseNew=new
#-----
## baseDN (5.1.1.2): The LDAP server configuration information - base.
##
# This parameter is used by the tpm5112backup script.
#-----
baseDN=ou=SWG,o=IBM,c=US
#-----
## groupBaseDN (5.1.1.2): The LDAP server configuration information - group.
##
# This parameter is used by the tpm5112backup script.
#-----
groupBaseDN=ou=groups.ou=SWG.o=IBM.c=US
#_____
## userBaseDN (5.1.1.2): The LDAP server configuration information - user.
##
# This parameter is used by the tpm5112backup script.
#_____
userBaseDN=ou=users,ou=SWG,o=IBM,c=US
**************
##
## Migration configurations for the 7.1.1 environment
##
```

#_____

```
## backupDir (7.1.1): The directory location of the backup artifacts.
##
# This directory must be manually created if it does not exist on the 7.1.1
# system. Before the restore script is run, the backup data from the 5.1.1.2
# system must be copied under this directory in the same folder structure
\# that was created when the data was backed up on the 5.1.1.2 system.
# This parameter is used by the tpm711restore and tpm711migrate scripts.
#-----
backupDir=/opt/IBM/tivoli/tpm/migration/backup
#-----
## fq5112HostName (7.1.1): The fully gualified host name for Tivoli
## Provisioning Manager 5.1.1.2.
##
# This parameter is used by the tpm711ChangeDBHost and tpm711ChangeOtherHost
# scripts.
#-----
fg5112HostName=risc40pa.rot.it.ibm.com
#-----
## fq711HostName (7.1.1): The fully gualified host name for Tivoli
## Provisioning Manager 7.1.1.
##
# This parameter is used by the tpm711ChangeDBHost and tpm711ChangeOtherHost
# scripts.
#_____
fg711HostName=risc550a.rot.it.ibm.com
#-----
## imagesDir (7.1.1): The directory location of the media images.
##
# You must create this directory on the 7.1.1 system, and then
# copy the agent manager, device manager service and the dynamic content
# delivery install binaries to this directory.
# The install binary for these three components can be found from the 7.1.1
# DVD media.
# This parameter is used by the tpm711migrate script.
#-----
imagesDir=/tpm images/U2823
#-----
## midDbBackup (7.1.1): Start a database backup halfway through the migration?
##
# ves = Perform database backup.
# no = Do not perform database backup.
# This parameter is used by the tpm711migrate script.
```

midDbBackup=no ## 7.1.1 Installation configurations _____ ## sdiClientSSLPort (7.1.1): The scalable distribution infrastructure client ## SSL port. ## # This parameter is used by the tpm711migrate script that is run on the # 7.1.1 system. #----sdiClientSSLPort=9046 #-----## sdiServerSSLPort (7.1.1): The scalable distribution infrastructure server ## SSL port. ## # This parameter is used by the tpm711migrate script. #----sdiServerSSLPort=9045 #-----## tpmfosdDataDir (7.1.1): The Tivoli Provisioning Manager for OS Deployment ## data location. ## # If Tivoli Provisioning Manager for OS Deployment software is not required, # remove this parameter. # This parameter is used by the tpm711ChangeOtherHost script. #_____ tpmfosdDataDir=/opt/tpmfosd files #-----## tpmHttpPort (7.1.1): The scalable distribution infrastructure server ## non-SSL port. ## # This parameter is used by the tpm711migrate script. #_____ tpmHttpPort=9080 _____ ## tpmHttpsPort (7.1.1): The Tivoli Provisioning Manager SSL port ## # This parameter is used by the tpm711migrate script. #_____

#-----

tpmHttpsPort=9443

_____ ## tpmUiUser (7.1.1): The administrative user login name for the provisioning ## Web interface. ## # This parameter is used by the tpm711migrate script. #----tpmUiUser=maxadmin _____ ## TrustedCertificateQuery.Host (7.1.1): The administrative user login name for the provisioning Web interface. ## ## # The fully qualified host name for the agent manager trusted certification # query service. The name is usually the same as the 5.1.1.2 fully qualified # host name. # # This parameter is used by the tpm711ChangeOtherHost script. #-----TrustedCertificateQuery.Host=risc40pa.rot.it.ibm.com ## 7.1.1 Services configurations #-----## CatalogueService.Host (7.1.1): The fully qualified host name for the ## catalogue service. ## # The name is usually the same as the 5.1.1.2 fully qualified host name # This parameter is used by the tpm711ChangeOtherHost script. CatalogueService.Host=risc40pa.rot.it.ibm.com #-----## dmsHome (7.1.1): The device manager service installation directory. ## # This directory is used to install device manager service code during # the data migration on the 7.1.1 system. # This parameter is used by the tpm711migrate and the wastioadminconfig scripts. #_____ dmsHome=/opt/IBM/DeviceManager #-----## httpServerHome (7.1.1): The HTTP server home directory. ## # This parameter is used by the tpm711ChangeOtherHost script.

```
#-----
httpServerHome=/usr/IBM/HTTPServer
## 7.1.1 Agent Manager configurations
_____
## AgentManagerQuery.Host (7.1.1): The fully qualified host name for the agent
## manager query service.
##
# The name is usually the same as the 5.1.1.2 fully qualified host name
# This parameter is used by the tpm711ChangeOtherHost script.
#-----
AgentManagerOuerv.Host=risc40pa.rot.it.ibm.com
#-----
## AgentQuery.Host (7.1.1): The fully gualified host name for the agent
## query service.
##
# The name is usually the same as the 5.1.1.2 fully qualified host name
# This parameter is used by the tpm711ChangeOtherHost script.
#-----
AgentQuery.Host=risc40pa.rot.it.ibm.com
#-----
## amCellName (7.1.1): The agent manager cell name.
##
# This parameter is used by the tpm711migrate script.
#------
amCellName=risc550aNode01Cell
#------
## amCrlPort (7.1.1): The agent manager public port.
##
# This parameter is used by the tpm711migrate script.
#-----
amCrlPort=9513
#_____
## amHome (7.1.1): The agent manager installation directory.
##
# The specified path will be used to install the agent manager during the
# data migration on the 7.1.1 system.
# This parameter is used by the tpm711migrate script.
#-----
amHome=/opt/IBM/AgentManager
```

```
_____
## amNodeName (7.1.1): The agent manager node name.
##
# This parameter is used by the tpm711migrate script.
#_____
amNodeName=risc550aNode01
#-----
## amPort (7.1.1): The agent manager registration port.
##
# This parameter is used by the tpm711migrate and tpm711ChangeOtherHost
# scripts.
#_____
amPort=9511
   _____
## amProfileName (7.1.1): The WebSphere Application Server agent manager
## profile name.
##
# This parameter is used by the tpm711migrate script.
#-----
amProfileName=casprofile
#-----
## amProfilePort (7.1.1): The agent manager starting port.
##
# This parameter is used by the tpm711migrate script.
#-----
amProfilePort=21000
#-----
## CertManagement.Host (7.1.1): The fully gualified host name for the agent
##
  manager certification manager.
##
# The name is usually the same as the 5.1.1.2 fully qualified host name.
# This parameter is used by the tpm711ChangeOtherHost script.
#-----
CertManagement.Host=risc4Opa.rot.it.ibm.com
           _____
## Registration.Server.Host (7.1.1): The fully qualified host name for the
## agent manager registration server.
##
# The name is usually the same as the 5.1.1.2 fully qualified host name
# This parameter is used by the tpm711ChangeOtherHost script.
#_____
Registration.Server.Host=risc4Opa.rot.it.ibm.com
```
```
#-----
## amUser (7.1.1): The agent manager resource manager user name.
##
# Use the amUser value that is provided unless it was changed during the 7.1.1 installation.
# This parameter is used by the tpm711migrate and tpm711ChangeOtherHost
# scripts.
#_____
amUser=manager
## 7.1.1 Dynamic content delivery configurations
## cdsHome (7.1.1): The dynamic content delivery installation directory.
##
# This directory will be used to install the dynamic content delivery code during
# the data migration on the 7.1.1 system.
# This parameter is used by the tpm711migrate and tpm711ChangeOtherHost
# scripts.
#-----
cdsHome=/opt/IBM/tivoli/CDS
## 7.1.1 Database Administration Server configurations
##------
  _____
## dasUserName (7.1.1): The Database Administration Server user name.
##
# This parameter is used by the tpm711ChangeDBHost script.
# This parameter is only used for DB2 configurations.
# If Oracle is used, remove this parameter.
#-----
dasUserName=dasusr1
## 7.1.1 Database configurations
##------
## dbAdminGroup (7.1.1): The Instance Database administration group.
##
\# DB2 = db2grp1
```

```
# Oracle = oinstall
# This parameter is used by the tpm711migrate script.
#_____
dbAdminGroup=db2iadm1
#_____
## dbAdminUser (7.1.1): The database server instance owner.
##
# DB2 = ctginst1
# Oracle = sys
# This parameter is used by the tpm711restore, tpm711migrate, and
# tpm711ChangeDBHost scripts.
#-----
dbAdminUser=ctginst1
#-----
## dbHome (7.1.1): The local database instance directory, or the database
## client directory if the database is remote.
##
# This parameter is used by the tpm711migrate and tpm711ChangeOtherHost
# scripts.
#-----
dbHome=/home/ctginst1/sqllib
#------
## dbHostname (7.1.1): The fully qualified host name for the database.
##
# This parameter is used by the tpm711migrate and tpm711ChangeOtherHost
# scripts..
#------
dbHostname=risc550a.rot.it.ibm.com
## dbInstanceName (7.1.1): The database instance name, or System ID for Oracle.
##
# This parameter is used by the tpm711restore, tpm711migrate, and
# tpm711ChangeDBHost scripts.
#-----
dbInstanceName=ctginst1
#-----
## dbNewSchemaName (7.1.1): The 7.1.1 database schema name.
##
# This parameter is used by the tpm711restore and tpm711migrate
# scripts.
#_____
dbNewSchemaName=MAXIMO
```

```
_____
## db0ldSchemaName (7.1.1): The 5.1.1.2 database schema name.
##
# This parameter is used by the tpm711restore script.
#_____
db01dSchemaName=DB2INST1
#-----
## dbOSUser (7.1.1): The 7.1.1 database instance owner name.
##
# This parameter is used by the tpm711restore script.
#-----
dbOSUser=ctginst1
#-----
## dbPort (7.1.1): The database host port.
##
# This parameter is used by the tpm711migrate and tpm711ChangeOtherHost
# scripts.
#-----
dbPort=50005
#-----
## orclChangeWordSize (7.1.1): Does the Oracle database need to change from
## 32-bit to 64-bit?
##
# yes = Perform word size change on Oracle database.
# no = Do not perform word size change on Oracle database.
# This parameter is used by the tpm711restore script.
# This parameter is only used for Oracle configurations.
# If DB2 is used, remove this parameter.
#-----
                           ------
#orclChangeWordSize=[no]
## 7.1.1 Deployment manager configurations
##------
  ## dmgrSoapPort (7.1.1): The deployment manager SOAP port.
##
# This parameter is used by the tpm711ChangeOtherHost.
#-----
dmgrSoapPort=8879
```

Considering that we installed all the Middleware components on a single machine, these database server and directory server parameters have been configured:

- dbIsRemote=no because we are using a local database server
- IdapUseNew=new because we installed a new directory server during the Middleware installation

Important: The default installation path for the Tivoli Provisioning Manager changed the case of the "ibm" subdirectory between 5.1.1.2 and 7.1.1 versions.

Tivoli Provisioning Manager Version 5.1.1.2 default installation path is:

/opt/ibm/tivoli/tpm

Tivoli Provisioning Manager Version 7.1.1 default installation path is:

/opt/IBM/tivoli/tpm

To avoid problems during the migration scripts execution, make sure the property file contains the right case for the paths of these parameters:

- outputDir=/opt/ibm/tivoli/tpm/migration/backup used by the Tivoli Provisioning Manager Version 5.1.1.2 server
- backupDir=/opt/IBM/tivoli/tpm/migration/backup used by the Tivoli Provisioning Manager Version 7.1.1 server

17.8 Migrating Tivoli Provisioning Manager

Now that the property file has been completed with the information required by the migration process, you can perform the migration tasks on the provisioning servers.

17.8.1 Migration tasks for the Tivoli Provisioning Manager Version 5.1.1.2 system

The following tasks need to be completed to back up the 5.1.1.2 provisioning server:

• Cancelling tasks and activity plans.

Any running task must be cancelled before starting the backup process to avoid database deadlocks and other issues.

- Stopping the provisioning server.
- Backing up a remote database server.

This task was not needed in our environment because we are using a local database server on both the 5.1.1.2 and the 7.1.1 provisioning servers.

► Backing up Tivoli Provisioning Manager Version 5.1.1.2.

Details about this task are provided next.

Backing up Tivoli Provisioning Manager Version 5.1.1.2

To back up the Tivoli Provisioning Manager Version 5.1.1.2 server, use the tpm5112backup.sh script as detailed in Example 17-11.

Important: If you configured the tpmmigrate_unix.properties file to delete the DB2 audit table entries by specifying the parameter removeAuditData=yes, and you see that the audit tables were not deleted but the tpm5112backup.sh script completed successfully, follow the steps outlined here:

- 1. If tpm5112backup.sh has run successfully before, delete \$TIO_LOGS/migration/tpm5112backup_status.log file.
- 2. Empty content of directory specified in backupDir in tpmmigrate_unix.properties file.
- 3. Replace **\$TI0_HOME/migration/scripts/tpm5112backup.sh** with the new version provided with this Redbooks publication. You can download this script using the instructions provided in Appendix D, "Additional material" on page 711. You can also see the source of this script in Example C-1 on page 700.
- 4. Change the script permission to 775 and set the ownership to tioadmin by running: chown tioadmin.tioadmin tpm5112backup.sh chmod 775 tpm5112backup.sh
- 5. Re-run tpm5112backup.sh.

This procedure will create a new backup set and delete the DB2 audit tables.

Example 17-11 tpm5112backup.sh script execution

Login as root into the Tivoli Provisioning Manager Version 5.1.1.2 system. From the *\$TIO HOME*/migration path set the permissions of these directories:

[tioadmin@risc40pa][/opt/ibm/tivoli/tpm/migration]> chmod -R 775 \$TI0_HOME/migration/scripts/*
[tioadmin@risc40pa][/opt/ibm/tivoli/tpm/migration]> chmod -R 775 \$TI0_HOME/migration/scripts/.*

Invoke the script by running this command:

[root@risc40pa][/opt/ibm/tivoli/tpm/migration/scripts]> tpm5112backup.sh

The output will look like:

--- [tpm5112backup.sh:PRE_CHECK_ENV] begins at Tue Aug 4 16:57:58 DFT 2009 ---

----- RECOMMENDATION -----

Before continuing, ensure that you have read the migration documentation and have completed all of the prerequisite steps in the checklist for this script. Are you sure you want to continue? To continue.....enter 1 To exit.....enter 2 --- [tpm5112backup.sh:PRE CHECK ENV] ended successfully at Tue Aug 4 16:57:59 DFT 2009 ------ [tpm5112backup.sh:VALIDATE INPUT] begins at Tue Aug 4 16:57:59 DFT 2009 ---The following values (with passwords masked) have been retrieved from /opt/ibm/tivoli/tpm/migration/scripts/tpmmigrate unix.properties file or loaded automatically from other configurations: -removeAuditData: yes -outputDir: /opt/ibm/tivoli/tpm/migration/backup -baseDN: ou=SWG,o=IBM,c=US -userBaseDN: ou=users.ou=SWG.o=IBM.c=US -groupBaseDN: ou=groups,ou=SWG,o=IBM,c=US -ldapType: ITDS -ldapUseNew: new -dbIsRemote: no -orclOSUser: -zipBackupFiles: no -wasUser: wasadmin -dbPass: {Variable value not shown here} -orclSysPass: {Variable value not shown here} Are you sure all the input are correct? Yes, they are correct.....enter 1 No, updates are needed.....enter 2 --- [tpm5112backup.sh:VALIDATE INPUT] ended successfully at Tue Aug 4 16:58:16 DFT 2009 ------ [tpm5112backup.sh:INITIAL CONFIG] begins at Tue Aug 4 16:58:16 DFT 2009 ------ [tpm5112backup.sh:INITIAL CONFIG] ended successfully at Tue Aug 4 16:58:26 DFT 2009 ---

```
--- [tpm5112backup.sh:CREATE LDIF] begins at Tue Aug 4 16:58:26 DFT 2009 ---
2009-08-04 16:58:27,199 INFO Migration home: /opt/ibm/tivoli/tpm
2009-08-04 16:58:27,203 INFO Migration config: /opt/ibm/tivoli/tpm/config
2009-08-04 16:58:27,208 INFO User factory file: /opt/ibm/tivoli/tpm/config/user-factory.xml
2009-08-04 16:58:27,462 INFO Migration from LDAP to LDAP begins.
2009-08-04 16:58:27,464 INFO Parameters passed to 1dap migration ...
2009-08-04 16:58:27,465 INFO -m: new
2009-08-04 16:58:27,481 INF0 -e: /opt/ibm/tivoli/tpm
2009-08-04 16:58:27,481 INFO -o: /opt/ibm/tivoli/tpm/migration/backup/ldap
2009-08-04 16:58:27,482 INFO Migration home: /opt/ibm/tivoli/tpm
2009-08-04 16:58:27,483 INFO Migration config: /opt/ibm/tivoli/tpm/config
2009-08-04 16:58:27,484 INFO User factory file: /opt/ibm/tivoli/tpm/config/user-factory.xml
2009-08-04 16:58:27,534 INFO Factory :
com.ibm.tivoli.tpm.userAndRoleFactory.IDSReadOnlyUserAndDBGroupFactory
2009-08-04 16:58:27,536 INFO Migrating to new ITDS.
2009-08-04 16:58:32,865 INFO -g: ou=groups,ou=SWG,o=IBM,c=US
2009-08-04 16:58:32,866 INF0 -u: ou=users,ou=SWG,o=IBM,c=US
2009-08-04 16:58:32,867 INFO -w: wasadmin
2009-08-04 16:58:34,325 INFO Concatenated filter for searching the rest of use in ldap:
((&(cn=tioappadmin)(objectclass=organizationalPerson))(&(cn=
admin)(objectclass=organizationalPerson)))
2009-08-04 16:58:34,334 INFO Concatenated filter for searching the rest of use in ldap:
((&(cn=tioappadmin)(objectclass=organizationalPerson))(&(cn=
admin)(objectclass=organizationalPerson)))
2009-08-04 16:58:34,338 INFO Concatenated filter for searching the rest of use in ldap:
(|(&(cn=tioappadmin)(objectclass=organizationalPerson))(&(cn=
admin)(objectclass=organizationalPerson)))
2009-08-04 16:58:34,341 WARN User, admin, cannot be found in ldap. This user will not be
processed.
2009-08-04 16:58:34,346 INFO Generating ldif file,
/opt/ibm/tivoli/tpm/migration/backup/ldap/LdapBackupNew.ldif.
2009-08-04 16:58:34,366 INFO Migrating users ...
2009-08-04 16:58:34,367 INFO Creating user, cn=tioappadmin,ou=users,ou=SWG,o=IBM,c=US
2009-08-04 16:58:34,371 INFO Generating ldif file,
/opt/ibm/tivoli/tpm/migration/backup/ldap/creation LdapBackupNew.ldif.
--- [tpm5112backup.sh:CREATE LDIF] ended successfully at Tue Aug 4 16:58:34 DFT 2009 ---
--- [tpm5112backup.sh:BACKUP CAS] begins at Tue Aug 4 16:58:34 DFT 2009 ---
--- [tpm5112backup.sh:BACKUP CAS] ended successfully at Tue Aug 4 16:58:50 DFT 2009 ---
--- [tpm5112backup.sh:REMOVE AUDIT] begins at Tue Aug 4 16:58:50 DFT 2009 ---
--- [tpm5112backup.sh:REMOVE AUDIT] ended successfully at Tue Aug 4 16:58:53 DFT 2009 ---
--- [tpm5112backup.sh:BACKUP DB] begins at Tue Aug 4 16:58:53 DFT 2009 ---
Calling /opt/ibm/tivoli/tpm/migration/scripts/.script/db2Backup.sh TC db2inst1
/opt/ibm/tivoli/tpm/migration/backup/database ...
Ouiesce database ...
db2 connect TO TC USER db2inst1
```

Database Connection Information

```
Database server = DB2/6000 8.2.4
SQL authorization ID = DB2INST1
Local database alias = TC
```

DB20000I The QUIESCE DATABASE command completed successfully. DB20000I The SQL command completed successfully. Database backup directory: /opt/ibm/tivoli/tpm/migration/backup/database Backing up database TC ... Unquiesce database ... db2 connect TO TC USER db2inst1

Database Connection Information

Database server = DB2/6000 8.2.4 SQL authorization ID = DB2INST1 Local database alias = TC

DB20000I The UNQUIESCE DATABASE command completed successfully. DB20000I The SQL command completed successfully. --- [tpm5112backup.sh:BACKUP DB] ended successfully at Tue Aug 4 16:59:35 DFT 2009 ---

--- [tpm5112backup.sh:COLLECT_FILES] begins at Tue Aug 4 16:59:35 DFT 2009 ---Backup process completed.

--- [tpm5112backup.sh:COLLECT_FILES] ended successfully at Tue Aug 4 16:59:35 DFT 2009 ---

**** End of [tpm5112backup.sh] ***

VALIDATION

To validate that the backup was successful, check the *\$TIO LOGS*/migration/tpm5112backup status.log file:

[root@risc40pa][/opt/ibm/tivoli/tpm]> cat \$TI0_LOGS/migration/tpm5112backup_status.log
PRE_CHECK_ENV|DONE
VALIDATE_INPUT|DONE
INITIAL_CONFIG|DONE
CREATE_LDIF|DONE
BACKUP_CAS|DONE
REMOVE_AUDIT|DONE
BACKUP_DB|DONE
COLLECT_FILES|DONE

All the steps are marked DONE as per a succesfull execution.

You are done with the Tivoli Provisioning Manager Version 5.1.1.2 migration tasks and you are now ready to continue with the Tivoli Provisioning Manager Version 7.1.1 migration tasks.

17.8.2 Migration tasks for the Tivoli Provisioning Manager Version 7.1.1 system

The following tasks needs to be completed to perform the migration to the 7.1.1 provisioning server:

- ► Starting the middleware
- Accessing the migration files
- Creating the DB2 database paths
- Restoring the remote database server
- Restoring and migrating data to 7.1.1

These tasks are detailed next. For the procedure to start the middleware, refer to Example 17-8 on page 568.

Accessing the migration files

This task consist in copying the data backed up on the 5.1.1.2 provisioning server to the 7.1.1 provisioning server.

Example 17-12 details the steps executed.

Example 17-12 Accessing the migration files

The data backed up on the 5.1.1.2 provisiong server have been stored in the location of the **outputDir** parameter specified in the tpmmigrate_unix.properties file. Copy them in a location accessible by the 7.1.1 provisioning server.

To accomplish this we created a tar file contained all the backed up data.

[root@risc40pa][/opt/ibm/tivoli/tpm/migration/backup]> ls -latr total 8 drwxrwxr-x 9 tioadmin tioadmin 256 Aug 04 16:35 .. drwxrwxrwx 7 tioadmin tioadmin 256 Aug 04 16:57 .

drwxrwxrwx2 tioadmin tioadmin256 Aug 04 16:58 ldapdrwxrwxrwx2 tioadmin tioadmin256 Aug 04 16:58 tcadrwxrwxrwx2 tioadmin tioadmin256 Aug 04 16:58 databasedrwxrwxrwx2 tioadmin tioadmin256 Aug 04 16:59 guiddrwxrwxrwx3 tioadmin tioadmin4096 Aug 04 16:59 config

[root@risc40pa][/opt/ibm/tivoli/tpm/migration/backup]> tar cvf
5112backup.tar ./*

The 5112backup.tar file has then been transfered to the 7.1.1 provisiong server and its content expanded in the location of the **backupDir** parameter specified in the tpmmigrate_unix.properties file.

The property file must then be copied on the 7.1.1 system in the *\$TIO_HOME/migration*

[root@risc550a][/opt/IBM/tivoli/tpm/migration/scripts]> ls -la
tpmmigrate_unix.properties
-rwxrwxr-x 1 tioadmin tioadmin 25420 Aug 04 19:58
tpmmigrate unix.properties

Creating the DB2 database paths

When you restore the 5.1.1.2 database backup, the same table space container paths must exist on the 7.1.1 database server. Check the container paths in the database backup and create any required paths on the 7.1.1 database server.

Follow Example 17-13 to check the container paths.

Example 17-13 Checking container paths

You can check the tablespace container paths by running the **db2ckbkp** command that inspects the content of a DB2 database backup file. In the command output, check all the table spaces. For each table space, look for the name under **Container CB**. If the **Container CB** name matches the table space name, the table space will be created in the default location; recreating the paths is not required on the 7.1.1 database server.

If there is a specific path associated with the container, create the corresponding path on the 7.1.1 database server.

A sample output is shown below for the CDS_TS tablespace.

[root@risc40pa][/opt/ibm/tivoli/tpm/migration/backup/database]>
db2ckbkp -T TC.0.db2inst1.NODE0000.CATN0000.20090804165857.001

... OUTPUT TRUNCATED ...

CDS TS

ID: 17 flags: 2102 flags2: 0

```
extent size: 64
                prefetch size: 32
                      version: 21
                      flavour: 4
                        state: 0
         statechangeobjectid: 0
           statechangepoolid: 0
                      LifeLSN: 0000 153D 83FA
               LoadPendingLSN: 0000 0000 0000
              LoadRecoveryLSN: 0000 0000 0000
                     BeginLSN: 0000 0000 0000
                       EndLSN: 0000 0000 0000
                   StordefLSN: 0000 153D 8F94
             Full Backup LSN: 0000 0000 0000
             Last Backup LSN: 0000 0000 0000
            Full Backup Time: 00000000 = "19700101010000"
            Last Backup Time: 00000000 = "19700101010000"
                   TotalPages: 32768
                 UseablePages: 32704
                  reorgPoolID: 0
                   reorgObjID: 0
               poolReorgCount: 0
              # of containers: 1
                current group: 0
                    cont csum: 389522152
         current map entries: 1
                   page size: 32768
                    map csum: 4294967294
         tsp rfwd encountered: 16
                Container CB
                                 Type: 6
                           TotalPages: 32768
                          UsablePages: 32704
                   # of OS rsvd bytes: 512
                        Page 0 offset: 2097152
                           Tag offset: 512
                        Extent offset: 0
                                 Name: cds ts.dat
... OUTPUT TRUNCATED ...
```

As you can see the **Container CB Name** shows cds_ts.dat without any path, therefore no actions are required on the 7.1.1 provisioning server.

Restoring the remote database server

This step was not required for the environment used for this Redbooks publication because we used a local database server.

In case you are using a remote database server for the 7.1.1 provisioning server, you must restore the 5.1.1.2 backup image to that server.

Restoring and migrating data to 7.1.1

To restore and migrate the Tivoli Provisioning Manager Version 5.1.1.2 data to the Tivoli Provisioning Manager Version 7.1.1 server, use the tpm711restore.sh and tpm711migrate.sh scripts as detailed respectively in Example 17-14 and Example 17-15.

Example 17-14 tpm711restore.sh script execution

Before running the tpm711restore.sh script, verify the these parameters are correctly set for the 7.1.1 provisioning server:

```
[root@risc550a][/opt/IBM/tivoli/tpm/migration/scripts]> grep dbIsRemote
tpmmigrate_unix.properties
## dbIsRemote (5.1.1.2 and 7.1.1): Is database remote or local?
dbIsRemote=no
[root@risc550a][/opt/IBM/tivoli/tpm/migration/scripts]> grep dbHostname
tpmmigrate_unix.properties
## dbHostname (7.1.1): The fully qualified host name for the database.
dbHostname=risc550a.rot.it.ibm.com
[root@risc550a][/opt/IBM/tivoli/tpm/migration/scripts]> grep wasUser tpmmigrate_unix.properties
## wasUser (5.1.1.2 and 7.1.1): WebSphere deployment manager administrator user
wasUser=wasadmin
```

Invoke the script by running this command:

[root@risc550a][/opt/IBM/tivoli/tpm/migration/scripts]> tpm711restore.sh

The output will look like:

--- [tpm711restore.sh:PRE_CHECK_ENV] begins at Tue Aug 4 21:40:44 GMT+02:00 2009 ---

------ WARNING ------

This script may perform irreversible changes to your environment.

Before continuing, ensure that you have read the migration documentation and have completed all of the prerequisite steps in the checklist for this script. Are you sure you want to continue? To continue.....enter 1 To exit.....enter 2 Enter 1 or 2 : 1 _____ Database information retrieval completed... dcm.xml validation completed... --- [tpm711restore.sh:PRE CHECK ENV] ended successfully at Tue Aug 4 21:40:51 GMT+02:00 2009 ------ [tpm711restore.sh:VALIDATE INPUT] begins at Tue Aug 4 21:40:51 GMT+02:00 2009 ---Enter the password for the database administrator user 'ctginstl': Re-enter the password to confirm: The following values (with passwords masked) have been retrieved from /opt/IBM/tivoli/tpm/migration/scripts/tpmmigrate unix.properties file or loaded automatically from other configurations: -dbAdminUser: ctginst1 -backupDir: /opt/IBM/tivoli/tpm/migration/backup -db01dSchemaName: DB2INST1 -dbNewSchemaName: MAXIMO -dbInstanceName: ctginst1 -dbIsRemote: no -dbAdminPass: {Variable value not shown here} -orclChangeWordSize: _____ Are you sure all the input are correct? Yes, they are correct.....enter 1 No, updates are needed.....enter 2 Enter 1 or 2 : 1 --- [tpm711restore.sh:VALIDATE INPUT] ended successfully at Tue Aug 4 21:41:05 GMT+02:00 2009 ---

```
--- [tpm711restore.sh:INITIAL CONFIG] begins at Tue Aug 4 21:41:05 GMT+02:00 2009 ---
--- [tpm711restore.sh:INITIAL_CONFIG] ended successfully at Tue Aug 4 21:41:11 GMT+02:00 2009
---
--- [tpm711restore.sh:DROP AND RESTORE DB] begins at Tue Aug 4 21:41:11 GMT+02:00 2009 ---
DB20000I The FORCE APPLICATION command completed successfully.
DB21024I This command is asynchronous and may not be effective immediately.
DB20000I The DROP DATABASE command completed successfully.
Calling /opt/IBM/tivoli/tpm/migration/scripts/.script/db2Restore.sh TC MAXDB71 ctginst1
/home/ctginst1/migratedb DB2INST1 MAXIMO ...
Ouiesce database ...
db2 connect TO MAXDB71 USER ctginst1
  Database Connection Information
                      = DB2/AIX64 9.5.3
Database server
SOL authorization ID = CTGINST1
Local database alias = MAXDB71
DB20000I The QUIESCE DATABASE command completed successfully.
DB20000I The SOL command completed successfully.
Restoring database TC to MAXDB71...
database backup directory: /home/ctginst1/migratedb
db2 connect TO MAXDB71 USER ctginst1
  Database Connection Information
Database server
                       = DB2/AIX64 9.5.3
SQL authorization ID = CTGINST1
Local database alias = MAXDB71
Renaming database schema...
Copying database schema...
DB200001 The SQL command completed successfully.
DB20000I The SQL command completed successfully.
 Return Status = 0
Dropping original database schema...
 Return Status = 0
Cleanup ...
DB20000I The SQL command completed successfully.
```

```
DB20000I The SQL command completed successfully.
Unquiesce database ...
DB20000I The UNQUIESCE DATABASE command completed successfully.
DB20000I The SQL command completed successfully.
Λ
--- [tpm711restore.sh:DROP AND RESTORE DB] ended successfully at Tue Aug 4 22:04:04 GMT+02:00
2009 ---
--- [tpm711restore.sh:SET GUID KEY] begins at Tue Aug 4 22:04:04 GMT+02:00 2009 ---
Tivoli GUID utility - Version 1, Release 3, Level 1.
(C) Copyright IBM Corporation 2002, 2005 All Rights Reserved.
Guid:b2.33.f7.5a.6c.ad.11.de.a0.ce.08.63.09.a8.2f.0c
--- [tpm711restore.sh:SET GUID KEY] ended successfully at Tue Aug 4 22:04:04 GMT+02:00 2009 ---
--- [tpm711restore.sh:REPLACE DB KEY] begins at Tue Aug 4 22:04:04 GMT+02:00 2009 ---
--- [tpm711restore.sh:REPLACE DB KEY] ended successfully at Tue Aug 4 22:04:04 GMT+02:00 2009
*** End of [ tpm711restore.sh ] ***
*** For references on most messages displayed on the screen, refer to
/usr/ibm/tivoli/common/COP/logs/migration/tpm711restore.log file. ***
VALIDATION
To validate that the backup was successful, check the
$TIO LOGS/migration/tpm711restore status.log file:
```

[root@risc550a] [/opt/IBM/tivoli/tpm/migration/scripts]> cat
\$TIO_LOGS/migration/tpm711restore_status.log
PRE_CHECK_ENV | DONE
VALIDATE_INPUT | DONE
INITIAL_CONFIG | DONE
DROP_AND_RESTORE_DB | DONE
SET_GUID_KEY | DONE
REPLACE_DB_KEY | DONE

Before running the next script, tpm711migrate.sh, make sure that you correctly remember the passwords in Table 17-4, because you will be prompted for them at the beginning of the script execution.

Password	Description	
Database administrator user	The password for the database administrator user 'ctginst1'	
Database user	The password for the database user 'maximo'	
Agent manager	The agent manager password that was used in 5.1.1.2	
Agent registration	The agent manager registration password that was used in 5.1.1.2	
Agent manager resource manager	The agent manager resource manager password that was used in 5.1.1.2. Unless changed after the installation, the default password created by the installer in 5.1.1.2 is password.	
WebSphere Application Server	The password for WebSphere Application Server administrator 'wasadmin' in 7.1.1	
Tivoli Provisioning Manager Keystore	The keystore password that was used in 5.1.1.2	

Table 17-4 Passwords required for the tpm711migrate.sh script

Important: It is very important to correctly provide the foregoing passwords to avoid installation errors.

The migration scripts perform several steps and both use passwords set on the 5.1.1.2 and 7.1.1 provisioning server at installation time.

The WebSphere Application Server administrator password is used to create the Agent Manager and the casprofile. The script prompts you for the wasadmin password, and checks if the password is the same as used for Tivoli Provisioning Manager Version 7.1.1 installation. If the password matches, it uses that password to create casprofile.

Usually you do not have to deal with the casprofile password, but if you want to change it, you can do that after the migration is done. See 17.8.3, "Changing the WebSphere Application Server casprofile profile password" on page 616 for details about how to do this.

Example 17-15 details the execution of the tpm711migrate.sh script.

This is the script responsible for actually perform the data migration from 5.1.1.2 to 7.1.1. During this script execution, the core components pieces that we did not select at install time will now be installed:

- Agent Manager
- Tivoli Provisioning Manager for Dynamic Content Delivery
- Device Manager Service

Example 17-15 tpm711migrate.sh script execution

Invoke the script by running this command:

[root@risc550a][/opt/IBM/tivoli/tpm/migration/scripts]> tpm711migrate.sh

The output will look like the following. We truncated some parts in the output to make it shorter:

--- [tpm711migrate.sh:PRE CHECK ENV] begins at Tue Aug 4 22:37:28 GMT+02:00 2009 ---

----- WARNING -----

This script may perform irreversible changes to your environment. Before continuing, ensure that you have read the migration documentation and have completed all of the prerequisite steps in the checklist for this script.

Are you sure you want to continue?

To continue.....enter 1 To exit.....enter 2

Build version file check completed...

Version number check completed...

--- [tpm711migrate.sh:PRE_CHECK_ENV] ended successfully at Tue Aug 4 22:37:35 GMT+02:00 2009

--- [tpm711migrate.sh:VALIDATE_INPUT] begins at Tue Aug 4 22:37:35 GMT+02:00 2009 ---

Database information retrieval completed...

The following values (with passwords masked) have been retrieved from /opt/IBM/tivoli/tpm/migration/scripts/tpmmigrate unix.properties file or loaded automatically from other configurations: -dbAdminUser: ctginst1 -dbPort: 50005 -dbHome: /home/ctginst1/sqllib -dbAdminGroup: db2iadm1 -dbIsRemote: no -dbInstanceName: ctginst1 -dbNewSchemaName: MAXIMO -amUser: manager -wasUser: wasadmin -amProfileName: casprofile -amProfilePort: 21000 -sdiClientSSLPort: 9046 -sdiServerSSLPort: 9045 -amPort: 9511 -amCrlPort: 9513 -amHome: /opt/IBM/AgentManager -amNodeName: risc550aNode01 -amCellName: risc550aNode01Cell -cdsHome: /opt/IBM/tivoli/CDS -dmsHome: /opt/IBM/DeviceManager -fq711HostName: risc550a.rot.it.ibm.com -fq5112HostName: risc40pa.rot.it.ibm.com -backupDir: /opt/IBM/tivoli/tpm/migration/backup -imagesDir: /tpm images/U2823 -tpmHttpPort: 9080 -tpmHttpsPort: 9443 -tpmUiUser: maxadmin -midDbBackup: no -wasNode: ctgNode01 -dbHostname: risc550a.rot.it.ibm.com -dbAdminPass: {Variable value not shown here} -dbPass: {Variable value not shown here} -amPass: {Variable value not shown here} -amRegPass: {Variable value not shown here} -amToolkitPass: {Variable value not shown here} -amResMgrPass: {Variable value not shown here} -amKsPass: {Variable value not shown here} -amTsPass: {Variable value not shown here} -keyStorePass: {Variable value not shown here} -wasPass: {Variable value not shown here} -orclOSUser: -ldapType: ITDS

Are you sure all the input are correct? Yes, they are correct.....enter 1 No, updates are needed.....enter 2 _____ --- [tpm711migrate.sh:VALIDATE INPUT] ended successfully at Tue Aug 4 22:38:31 GMT+02:00 2009 ------ [tpm711migrate.sh:MIGRATE DATA] begins at Tue Aug 4 22:38:31 GMT+02:00 2009 ---Update database configuration parameters, migrate buffer pools and create table spaces. Database is DB2JCC Performing database configuration. Database name MAXDB71 Connecting to MAXDB71 user ctginst1 Database Connection Information Database server = DB2/AIX64 9.5.3SOL authorization ID = CTGINST1 Local database alias = MAXDB71 Updating the db cfg for MAXDB71 using app ctl heap sz 8192 DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. SOL1363W One or more of the parameters submitted for immediate modification were not changed dynamically. For these configuration parameters, all applications must disconnect from this database before the changes become effective. Updating the db cfg for MAXDB71 using applheapsz 8192 DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. Updating the db cfg for MAXDB71 using catalogcache sz 800 DB200001 The UPDATE DATABASE CONFIGURATION command completed successfully. Updating the db cfg for MAXDB71 using database memory AUTOMATIC DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. Updating the db cfg for MAXDB71 using locklist AUTOMATIC SQL5146W "MAXLOCKS" must be set to "AUTOMATIC" when "LOCKLIST" is "AUTOMATIC". "MAXLOCKS" has been set to "AUTOMATIC". Updating the db cfg for MAXDB71 using logfilsiz 4096 DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. SOL1363W One or more of the parameters submitted for immediate modification were not changed dynamically. For these configuration parameters, all applications must disconnect from this database before the changes become effective. Updating the db cfg for MAXDB71 using maxappls AUTOMATIC DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. Updating the db cfg for MAXDB71 using maxlocks AUTOMATIC DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully.

Updating the db cfg for MAXDB71 using pckcachesz AUTOMATIC DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. Updating the db cfg for MAXDB71 using self tuning mem ON DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. Updating the db cfg for MAXDB71 using sheapthres shr AUTOMATIC SOL5146W "SORTHEAP" must be set to "AUTOMATIC" when "SHEAPTHRES SHR" is "AUTOMATIC". "SORTHEAP" has been set to "AUTOMATIC". Updating the db cfg for MAXDB71 using softmax 520 DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. SQL1363W One or more of the parameters submitted for immediate modification were not changed dynamically. For these configuration parameters, all applications must disconnect from this database before the changes become effective. Updating the db cfg for MAXDB71 using sortheap AUTOMATIC DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. Updating the db cfg for MAXDB71 using stmtheap 4096 DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. Altering the db bufferpool IBMDEFAULTBP immediate size 1000 DB20000I The SQL command completed successfully. Reseting database connection... DB20000I The SQL command completed successfully. Database user name maximo connect to MAXDB71 user ctginst1

Database Connection Information

Database server = DB2/AIX64 9.5.3 SQL authorization ID = CTGINST1 Local database alias = MAXDB71

Migrate buffer pool and create tablespaces... ALTER BUFFERPOOL IBM8K IMMEDIATE SIZE 1000 AUTOMATIC DB20000I The SQL command completed successfully.

ALTER BUFFERPOOL IBM16K IMMEDIATE SIZE 1000 AUTOMATIC DB200001 The SQL command completed successfully.

ALTER BUFFERPOOL IBM32K IMMEDIATE SIZE 1000 AUTOMATIC DB200001 The SQL command completed successfully.

ALTER BUFFERPOOL CDS_BP IMMEDIATE SIZE 1000 AUTOMATIC DB200001 The SQL command completed successfully.

CREATE REGULAR TABLESPACE IBM32KSPACE PAGESIZE 32K MANAGED BY SYSTEM USING ('IBM32KSPACE') BUFFERPOOL IBM32K DROPPED TABLE RECOVERY OFF DB20000I The SQL command completed successfully.

Granting use of tablespace IBM32KSPACE to user maximo DB20000I The SQL command completed successfully.

ALTER BUFFERPOOL CDS_BP IMMEDIATE SIZE 1000 AUTOMATIC DB20000I The SQL command completed successfully.

CREATE BUFFERPOOL IBM4K SIZE 1000 AUTOMATIC PAGESIZE 4K DB20000I The SQL command completed successfully.

CREATE REGULAR TABLESPACE IBM4KSPACE PAGESIZE 4K MANAGED BY SYSTEM USING ('IBM4KSPACE') BUFFERPOOL IBM4K DROPPED TABLE RECOVERY OFF DB20000I The SQL command completed successfully.

CREATE TEMPORARY TABLESPACE IBM4KTEMPSPACE PAGESIZE 4K MANAGED BY SYSTEM USING ('IBM4KTEMPSPACE') BUFFERPOOL IBM4K DROPPED TABLE RECOVERY OFF DB20000I The SQL command completed successfully.

Granting use of tablespace IBM4KSPACE to user maximo DB20000I The SQL command completed successfully. Granting DBADM to user maximo DB20000I The SQL command completed successfully. Granting select on SYSIBM.SYSDUMMY1 to user maximo DB20000I The SQL command completed successfully. Reset database connection DB20000I The SQL command completed successfully. 2009-08-04 22:39:16.044 INFO COPUTL016I Data migration beginning. 2009-08-04 22:39:16,047 INFO COPUTL017I Processing pre-migration ... 2009-08-04 22:39:16,073 INFO COPUTL023E Processing Migration Step: generate drop foreign keys SOL 2009-08-04 22:39:16,080 INFO COPUTL024I Performing Java command: com.ibm.tivoli.orchestrator.datamigration.command.GenerateKeysConstraintSQL 2009-08-04 22:39:19,795 INFO COPUTL023E Processing Migration Step: generate script to drop check constraint 2009-08-04 22:39:19,800 INFO COPUTL024I Performing Java command: com.ibm.tivoli.orchestrator.datamigration.command.GenerateDropCheckConstraintScript 2009-08-04 22:39:19,862 INFO COPUTL023E Processing Migration Step: generate script to drop check constraint 2009-08-04 22:39:19,866 INFO COPUTL024I Performing Java command: com.ibm.tivoli.orchestrator.datamigration.command.GenerateDropUniqueConstraintScript 2009-08-04 22:39:19,917 INFO COPUTL018I Processing data migration ... 2009-08-04 22:39:19,921 INFO COPUTL023E Processing Migration Step: drop tio constraints

```
... OUTPUT TRUNCATED ...
```

At this point these SQL are executed:

```
sql/db2/drop.referential.all.tables.sql
sql/drop.referential.all.tables.sql
sql/db2/dropFKFromExtentionTable.sql
sql/dropFKFromExtentionTable.sql
sql/db2/dropAllPrimaryKeys.5112to711.sql
sql/db2/dropTableUniqueConstraint.sql
```

```
sql/dropTableUniqueConstraint.sql
sql/db2/dropAllIndexes.5112to711.sql
sql/db2/dropViews.5112to711.sql
sql/db2/dropSoftwareFunctions.sql
sql/dropSoftwareFunctions.sql
sql/db2/dropTriggers.5112to711.sql
sql/db2/dropTableCheckConstraint.sql
sql/dropTableCheckConstraint.sql
sql/db2/createTables.5112to711.sql
sql/db2/add.langcode.enum.tables.5112to711.sql
sql/db2/migrateColumnChanges.5112to711.sql
sql/db2/migrateColumnChangesNotCoveredByGeneratedScript.5112to711.sql
sql/db2/migrateEnumValues.5112to711.sql
sql/migrateEnumValues.5112to711.sql
sql/db2/migrateResourceRequestLockKey.sql
sql/migrateResourceRequestLockKey.sql
sql/db2/migrateSequences.5112to711.sql
sql/migrateSequences.5112to711.sql
sql/db2/migrateTriggers.5112to711.sql
sql/db2/migrateDefaultValues.5112to711.sql
sql/migrateDefaultValues.5112to711.sql
sql/db2/migrateData.5112to711.sql
sql/migrateData.5112to711.sql
sql/db2/addAllIndexes.5112to711.sql
sql/addAllIndexes.5112to711.sql
sql/db2/addAllPrimaryKeys.5112to711.sql
sql/addAllPrimaryKeys.5112to711.sql
sql/db2/addAllForeignKeys.5112to711.sql
sql/addAllForeignKeys.5112to711.sql
sql/db2/restoreFKFromExtentionTable.sql
sql/restoreFKFromExtentionTable.sql
sql/db2/migrateUniqueConstraint.5112to711.sql
sql/migrateUniqueConstraint.5112to711.sql
sql/db2/migrateCheckConstraint.5112to711.sql
sql/migrateCheckConstraint.5112to711.sql
sql/db2/reportViews.sql
sql/db2/dropTables.5112to711.sql
sql/dropTables.5112to711.sql
sql/db2/dropColumns.5112to711.sql
sql/db2/update.activityplantype.sql
sql/update.activityplantype.sql
sql/db2/update.activityPlanEditorActivityPlanCreatedByUser.sql
sql/update.activityPlanEditorActivityPlanCreatedByUser.sql
sql/db2/update.allTasksUseridsToCapital.sql
sql/db2/migrateTCA.5112to711.sql
sql/migrateTCA.5112to711.sql
sql/db2/migrate eDMSLWI.5112to711.sql
sql/migrate eDMSLWI.5112to711.sql
```

The log then continues with:

2009-08-04 22:45:30,917 INFO COPUTL020I Data migration was completed successfully.

And these other actions are perfomed:

Uninstalling obsolete automation packages Uninstalling obsolete automation package jes-subagent Uninstalling obsolete automation package rembo Loading Automation Packages Populating data center model with software signatures user.dir=[/home/tioadmin] Populating data center model with custom software signatures user.dir=[/home/tioadmin] Updates the statistics that are used by the DB2 optimizer.

The log then continues with:

--- [tpm711migrate.sh:MIGRATE DATA] ended successfully at Tue Aug 4 23:11:51 GMT+02:00 2009 ---

--- [tpm711migrate.sh:INSTALL CAS] begins at Tue Aug 4 23:11:51 GMT+02:00 2009 ---Creating CAS profile in WAS INSTCONFSUCCESS: Success: Profile casprofile now exists. Please consult /usr/IBM/WebSphere/AppServer/profiles/casprofile/logs/AboutThisProfile.txt for more information about this profile. WAS profile casprofile was created successfully - exit 0 Updating Agent Manager response file Install new agent manager Update /opt/IBM/tivoli/tpm/tools/setupCmdLine.sh Running migration closure tool CTGEM2453I Migration or merging closure process status report. CTGEM2451I The current runtime mode is the following: migration CTGEM2452I The number of common agents that are not configured: 4 CTGEM2456I Closing the migration or merging mode. WASX7357I: By request, this scripting client is not connected to any server process. Certain configuration and application operations will be availabl e in local mode. WASX73031: The following options are passed to the scripting environment and are available as arguments that are stored in the argy variable: "[-actio n, removeHTTPTransports, -propfile, /tmp/script3933585904281614609.tmp, -logDir, ../logs]" Aug 4, 2009 11:25:20 PM com.ibm.tivoli.cas.manager.ismp.utils.LogUtilsIcl EPMAppServer.jacl.main INFO: CTGEM2100I The WebSphere configuration script EPMAppServer.jacl started. The action taken is removeHTTPTransports. Aug 4, 2009 11:25:20 PM com.ibm.tivoli.cas.manager.ismp.utils.LogUtilsIcl EPMAppServer.jacl.main INFO: CTGEM2100I The WebSphere configuration script EPMAppServer.jacl started. The action taken is removeHTTPTransports.

Aug 4, 2009 11:25:22 PM com.ibm.tivoli.cas.manager.ismp.utils.LogUtilsIcl EPMAppServer.jacl.remove_Transport_chain INFO: CTGEM2107I The object of the following type TCPInboundChannel and ID chain_EP_9613.TCP(cells/risc550aNode01Cell/nodes/risc550aNode01/servers/ser ver1|server.xml#TCPInboundChannel_1249420859859) was deleted.

... OUTPUT TRUNCATED ...

Stopping agent manager server ADMU0116I: Tool information is being logged in file /usr/IBM/WebSphere/AppServer/profiles/casprofile/logs/server1/stopServer.log ADMU0128I: Starting tool with the casprofile profile ADMU3100I: Reading configuration for server: server1 ADMU3201I: Server stop request issued. Waiting for stop status. ADMU4000I: Server server1 stop completed. Sleep 30 ... Starting agent manager server ADMU0116I: Tool information is being logged in file /usr/IBM/WebSphere/AppServer/profiles/casprofile/logs/server1/startServer.log ADMU0128I: Starting tool with the casprofile profile ADMU3100I: Reading configuration for server: server1 ADMU3200I: Server launched. Waiting for initialization status. ADMU3000I: Server server1 open for e-business; process id is 393290 Successfully installed CAS --- [tpm711migrate.sh:INSTALL CAS] ended successfully at Tue Aug 4 23:27:54 GMT+02:00 2009 ------ [tpm711migrate.sh:REGISTER CAS] begins at Wed Aug 5 00:07:54 GMT+02:00 2009 ---Change agent registration password 2009-08-05 00:07:55,696 INFO COPCOM447I The password for agent will be changed. 2009-08-05 00:07:58,427 INFO COPCOM448I The password for agent was successfully changed. Change resource manager password 2009-08-05 00:07:59,807 INFO COPCOM447I The password for resourcemgr will be changed. 2009-08-05 00:08:02,428 INFO COPCOM448I The password for resourcemgr was successfully changed. Update agent manager hostname in endpoint.properties risc550a.rot.it.ibm.com Update the resource manager name in agentmanager.xml Comment out SSL.KeyRing.PW property in endpont.properties Remove SSL pwd and agenttrust.jks file Copy agentTrust.jks from agent manager to TPM Copy agentTrust.jks from agent manager to TCA respository Ping agent manager 2009-08-05 00:08:09,727 INFO Attempting to register TPM resource manager with description: 2009-08-05 00:08:09,728 INFO Agent ID = file:///opt/IBM/tivoli/tpm; ID Format = null; Version = 7; Major Release Number = 1; Minor Release Number = 1 ; Install Date = Wed Aug 05 00:08:09 CEST 2009; Label = null; Credentials = null; Observed IP Address = null; Feature Name = Tivoli Provisioning Manag er: Product Name = Tivoli Provisioning Manager: Owner Name = Tivoli: Owner Contact Description = http://www.ibm.com/tivoli; Admin. State = 2

Aug 5, 2009 12:08:12 AM com.ibm.tivoli.cas.utils.slp.SLPEngine checkInitialized INFO: CTGEM2023I Initialize the internal Service Location Protocol engine. Aug 5, 2009 12:08:12 AM com.ibm.tivoli.cas.utils.slp.SLPEngine checkInitialized INFO: CTGEM2024I Initialization passed in time=0.05 seconds. 2009-08-05 00:08:22,321 INFO Registration is successful. TPM successfully registered with CAS --- [tpm711migrate.sh:REGISTER CAS] ended successfully at Wed Aug 5 00:08:22 GMT+02:00 2009 ------ [tpm711migrate.sh:CONFIG SSL] begins at Wed Aug 5 00:13:57 GMT+02:00 2009 ---This section is made of 12 steps: Step 1: Create CDS DMS VH Step2: Create TPM SSL Keystore and Truststore Step3: Create self-signed certificate and add to key store Step4: Create self-signed certificate and add to trust store Step5: Create TPM SSL Profile Step6: Create TPM SSL transport chain Step 7: Create AM SSL Keystore and Truststore Step 8: Create AM Server SSL Profile Step 9: Create AM Client SSL Profile Step 10: Create SDI Mutual Authentication SSL transport chain Step 11: Create SDI Server Authentication SSL transport chain Step 12: Modify thread pool for TPM UI and SDI Server Transport Chain Once completed the log continues with: Config SSL is done completely SSL configuration has been completed. --- [tpm711migrate.sh:CONFIG SSL] ended successfully at Wed Aug 5 00:35:25 GMT+02:00 2009 ------ [tpm711migrate.sh:CONFIG SOAP SSL] begins at Wed Aug 5 00:35:25 GMT+02:00 2009 ---Check if cert exists in cacerts Check if cert file exists /opt/IBM/tivoli/tpm/cert/tpmui.cer is not found, export tpmuicert from keystore Certificate stored in file </opt/IBM/tivoli/tpm/cert/tpmui.cer> Import tpmuicert to cacerts Certificate was added to keystore Soap SSL configuration has been completed. --- [tpm711migrate.sh:CONFIG SOAP SSL] ended successfully at Wed Aug 5 00:35:31 GMT+02:00 2009 ------ [tpm711migrate.sh:COPY CLI KEY STORE] begins at Wed Aug 5 00:35:31 GMT+02:00 2009 ---Client key store files copied. --- [tpm711migrate.sh:COPY_CLI_KEY_STORE] ended successfully at Wed Aug 5 00:35:31 GMT+02:00 2009 ---

--- [tpm711migrate.sh:INSTALL_CDS] begins at Wed Aug 5 00:35:31 GMT+02:00 2009 --- Update CDS response file

Run database upgrade script

Database Connection Information

Database server	= DB2/AIX64 9.5.3
SQL authorization ID	= MAXIMO
Local database alias	= MAXDB71

RC=0

```
INSERT INTO CDSSCHEMA.CONFIGURATION (NAME, VALUE) VALUES ('DP_ENABLE_CLIENT_CHECKSUMS','2') DB20000I The SQL command completed successfully.
```

```
... OUTPUT TRUNCATED ...
```

--- [tpm711migrate.sh:INSTALL CDS] ended successfully at Wed Aug 5 00:44:32 GMT+02:00 2009 ---

```
--- [tpm711migrate.sh:INSTALL DMS] begins at Wed Aug 5 00:44:32 GMT+02:00 2009 ---
Update DMS response file
Install DMS
Starting the DMS Install, please wait....
Upgrade DMS tables
Running configuration task dms-upgrade-db. Log information can be found in
/opt/IBM/DeviceManager/log
Please wait...
Install Successful!
Upgrade DMS
Configuring DMS. Log information can be found in /opt/IBM/DeviceManager/log
Please wait...
Install Successful!
TPM successfully installed and configured DMS
DMS installation has been completed.
--- [tpm711migrate.sh:INSTALL DMS] ended successfully at Wed Aug 5 01:07:12 GMT+02:00 2009 ---
--- [tpm711migrate.sh:UPDATE CLI PROPS] begins at Wed Aug 5 01:07:12 GMT+02:00 2009 ---
--- [tpm711migrate.sh:UPDATE CLI PROPS] ended successfully at Wed Aug 5 01:07:16 GMT+02:00 2009
---
--- [tpm711migrate.sh:WAS WITH TIOADMIN] begins at Wed Aug 5 01:46:01 GMT+02:00 2009 ---
Starting run was runastioadmin.py
WASX7209I: Connected to process "dmgr" on node ctgCellManager01 using SOAP connector; The type
of process is: DeploymentManager
WASX7303I: The following options are passed to the scripting environment and are available as
arguments that are stored in the argv variable: "[true,
ctgNode01, MXServer, false]"
App Server Node name is ctgNode01
Check if node agent is running on ctgNode01
Nodeagent appears to be running.
Found Deployment manager
change this server run as tioadmin
```

Server name is: MXServer Found MXServer change this server run as tioadmin Server name is: nodeagent Found NodeAgent change this server run as tioadmin Server name is: webserver1 It is neither NodeAgent nor MXServer, skip it Saving configuration ... Configuration saved successfully. synchronizing nodes ... INFO: Nodes synchronization completes successfully. was runastioadmin.py is completed successfully /opt/IBM/tivoli/tpm/migration/scripts/.script/was runastioadmin.sh is finished successfully ADMU0116I: Tool information is being logged in file /usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/logs/MXServer/stopServer.log ADMU0128I: Starting tool with the ctgAppSrv01 profile ADMU3100I: Reading configuration for server: MXServer ADMU32011: Server stop request issued. Waiting for stop status. ADMU4000I: Server MXServer stop completed. ADMU0116I: Tool information is being logged in file. /usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/logs/nodeagent/stopServer.log ADMU0128I: Starting tool with the ctgAppSrv01 profile ADMU3100I: Reading configuration for server: nodeagent ADMU32011: Server stop request issued. Waiting for stop status. ADMU4000I: Server nodeagent stop completed. ADMU0116I: Tool information is being logged in file /usr/IBM/WebSphere/AppServer/profiles/ctqDmgr01/logs/dmgr/stopServer.log ADMU0128I: Starting tool with the ctgDmgr01 profile ADMU3100I: Reading configuration for server: dmgr ADMU32011: Server stop request issued. Waiting for stop status. ADMU4000I: Server dmgr stop completed. change the ownership and group for /usr/IBM/WebSphere/AppServer/profiles/ctgDmgr01 change the ownership and group for /usr/IBM/WebSphere/AppServer/logs/manageprofiles/ctgDmgr01 change the ownership and group for /usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01 change the ownership and group for /usr/IBM/WebSphere/AppServer/logs/manageprofiles/ctgAppSrv01 change the ownership and group for /usr/IBM/WebSphere/AppServer/temp change the ownership and group for /usr/IBM/WebSphere/AppServer/properties change the ownership and group for /usr/IBM/WebSphere/AppServer/systemApps/isclite.ear WAS Unix setup is completed successfully ADMU0116I: Tool information is being logged in file /usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/logs/nodeagent/startServer.log ADMU0128I: Starting tool with the ctgAppSrv01 profile ADMU3100I: Reading configuration for server: nodeagent ADMU3200I: Server launched. Waiting for initialization status. ADMU3000I: Server nodeagent open for e-business; process id is 1286150

*** End of [tpm711migrate.sh] ***

*** For references on most messages displayed on the screen, refer to
/usr/ibm/tivoli/common/COP/logs/migration/tpm711migrate.log file. ***

VALIDATION

To validate that the backup was successful, check the *\$TIO_LOGS*/migration/tpm711migrate_status.log file:

[tioadmin@risc550a][/opt/IBM/tivoli/tpm]> cat \$710_LOGS/migration/tpm711migrate_status.log PRE CHECK ENVIDONE VALIDATE INPUT DONE MIGRATE DATA DONE INSTALL CAS:CREATE CAS PROFILE DONE INSTALL CAS: INSTALL AGNT MNGR DONE INSTALL CAS:UPDATE SETUP CMD LINE DONE INSTALL CAS:MIGRATION CLOSURE TOOL DONE INSTALL_CAS:RESTART AGENT MANAGER DONE INSTALL CAS DONE REGISTER CAS:UPDATE HOSTNAME DONE REGISTER CAS:UPDATE RES NAME DONE REGISTER CAS:PING AM DONE REGISTER CAS DONE CONFIG SSL DONE CONFIG SOAP SSL DONE COPY CLI KEY STORE DONE INSTALL CDS:UPGRADE DB DONE INSTALL CDS:CDS INSTALL DONE INSTALL CDS:REORG TABLES DONE INSTALL CDS DONE INSTALL DMS:DMS INSTALL DONE INSTALL DMS:UPGRADE TBLS DONE INSTALL DMS:UPGRADE DMS DONE INSTALL DMS DONE UPDATE CLI PROPSIDONE WAS WITH TIOADMIN DONE WAS WITH TIOADMIN: CONFIG CAS PROFILE DONE

17.8.3 Changing the WebSphere Application Server casprofile profile password

Generally you are not requested to change the casprofile password. But in case you need to do this, Example 17-16 details the procedure to follow.

Example 17-16 casprofile password change procedure

```
1. start the server by running:
<WAS HOME>/profiles/casprofile/bin/startServer.sh server1
The default value for <WAS HOME> is /usr/IBM/WebSphere/AppServer
2. create a new file /tmp/test.py and cut and paste the following line
in test.py. (Replace <your new was admin password> with your new was
admin password)
AdminTask.changeFileRegistryAccountPassword(['-userId', 'wasadmin',
'-password', '<your new was admin password>', '-uniqueName',
'uid=wasadmin,o=defaultWIMFileBasedRealm'])
AdminConfig.save()
3. Run this command with the current wasadmin user password:
<WAS HOME>/profiles/casprofile/bin/wsadmin.sh -lang jython -user
wasadmin -password <current wasadmin password> -f /tmp/test.py
4. Restart the server by running:
<WAS HOME>/profiles/casprofile/bin/stopServer.sh server1 -user wasadmin
-password <current wasadmin password>
5. Restart the server by running:
<WAS HOME>/profiles/casprofile/bin/startServer.sh server1
The casprofile wasadmin password is now changed and you can start using
the new password.
```

17.8.4 Installing the base services and the Web components

The next step in the migration process is to complete the Tivoli Provisioning Manager Version 7.1.1 components installation by installing the base services and the Web components.

Installing base services

Before the base services installation, we backed up the application server and database server data, as shown in Example 17-17.

Example 17-17 back up application server and database server data

To backup the application server and database server data you have to first stop the services as detailed below:

Stop the application server

MXServer

[root@risc550a][/usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/bin]>
stopServer.sh MXServer

Node

[root@risc550a][/usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/bin]>
stopNode.sh

Deployment Manager [root@risc550a][/usr/IBM/WebSphere/AppServer/profiles/ctgDmgr01/bin]> stopManager.sh

Stop the solution installer

[root@risc550a][/tpm_images/U2823]> /usr/ibm/common/acsi/bin/acsisrv.sh
-stop

Stop the database server

[ctginst1@risc550a][/home/ctginst1]> db2stop 08/05/2009 10:24:26 0 0 SQL1064N DB2STOP processing was successful. SQL1064N DB2STOP processing was successful.

Stop the directory server

[root@risc550a][/opt/IBM/ldap/V6.2/sbin]> ibmslapd -I idsccmdb -k GLPSRV176I Terminated directory server instance 'idsccmdb' normally. [root@risc550a][/opt/IBM/ldap/V6.2/sbin]> idsdiradm -I idsccmdb -k GLPADM034I Stopped Admin server instance: 'idsccmdb'.

Stop the Monitoring Agent for Provisioning

[root@risc550a][/opt/IBM/tivoli/ITM/bin]> ./itmcmd agent stop pe

Stopping Monitoring Agent for Provisioning ... Product Monitoring Agent for Provisioning was stopped gracefully. Agent stopped...

Stop Tivoli Provisioning Manager for OS Deployment

[root@risc550a][/opt/IBM/tivoli/ITM/bin]> /etc/rc.d/init.d/rbagent stop IBM Tivoli Provisioning Manager for OS Deployment Stopping Web interface extension [root@risc550a][/opt/IBM/tivoli/ITM/bin]> /etc/rc.d/init.d/rembo stop IBM Tivoli Provisioning Manager for OS Deployment Stopping OS Deployment server [root@risc550a][/opt/IBM/tivoli/ITM/bin]> /etc/rc.d/init.d/dbgw stop IBM Tivoli Provisioning Manager for OS Deployment Stopping Database gateway

You are now ready to backup the application server (below referenced as WAS) and the database server (below referenced as DB2)

WAS

Backup the WebSpere Application Server Deployment Manager and Application Server by running these commands:

backupConfig.sh /tpm711_backups/dmgr_beforeMBSbackup.zip -nostop -quiet -logfile /tpm711 backups/backup dmgr.log -profileName ctgDmgr01 -trace

backupConfig.sh /tpm711_backups/appSrv01_beforeMBSbackup.zip -nostop
-quiet -logfile /tpm711_backups/backup_appSrv01.log -profileName
ctgAppSrv01 -trace

DB2

Backup the database server by running these commands:

```
[ctginst1@risc550a] [/home/ctginst1]> db2stop force
08/05/2009 10:48:02 0 0 SQL1032N No start database manager
command was issued.
SQL1032N No start database manager command was issued. SQLSTATE=57019
[ctginst1@risc550a] [/home/ctginst1]> db2start
08/05/2009 10:48:21 0 0 SQL1063N DB2START processing was
successful.
SQL1063N DB2START processing was successful.
[ctginst1@risc550a] [/home/ctginst1]> db2 connect to maxdb71
```

Database Connection Information

Database server = DB2/AIX64 9.5.3 SQL authorization ID = CTGINST1 Local database alias = MAXDB71

[ctginst1@risc550a][/home/ctginst1]> db2 QUIESCE DATABASE IMMEDIATE
FORCE CONNECTIONS

DB20000I The QUIESCE DATABASE command completed successfully. [ctginst1@risc550a][/home/ctginst1]> **db2 connect reset** DB20000I The SQL command completed successfully.

[ctginst1@risc550a][/]> db2 BACKUP DATABASE maxdb71 T0 /tpm711_backups
WITH 2 BUFFERS BUFFER 1024 PARALLELISM 1 COMPRESS WITHOUT PROMPTING

Backup successful. The timestamp for this backup image is : 20090805105312

You can list the files backed up:

[root@risc550a][/tpm711 backups]> ls -latr total 373568 drwxrwxrwx 2 root system 256 Aug 05 10:37 lost+found drwxr-xr-x 30 root svstem 4096 Aug 05 10:37 .. -rwxrwxrwx 1 root 49268908 Aug 05 10:45 system dmgr beforeMBSbackup.zip -rwxrwxrwx 1 root system 142947 Aug 05 10:45 backup dmgr.log -rwxrwxrwx 1 root system 160799 Aug 05 10:46 backup appSrv01.log -rwxrwxrwx 1 root 49383963 Aug 05 10:46 system appSrv01 beforeMBSbackup.zip drwxrwxrwx 3 root svstem 4096 Aug 05 10:53 . -rw----- 1 ctginst1 db2iadm1 92295168 Aug 05 10:53 MAXDB71.0.ctginst1.NODE0000.CATN0000.20090805105312.001

Now that you backed up the database server and application server data, you have to:

- Start the middleware as described in Example 17-8.
- Start the solution installer by running /usr/ibm/common/acsi/bin/acsisrv.sh -start as root user.
- Start the launchpad.

Before installing the base services, you have to first verify the installation prerequisites by clicking the corresponding link and selecting the check box at the bottom of the page you get. You are then redirected to the Custom Installation panel where you can select **Install base services**.

After the installer starts, some pre-installation processing steps are performed as shown in Figure 17-9.

	2		
	Package Summary		
Please wait while the installer performs various pre-install	ation processing.		
The installer is installing or upgrading the IBM Autonomic Computing Deployment Engine and analyzing the system to determine the changes that need to be initiated to deploy the packages required by the offering.			
-Pre-installation Activities			
Activity	Progress		
Installing or Upgrading the Deployment Engine	100%		
Detecting and Analyzing Packages Required for Offering	100%		

Figure 17-9 base services pre-installation processing

After this panel, you get the license agreement and you specify the installation folder (the default path is /opt/IBM/SMP).

Note: You now have to select the **Custom** option in the Choose Deployment panel; the **Simple** option is not supported.

The following panels are shown:

1. Import Middleware Configuration Information:

Click the Import middleware configuration information check box.

2. Database Type:

Select DB2.

3. Database:

Verify the data imported from the middleware configuration information and provide the ctginst1 database user password.

4. Automate Database Configuration:

Select **Automate Database Configuration** to allow the base services installer to automatically configure the database for use by Tivoli Provisioning Manager Version 7.1.1 (creating table spaces, database tables, database schemas and database users).

5. Remote Access Authorization:

Specify root user password.

6. DB2 Administration:

Verify the data imported from the middleware configuration information and provide the ctginst1 database user password.

7. DB2 Tablespace:

Click Next.

8. Application Server Type:

Select IBM WebSphere Application Server.

9. WebSphere Connectivity:

Verify the data imported from the middleware configuration information.

10. Automate WebSphere Configuration:

Select Automate WebSphere configuration to allow the base services installer to automatically configure the database for use by Tivoli Provisioning Manager Version 7.1.1.

11.WebSphere Remote Access Authorization:

You must specify tioadmin user and password.

12. WebSphere Deployment Manager Configuration:

Verify the data imported from the middleware configuration information and provide the wasadmin user password.

13. WebSphere Application Server Configuration:

Verify the data imported from the middleware configuration information.

14. Security:

Select Use WebSphere application security for authentication and authorization.

15.Security (LDAP schema):

Verify the data imported from the middleware configuration information and click the **Create the required users** check box.

16. Integration Adapter JMS Configuration:

Click Next.

17.SMTP configuration:

Fill in the SMTP server and Administrator e-mail fields.

18. Run Configuration Steps:

Select **Perform installation configuration now** and **Deploy application files automatically**.

19. Choose Link Folder:

We selected Other and specified /home/tioadmin.

In the Input Summary panel, you can review all the foregoing selections and the input data.

You then get the Pre-Installation Summary panel as shown in Figure 17-10.



Figure 17-10 Pre-Installation Summary panel

When the installation completes, click **Done**.
You can verify the installation by trying to log in to the following URL: http://<fully qualified hostname>:9080/maximo

You do this using maxadmin/maxadmin as user and password.

You will get the page shown in Figure 17-11.

🕙 Start Center - Mozilla Firefox						_ 🗆 ×
Eile Edit View History Bookmarks Iools Help						
🕜 🕞 C 🗙 🏠 🗋 http://risc550a.rot.it.i	ibm.com:9080/maximo/ui/	ogin		5	🛆 🔹 💦 Google	P
应 Most Visited Firefox Help 🔚 Firefox Support 🧦 Windo	ows Live Hotmail 💹 Plug	-in FAQ 🖑 playonline.ht	ml 💩 Riepilogo de Il mio eBa	ay 🕐 Canon EOS 400D / Di	Contact Reference File	»
Start Center 🔶						-
Welcome, MAXADMIN		오 Web Replay	🔸 🔒 <u>B</u> ulletins: (0) 🛛 🎤 <u>G</u> o To	⊔LLL <u>R</u> eports h [®] Start <u>C</u> enter	Profile X Sign Out ?	Help IBM. A
	다. Ch	ange Content/Layout 🕴	🔡 Display Settings 🛛 📲 Cr	eate New Template 🛛 🔏 Moo	lify Existing Template 🔌	B Update Start Center
Quick Insert 🧷 🖻 👔	Inbox / Assignment	s				100
You do not have access to the selected actions.	Description	APP	DESCRIPTION	DUEDATE	PRIORITY	Route
Favorite Applications 🥒 🗇 🏦			No Assignments	found for MAXADMIN		
You do not have access to the selected actions.	9 Bulletin Board	Filter 🛱 🖃				*
ITUP Documents 🗸 Filter > 🚓 🕽 🄗 🛛 🧷 🗇 👔	Subject	Message	Post Date	Expiration Date	View	/ed?
This portlet has not been set up. To set up, select the edit icon \checkmark in the portlet header.			There are currently no bu	lletin board messages to view.	1	
	My Active Process	Requests 💗 Filter > 🚜	1210			/==
	This portlet has not b	een set up. To set up, sele	ect the edit icon γ in the portle	t header.		
	My Process Reques	sts Rejected in the pas	t7 days 🔻 Filter > dfb 🔭	0		100
	This portlet has not b	een set up. To set up, sele	act the edit icon $^{\prime\prime}$ in the portle	t header.		
	My Draft Process R	equests 🛛 🔻 Filter > 🔞	5 0	~		/==
	This portlet has not b	een set up. To set up, sele	ct the edit icon 🥖 in the portle	it header.		
<u>र</u>						¥ F

Figure 17-11 Verifying base services installation

Installing Web components

You can now install the Web components by starting the launchpad.

Before installing the Web components, you have to first verify the installation prerequisites by clicking the corresponding link and selecting the check box at the bottom of the page you get. You are then redirected to the Custom Installation panel where you can select **Install Web components**.

After you have accepted the license agreement, you get a Process Solution Installer Packages Installation panel where you have to provide this information:

1. Database User ID:

Default value is maximo.

2. WebSphere Application Server Administrative User Name:

Default value is wasadmin.

3. WebSphere Application Server Remote Access User Name:

Enter tioadmin for UNIX.

4. Base Services Installation Directory:

Verify that the field contains the correct value (the default path is /opt/IBM/SMP).

5. Provide the passwords for all the above-mentioned users, then click **Next** at the Install Preview panel:

When the installation completes, you get the Installation Summary panel shown in Figure 17-12.

Untitled		
	TDV	Installation Summary
	IBM.	Installation Summary The Tivoli Provisioning Manager Web components are installed successfully. To complete the installation, before starting Tivoli Provisioning Manager, you must perform the post-installation tasks and read the documentation about properly starting Tivoli Provisioning Manager. This documentation is available in the Post-installation tasks chapter in the Tivoli Provisioning Manager Installation guide. Log out and log back in as the tioadmin user before starting IBM Tivoli Provisioning Manager.
InstallShield	d k	
		< Back Next > Finish

Figure 17-12 Installation Summary panel

6. Click Finish to return to the launchpad.

With the Web components installation, all the installation steps have been completed. No other software is required to run the Tivoli Provisioning Manager Version 7.1.1, but considering that this is a migration installation, you have to perform the hostnames assignments and continue the migration process on the 7.1.1 provisioning server.

17.8.5 Assigning the hostnames

The next step in the migration process is to assign the 5.1.1.2 hostnames to the 7.1.1 provisioning environment, and this is accomplished by:

- 1. Assigning the 5.1.1.2 hostname to the 7.1.1 provisioning server
- 2. Updating the database server hostname
- 3. Updating the remaining hostnames

These steps are detailed next.

Assigning the 5.1.1.2 hostname to the 7.1.1 provisioning server

To complete this task, you have to change the IP address and hostname of the 7.1.1 provisioning server to match the 5.1.1.2 provisioning server and execute the tpm711ChangeDBHost.sh script as detailed in Example 17-18.

Example 17-18 Assigning the 5.1.1.2 hostname to the 7.1.1 provisioning server

On AIX you can either use the Command Line Interface (CLI) or **smitty** to change the hostname of the system.

You must logon as root user before running on the next commands:

CLI

```
[root@risc550a][/]> /usr/sbin/mktcpip -h'risc40pa' -a'9.168.47.12' -m'255.255.255.128' -i'en0'
-n'9.64.162.21' -d'rot.it.ibm.com' -g'9.168.47.1' -A'no' -t'N/A'
```

The above command changes the hostname and the ip address of the 7.1.1 provisioning server (risc550a) to match the hostname and ip address of the 5.1.1.2 provisioning server, respectively risc40pa and 9.168.47.12.

SMITTY

The same could have been done using smitty mktcpip command.

You can now reboot the system. At startup logon as root and kill any WebSphere Application Server Java process by running these commands:

ps -ef | grep java | grep WebSphere

This lists the WebSphere Application Java processes. Use the process ID, in the PID column, to stop each process by running the following command:

kill -9 <process_ID> for each process

You can now invoke the tpm711ChangeDBHost.sh script:

[root@risc40pa][/opt/IBM/tivoli/tpm/migration/scripts]> tpm711ChangeDBHost.sh

The result will look like:

--- [tpm711ChangeDBHost.sh:PRE CHECK ENV] begins at Sat Aug 8 00:11:08 GMT+02:00 2009 ---

----- WARNING -----

This script may perform irreversible changes to your environment. Before continuing, ensure that you have read the migration documentation and have completed all of the prerequisite steps in the checklist for this script.

Are you sure you want to continue?

To continue.....enter 1 To exit.....enter 2

Enter 1 or 2 : 1

Database information retrieval completed... --- [tpm711ChangeDBHost.sh:PRE_CHECK_ENV] ended successfully at Sat Aug 8 00:11:17 GMT+02:00 2009 ---

--- [tpm711ChangeDBHost.sh:VALIDATE_INPUT] begins at Sat Aug 8 00:11:17 GMT+02:00 2009 ---

Enter the password for the database administrator user 'ctginstl': Re-enter the password to confirm:

Enter the password for the database user 'maximo': Re-enter the password to confirm:

The following values (with passwords masked) have been retrieved from /opt/IBM/tivoli/tpm/migration/scripts/tpmmigrate_unix.properties file or loaded automatically from other configurations:

-fq711HostName: risc550a.rot.it.ibm.com

```
-fq5112HostName: risc40pa.rot.it.ibm.com
-dbOSUser: ctginst1
-dbPassword: {Variable value not shown here}
-dbIsRemote: no
-dasUserName: dasusr1
-dbAdminUser: ctginst1
-dbInstanceName: ctginst1
_____
Are you sure all the input are correct?
Yes, they are correct.....enter 1
No, updates are needed.....enter 2
Enter 1 or 2:1
                          -----
--- [tpm711ChangeDBHost.sh:VALIDATE INPUT] ended successfully at Sat Aug 8 00:11:49 GMT+02:00
2009 ---
--- [tpm711ChangeDBHost.sh:INITIAL CONFIG] begins at Sat Aug 8 00:11:49 GMT+02:00 2009 ---
--- [tpm711ChangeDBHost.sh:INITIAL CONFIG] ended successfully at Sat Aug 8 00:11:49 GMT+02:00
2009 ---
--- [tpm711ChangeDBHost.sh:MIGRATE DB HOST] begins at Sat Aug 8 00:11:49 GMT+02:00 2009 ---
Stopping database ...
SQL4410W The DB2 Administration Server is not active.
Modifying configuration files ...
/home/idsccmdb/sqllib/db2nodes.cfg
/home/db2inst1/sqllib/db2nodes.cfg
/home/ctginst1/sqllib/db2nodes.cfg
Changing DB2SYSTEM setup ...
db2 update admin cfg using ...
DB20000I The UPDATE ADMIN CONFIGURATION command completed successfully.
db2 get admin cfg ...
Starting database ...
SQL4406W The DB2 Administration Server was started successfully.
--- [tpm711ChangeDBHost.sh:MIGRATE DB HOST] ended successfully at Sat Aug 8 00:50:28 GMT+02:00
2009 ---
--- [tpm711ChangeDBHost.sh:MIGRATE DB MAXPROP] begins at Sat Aug 8 00:50:28 GMT+02:00 2009 ---
Calling /opt/IBM/tivoli/tpm/migration/scripts/.script/db2UpdateMaxPropValue.sh MAXDB71 maximo
no risc40pa.rot.it.ibm.com ...
Connecting to MAXDB71 user maximo
  Database Connection Information
```

Database server = DB2/AIX64 9.5.3 SQL authorization ID = MAXIMO Local database alias = MAXDB71

Updating the maximo.maxpropvalue, set WAS.DeploymentManagerHostName to risc40pa.rot.it.ibm.com DB20000I The SQL command completed successfully. Updating the maximo.maxpropvalue, set WAS.WebServerHostName to risc40pa.rot.it.ibm.com DB20000I The SQL command completed successfully. Updating the maximo.maxpropvalue, set WAS.SibDBServerName to risc40pa.rot.it.ibm.com DB20000I The SQL command completed successfully. Updating the maximo.maxpropvalue, set Database.DB2.ServerHostName to risc4Opa.rot.it.ibm.com DB20000I The SQL command completed successfully. Updating the maximo.maxpropvalue, set mxe.db.url to idbc:db2://risc40pa.rot.it.ibm.com:50005/maxdb71 DB20000I The SQL command completed successfully. Reseting database connection... DB20000I The SQL command completed successfully. --- [tpm711ChangeDBHost.sh:MIGRATE DB MAXPROP] ended successfully at Sat Aug 8 00:51:58 GMT+02:00 2009 ------ [tpm711ChangeDBHost.sh:UNDO MAXIMO CONFIG] begins at Sat Aug 8 00:51:58 GMT+02:00 2009 ---Calling /opt/IBM/tivoli/tpm/migration/scripts/.script/db2ConfigUndoMaximo.sh MAXDB71 ctginst1 no ... Connecting to MAXDB71 user ctginst1 Database Connection Information Database server = DB2/AIX64 9.5.3SQL authorization ID = CTGINST1 local database alias = MAXDB71 alter BUFFERPOOL MAXBUFPOOL IMMEDIATE SIZE 1000 AUTOMATIC DB20000I The SQL command completed successfully. update db cfg using applheapsz 8192 DB200001 The UPDATE DATABASE CONFIGURATION command completed successfully. update db cfg using dbheap 4000 DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. update db cfg using dft queryopt 5 DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. update db cfg using locklist automatic DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. update db cfg using maxlocks automatic DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. update db cfg using logprimary 30 DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully.

SQL1363W One or more of the parameters submitted for immediate modification were not changed dynamically. For these configuration parameters, all applications must disconnect from this database before the changes become effective.

update db cfg using logsecond 20 DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully.

update db cfg using maxfilop 32768 DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully.

update db cfg using pckcachesz AUTOMATIC DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully.

update db cfg using self_tuning_mem ON DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully.

update db cfg using softmax 520 DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. SQL1363W One or more of the parameters submitted for immediate modification were not changed dynamically. For these configuration parameters, all applications must disconnect from this database before the changes become effective.

update db cfg using auto_reorg off immediate DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully.

update db cfg using auto_db_backup off immediate DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully.

DB21007E End of file reached while reading the command. Reseting database connection... DB200001 The SQL command completed successfully. Restarting database ... 08/08/2009 00:52:05 0 0 SQL1064N DB2STOP processing was successful. SQL1064N DB2STOP processing was successful. 08/08/2009 00:52:08 0 0 SQL1063N DB2START processing was successful. SQL1063N DB2START processing was successful. --- [tpm711ChangeDBHost.sh:UND0_MAXIM0_CONFIG] ended successfully at Sat Aug 8 00:52:08 GMT+02:00 2009 ---

*** For references on most messages displayed on the screen, refer to
/usr/ibm/tivoli/common/COP/logs/migration/tpm711ChangeDBHost.log file. ***
[root@risc40pa][/opt/IBM/tivoli/tpm/migration/scripts]>

VALIDATION

To validate that the backup was successful, check the *\$TIO LOGS*/migration/tpm711ChangeDBHost status.log file:

[root@risc40pa][/opt/IBM/tivoli/tpm/migration/scripts]> cat
\$TIO_LOGS/migration/tpm711ChangeDBHost_status.log
PRE_CHECK_ENV|DONE
VALIDATE_INPUT|DONE
INITIAL_CONFIG|DONE
MIGRATE_DB_HOST|DONE
MIGRATE_DB_MAXPROP|DONE
UNDO MAXIMO CONFIG|DONE

Updating the database server hostname

Before starting the procedure, make sure that the database server and the LDAP server are running, then change the IP address and hostname of the database server by following the steps detailed in Example 17-19.

Example 17-19 Updating the database server hostname

To check the directory server status you can run this command: root@risc40pa][/opt/IBM/tivoli/tpm/migration/scripts]> ps -ef[grep ids - 0:00 dsccmdb 356526 1 0 23:41:46 /opt/IBM/ldap/V6.2/sbin/64/ibmdiradm -I idsccmdb root 434390 467082 0 00:56:53 pts/0 0:00 grep ids from the above output you see that only the administrative daemon is running. To start the instance you must run these commands: su - idsccmdb followed by db2start to start the directory server database /opt/IBM/ldap/V6.2/sbin/ibmslapd -I idsccmdb to start the directory server instance. To verify the correct directory server instance stratup you can look for the listening port 389 in the netstat command output: root@risc40pa][/opt/IBM/tivoli/tpm/migration/scripts]> netstat -an

|grep -i 389 cp 0 0 *.389 *.* LISTEN To start the database for the ctginst1 instance run these commands:

```
su - ctginst1 followed by db2start.
```

To complete the database server hostname and ip address change you have to change the maximo.properties file as detailed below:

- edit the file /opt/IBM/SMP/etc/maximo.properties_orig and change the hostname. If necessary update the password as well:

```
mxe.db.password=root550a
mxe.db.url=jdbc:db2://risc40pa.rot.it.ibm.com:50005/maxdb71
mxe.db.driver=com.ibm.db2.jcc.DB2Driver
mxe.db.user=maximo
mxe.registry.port=13400
mxe.rmi.port=0
mxe.name=MXServer
mxe.db.schemaowner=maximo
```

- delete the following line from the file:

mxe.crontask.donotrun=ALL
In our environment it was not present.

```
- copy the maximo.properties_orig as maximo.properties in
/opt/IBM/SMP/maximo/applications/maximo/properties after deleting the
existing maximo.properties file
```

- encrypt the maximo.properties file by running this command:

[root@risc40pa][/opt/IBM/SMP/maximo/tools/maximo]> encryptproperties.sh

The execution of this command prints out several information on the screen. A succesfull execution will end with: BMXAA6875I - The EncryptProperties process completed successfully. BMXAA6820I - EncryptProperties completed without errors. Sat Aug 08 01:11:00 CEST 2009

```
- su - tioadmin
```

```
- copy into
```

/opt/IBM/tivoli/tpm/lwi/runtime/tpm/eclipse/plugins/tpm_pmp/properties
the modified maximo.properties file

Updating the remaining hostnames

The last step in the hostnames changes is the execution of the tpm711ChangeOtherHost.sh script as detailed in Example 17-20.

Before running the script, make sure the database server, the LDAP server, and the administrative daemon are running as detailed at the beginning of the previous Example 17-19 on page 630.

Table 17-5 describes the passwords you will be prompted for at the beginning of the script execution.

Password	Description
WebSphere Application Server	The password for WebSphere Application Server administrator 'wasadmin'
Database user	The password for the database user 'maximo'
Agent manager resource manager	The agent manager resource manager password. Unless changed after the installation, the default password created by the installer in 7.1.1 is password.
Resource manager SSL	The resource manager SSL password. The default password is CDSRMPASS

Table 17-5 Passwords required for the tpm711ChangeOtherHost.sh script

Example 17-20 shows the tpmChangeOtherHost.sh script execution details.

Example 17-20 tpm711ChangeOtherHost.sh script execution

To invoke the script run this command as root user:

[root@risc40pa][/opt/IBM/tivoli/tpm/migration/scripts]> tpm711ChangeOtherHost.sh

The output will look like:

--- [tpm711ChangeOtherHost.sh:PRE_CHECK_ENV] begins at Sat Aug 8 01:17:28 GMT+02:00 2009 ---

----- WARNING -----

This script may perform irreversible changes to your environment. Before continuing, ensure that you have read the migration documentation and have completed all of the prerequisite steps in the checklist for this script. _____ Are you sure you want to continue? To continue.....enter 1 To exit.....enter 2 Enter 1 or 2:1--------- [tpm711ChangeOtherHost.sh:PRE CHECK ENV] ended successfully at Sat Aug 8 01:17:32 GMT+02:00 2009 ------ [tpm711ChangeOtherHost.sh:VALIDATE INPUT] begins at Sat Aug 8 01:17:32 GMT+02:00 2009 ---Enter the WebSphere Application Server user password: Re-enter the password to confirm: risc40pa.rot.it.ibm.com check passed Enter the password for the database user 'maximo': Re-enter the password to confirm: Enter the agent manager resource manager password: Re-enter the password to confirm: Enter the resource manager SSL password: Re-enter the password to confirm: The following values (with passwords masked) have been retrieved from /opt/IBM/tivoli/tpm/migration/scripts/tpmmigrate unix.properties file or loaded automatically from other configurations: -fg711HostName: risc550a.rot.it.ibm.com -fg5112HostName: risc4Opa.rot.it.ibm.com -wasUser: wasadmin -wasUserPasswd: {Variable value not shown here}

-wasCellName: ctgCell01 -httpServerHome: /opt/IBM/HTTPServer -dmgrSoapPort: 8879 -CatalogueService.Host: risc40pa.rot.it.ibm.com -CertManagement.Host: risc40pa.rot.it.ibm.com -AgentOuerv.Host: risc40pa.rot.it.ibm.com -Registration.Server.Host: risc4Opa.rot.it.ibm.com -TrustedCertificateQuery.Host: risc40pa.rot.it.ibm.com -AgentManagerQuery.Host: risc40pa.rot.it.ibm.com -dbPort: 50005 -cdsHome: /opt/IBM/tivoli/CDS -amUser: manager -amPort: 9511 -dbPass: {Variable value not shown here} -amResMgrPass: {Variable value not shown here} -cdsRMPass: {Variable value not shown here} -dbIsRemote: no -tpmfosdDataDir: /opt/tpmfosd files Are you sure all the input are correct? Yes, they are correct.....enter 1 No, updates are needed.....enter 2 Fnter 1 or 2 : 1 risc550a.rot.it.ibm.com check passed --- [tpm711ChangeOtherHost.sh:VALIDATE INPUT] ended successfully at Sat Aug 8 01:19:20 GMT+02:00 2009 ------ [tpm711ChangeOtherHost.sh:INITIAL CONFIG] begins at Sat Aug 8 01:19:20 GMT+02:00 2009 ------ [tpm711ChangeOtherHost.sh:INITIAL CONFIG] ended successfully at Sat Aug 8 01:19:21 GMT+02:00 2009 ------ [tpm711ChangeOtherHost.sh:UPDATE USERFACTORY] begins at Sat Aug 8 01:19:21 GMT+02:00 2009 ------ [tpm711ChangeOtherHost.sh:UPDATE USERFACTORY] ended successfully at Sat Aug 8 01:19:21 GMT+02:00 2009 ------ [tpm711ChangeOtherHost.sh:UPDATE WAS ND] begins at Mon Aug 24 09:29:54 GMT+02:00 2009 ---Buildfile: /opt/IBM/tivoli/tpm/migration/scripts/../config/changeWASHostname.xml

```
[YOU HAVE NEW MAIL]
App Node Name is ctgNode01
Stopping MXServer ...
ADMU0116I: Tool information is being logged in file
/usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/logs/MXServer/stopServer.log
ADMU0128I: Starting tool with the ctgAppSrv01 profile
ADMU3100I: Reading configuration for server: MXServer
ADMU0509I: The server "MXServer" cannot be reached. It appears to be stopped.
ADMU0211I: Error details may be seen in the file:
/usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/logs/MXServer/stopServer.log
Stopping casprofile ...
ADMU0116I: Tool information is being logged in file
/usr/IBM/WebSphere/AppServer/profiles/casprofile/logs/server1/stopServer.log
ADMU0128I: Starting tool with the casprofile profile
ADMU3100I: Reading configuration for server: server1
ADMU0509I: The server "server1" cannot be reached. It appears to be stopped.
ADMU0211I: Error details may be seen in the file:
/usr/IBM/WebSphere/AppServer/profiles/casprofile/logs/server1/stopServer.log
casprofile is stopped completely.
MXServer is stopped completely.
Stopping node agent ...
ADMU0116I: Tool information is being logged in file
/usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/logs/nodeagent/stopServer.log
ADMU0128I: Starting tool with the ctgAppSrv01 profile
ADMU3100I: Reading configuration for server: nodeagent
ADMU05091: The server "nodeagent" cannot be reached. It appears to be stopped.
ADMU0211I: Error details may be seen in the file:
/usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/logs/nodeagent/stopServer.log
node agent is stopped completely.
Stopping deployment manager ...
ADMU0116I: Tool information is being logged in file
           /usr/IBM/WebSphere/AppServer/profiles/ctqDmgr01/logs/dmgr/stopServer.log
ADMU0128I: Starting tool with the ctgDmgr01 profile
ADMU3100I: Reading configuration for server: dmgr
ADMU0509I: The server "dmgr" cannot be reached. It appears to be stopped.
ADMU0211I: Error details may be seen in the file:
           /usr/IBM/WebSphere/AppServer/profiles/ctqDmgr01/logs/dmgr/stopServer.log
deployment manager is stopped completely.
java processes are stopped
```

Buildfile: /opt/IBM/tivoli/tpm/migration/scripts/../config/changeWASHostname.xml
DM profile is edited successfully
Buildfile: /opt/IBM/tivoli/tpm/migration/scripts/../config/changeWASHostname.xml
APP profile is edited successfully

Buildfile: /opt/IBM/tivoli/tpm/migration/scripts/../config/changeWASHostname.xml

casprofile profile is edited successfully
Transaction.properties file modified successfully
--- [tpm711ChangeOtherHost.sh:UPDATE_WAS_ND] ended successfully at Mon Aug 24
13:02:58 GMT+02:00 2009 ---

--- [tpm711ChangeOtherHost.sh:UPDATE_SDI_HOSTNAME] begins at Mon Aug 24 13:02:58 GMT+02:00 2009 ---

--- [tpm711ChangeOtherHost.sh:UPDATE_SDI_HOSTNAME] ended successfully at Mon Aug 24 13:03:02 GMT+02:00 2009 ---

--- [tpm711ChangeOtherHost.sh:MIGRATE_DCM_XML] begins at Mon Aug 24 13:03:02 GMT+02:00 2009 ---

--- [tpm711ChangeOtherHost.sh:MIGRATE_DCM_XML] ended successfully at Mon Aug 24 13:03:02 GMT+02:00 2009 ---

--- [tpm711ChangeOtherHost.sh:UPDATE_DCM_LOCAL_HOST] begins at Mon Aug 24 13:03:02 GMT+02:00 2009 ---

[YOU HAVE NEW MAIL]

Success: The Local server name is already fully qualified or it has been updated successfully.

--- [tpm711ChangeOtherHost.sh:UPDATE_DCM_LOCAL_HOST] ended successfully at Mon Aug 24 13:03:25 GMT+02:00 2009 ---

--- [tpm711ChangeOtherHost.sh:CHANGE TPMFOSD HOST] begins at Mon Aug 24 13:03:25 GMT+02:00 2009 ---TPMfOSd installation detected, updating configuration... IBM Tivoli Provisioning Manager for OS Deployment Stopping OS Deployment server OS deployment server is not running IBM Tivoli Provisioning Manager for OS Deployment Starting OS Deployment server IBM Tivoli Provisioning Manager for OS Deployment server v.7.1.0.0 (080.96) Licensed Materials - Property of IBM. L-BMIK-7GTL7K (C) Copyright IBM Corporation 1998, 2009. All Rights Reserved. IBM, the IBM logo, and Tivoli are trademarks of IBM Corporation in the United States, other countries or both. * Using interface 9.168.47.12 (auto-detected) user.dir=[/opt/IBM/tivoli/tpm/migration/scripts] file:/opt/IBM/tivoli/tpm/xml/tpmfosdbootserver.xml

2009-08-24 13:03:43,251 INFO Import took 8951 millisecs --- [tpm711ChangeOtherHost.sh:CHANGE_TPMFOSD_HOST] ended successfully at Mon Aug 24 13:03:49 GMT+02:00 2009 ---

--- [tpm711ChangeOtherHost.sh:UPDATE_TIVOLI_SEND_RECEIVE_CONF] begins at Mon Aug 24 13:03:49 GMT+02:00 2009 ---

--- [tpm711ChangeOtherHost.sh:UPDATE_TIVOLI_SEND_RECEIVE_CONF] ended successfully at Mon Aug 24 13:03:49 GMT+02:00 2009 ---

--- [tpm711ChangeOtherHost.sh:REGISTER_CDS] begins at Mon Aug 24 13:03:49 GMT+02:00 2009 ---

Aug 24, 2009 1:04:20 PM com.ibm.tivoli.cas.utils.slp.SLPEngine checkInitialized INFO: CTGEM2023I Initialize the internal Service Location Protocol engine. Aug 24, 2009 1:04:20 PM com.ibm.tivoli.cas.utils.slp.SLPEngine checkInitialized INFO: CTGEM2024I Initialization passed in time=0.07 seconds.

The Resource Manager was registered successfully with the Agent Manager.

--- [tpm711ChangeOtherHost.sh:REGISTER_CDS] ended successfully at Mon Aug 24 13:04:33 GMT+02:00 2009 ---

--- [tpm711ChangeOtherHost.sh:CHANGE_INFOCENTER_HOST] begins at Mon Aug 24 13:04:33 GMT+02:00 2009 ---

--- [tpm711ChangeOtherHost.sh:CHANGE_INFOCENTER_HOST] ended successfully at Mon Aug 24 13:04:33 GMT+02:00 2009 ---

*** End of [tpm711ChangeOtherHost.sh] ***

*** For references on most messages displayed on the screen, refer to
/usr/ibm/tivoli/common/COP/logs/migration/tpm711ChangeOtherHost.log file. ***

VALIDATION

To validate that the backup was successful, check the \$TIO_LOGS/migration/tpm711ChangeOtherHost_status.log file:

[root@risc40pa][/usr/ibm/tivoli/common/COP/logs/migration]> cat
\$TI0_LOGS/migration/tpm711ChangeOtherHost_status.log
PRE_CHECK_ENV|DONE
VALIDATE_INPUT|DONE
INITIAL_CONFIG|DONE
UPDATE_USERFACTORY|DONE
UPDATE_WAS_ND|DONE
UPDATE_SDI_HOSTNAME|DONE
MIGRATE_DCM_XML|DONE
UPDATE_DCM_LOCAL_HOST|DONE

CHANGE_TPMFOSD_HOST|DONE UPDATE_TIVOLI_SEND_RECEIVE_CONF|DONE REGISTER_CDS|DONE CHANGE_INFOCENTER_HOST|DONE

To continue the validation, make sure that the following files do not contain anymore references to the old hostname, risc550a, but only to the new, risc40pa:

endpoint.properties file

[root@risc40pa][/usr/ibm/tivoli/common/COP/logs]> grep risc550a
\$TI0_HOME/config/endpoint.properties

[root@risc40pa][/usr/ibm/tivoli/common/COP/logs]> grep risc40pa
\$TI0_HOME/config/endpoint.properties
CatalogueService.Host=risc40pa.rot.it.ibm.com
CertManagement.Host=risc40pa.rot.it.ibm.com
AgentQuery.Host=risc40pa.rot.it.ibm.com
Registration.Server.Host=risc40pa.rot.it.ibm.com
TrustedCertificateQuery.Host=risc40pa.rot.it.ibm.com
AgentManagerQuery.Host=risc40pa.rot.it.ibm.com

dcm.xml file

[root@risc40pa][/usr/ibm/tivoli/common/COP/logs]> grep risc550a
\$TI0_HOME/config/dcm.xml

17.8.6 Continuing the migration on the 7.1.1 provisioning server

This section describes some steps to continue the migration in the 7.1.1 provisioning server that include:

- 1. Starting the 7.1.1 provisioning server
- 2. Validating the migration
- 3. Restoring the 5.1.1.2 LDAP information to 7.1.1
- 4. Migrating access groups
- 5. Backing up the database
- 6. Migrating dynamic groups

These steps are detailed next.

Starting the 7.1.1 provisioning server

You can now start the new migrated Tivoli Provisioning Manager Version 7.1.1 server.

You can eventually change the tioadmin user password to match the one used in 5.1.1.2 provisioning server by using the changePassword.sh script.

Example 17-21 details the steps executed to start the new migrated provisioning server for the first time.

```
Example 17-21 Starting the 7.1.1 provisioning server
```

We first rebooted the system after the hostnames change procedure and restarted these products in the following sequence:

```
    1) db2start for the idsccmdb instance
    2) db2start for the ctginst1 instance
    3) checked that the LDAP administrative daemon (ibmdiradm) started succesfully at system boot
    4) started the LDAP instance
```

Started Tivoli Provisioning Manager Version 7.1.1 by running **tio.sh start** command as tioadmin user. Follows the startup result:

```
[tioadmin@risc40pa][/opt/IBM/tivoli/tpm/tools]> tio.sh start
Start TPM engines
```

```
...waiting
...waiting
The lightweight runtime has started successfully.
Start Deployment Manager
ADMU0116I: Tool information is being logged in file
```

/usr/IBM/WebSphere/AppServer/profiles/ctgDmgr01/logs/dmgr/startServer.l
og
ADMU0128I: Starting tool with the ctgDmgr01 profile
ADMU3100I: Reading configuration for server: dmgr
ADMU3200I: Server launched. Waiting for initialization status.
ADMU3000I: Server dmgr open for e-business; process id is 118796
Start Agent Manager server1
ADMU0116I: Tool information is being logged in file

```
/usr/IBM/WebSphere/AppServer/profiles/casprofile/logs/server1/startServ
er.log
ADMU0128I: Starting tool with the casprofile profile
ADMU3100I: Reading configuration for server: server1
ADMU3200I: Server launched. Waiting for initialization status.
```

ADMU3000I: Server server1 open for e-business; process id is 462878 Start Node ADMU0116I: Tool information is being logged in file

/usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/logs/nodeagent/startS
erver.log
ADMU0128I: Starting tool with the ctgAppSrv01 profile
ADMU3100I: Reading configuration for server: nodeagent
ADMU3200I: Server launched. Waiting for initialization status.
ADMU3000I: Server nodeagent open for e-business; process id is 368830
Start Server MXServer
ADMU0116I: Tool information is being logged in file

/usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/logs/MXServer/startSe rver.log ADMU0128I: Starting tool with the ctgAppSrv01 profile ADMU3100I: Reading configuration for server: MXServer ADMU3200I: Server launched. Waiting for initialization status. ADMU3000I: Server MXServer open for e-business; process id is 106498 TPM startup completed.

```
Check the following logs for startup errors:
/usr/ibm/tivoli/common/COP/logs/tio_start.log
/usr/ibm/tivoli/common/COP/logs/tio_start_service.log
/opt/IBM/tivoli/tpm/lwi/logs
/usr/IBM/WebSphere/AppServer/profiles/ctgDmgr01/logs/dmgr
/usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/logs/nodeagent
/usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/logs/MXServer
/usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/logs/MXServer
```

We then checked the SystemOut.log for the MXServer:

[8/24/09 14:01:50:201 CEST] 00000017 SystemOut 0 24 Aug 2009 14:01:50:201 [INFO] BMXAA6467I - A remote object with name rmi://risc40pa.rot.it.ibm. com:13400/MXServer already exists while trying to bind remote object.A cluster configuration is assumed. [8/24/09 14:02:06:640 CEST] 00000017 ServletWrappe I SRVE0242I: [MAXIMO] [/mbo] [MAXIMOStartupServlet]: Initialization successful. [8/24/09 14:02:06:686 CEST] 00000017 ServletWrappe I SRVE0242I: [MAXIMO] [/mbo] [ToolClientServlet]: Initialization successful. [8/24/09 14:02:06:701 CEST] 00000017 VirtualHost I SRVE0250I: Web Module MBO Web Application has been bound to maximo host[*:9443]. [8/24/09 14:02:06:838 CEST] 00000017 WebGroup A SRVE0169I: Loading Web Module: MEA Web Application.

[8/24/09 14:02:07:662 CEST] 00000017 DeploymentEng I org.apache.axis2.deployment.DeploymentEngine prepareRepository No services directory was found un der /usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/installedApps/ctgCell 01/MAXIMO.ear/meaweb.war/WEB-INF. [8/24/09 14:02:07:677 CEST] 00000017 DeploymentEng I org.apache.axis2.deployment.DeploymentEngine prepareRepository No modules directory was found und er /usr/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/installedApps/ctgCell 01/MAXIMO.ear/meaweb.war/WEB-INF. [8/24/09 14:02:08:394 CEST] 00000017 ServletWrappe I SRVE0242I: [MAXIMO] [/meaweb] [AxisServlet]: Initialization successful. [8/24/09 14:02:08:409 CEST] 00000017 VirtualHost I SRVE0250I: Web Module MEA Web Application has been bound to maximo host[*:9443]. [8/24/09 14:02:08:439 CEST] 00000017 ApplicationMg A WSVR0221I: Application started: MAXIMO [8/24/09 14:02:08:497 CEST] 0000000a TCPChannel TCPC0001I: TCP Ι Channel TCP 1 is listening on host * (IPv6) port 9061. [8/24/09 14:02:08:764 CEST] 0000000a WSChannelFram A CHFW0019I: The Transport Channel Service has started chain WCInboundAdmin. [8/24/09 14:02:08:781 CEST] 0000000a TCPChannel T TCPC0001I: TCP Channel TCP 2 is listening on host * (IPv6) port 9080. [8/24/09 14:02:09:050 CEST] 0000000a WSChannelFram A CHFW0019I: The Transport Channel Service has started chain WCInboundDefault. [8/24/09 14:02:09:063 CEST] 0000000a TCPChannel TCPC0001I: TCP Ι Channel TCP 3 is listening on host * (IPv6) port 9044. [8/24/09 14:02:09:322 CEST] 0000000a WSChannelFram A CHFW0019I: The Transport Channel Service has started chain WCInboundAdminSecure. [8/24/09 14:02:09:367 CEST] 0000000a TCPChannel TCPC0001I: TCP Ι Channel TCP 4 is listening on host * (IPv6) port 9443. [8/24/09 14:02:09:643 CEST] 0000000a WSChannelFram A CHFW0019I: The Transport Channel Service has started chain WCInboundDefaultSecure. [8/24/09 14:02:09:668 CEST] 0000000a TCPChannel I TCPC0001I: TCP Channel SDIMutualTcpChannel is listening on host * (IPv6) port 9046. [8/24/09 14:02:09:947 CEST] 0000000a WSChannelFram A CHFW0019I: The Transport Channel Service has started chain SDIMutualTransportChain. [8/24/09 14:02:09:988 CEST] 0000000a TCPChannel I TCPC0001I: TCP Channel SDIServerTcpChannel is listening on host * (IPv6) port 9045. [8/24/09 14:02:10:273 CEST] 0000000a WSChannelFram A CHFW0019I: The Transport Channel Service has started chain SDIServerTransportChain. [8/24/09 14:02:10:307 CEST] 0000000a WSChannelFram A CHFW0019I: The Transport Channel Service has started chain SOAPAcceptorChain1.

[8/24/09 14:02:10:337 CEST] 0000000a WSChannelFram A CHFW0019I: The Transport Channel Service has started chain SOAPAcceptorChain2. [8/24/09 14:02:10:367 CEST] 0000000a WSChannelFram A CHFW0019I: The Transport Channel Service has started chain SOAPAcceptorChain3. [8/24/09 14:02:10:391 CEST] 0000000a WSChannelFram A CHFW0019I: The Transport Channel Service has started chain SOAPAcceptorChain4. [8/24/09 14:02:10:427 CEST] 0000000a WSChannelFram A CHFW0019I: The Transport Channel Service has started chain SOAPAcceptorChain5. [8/24/09 14:02:10:457 CEST] 0000000a WSChannelFram A CHFW0019I: The Transport Channel Service has started chain SOAPAcceptorChain6. [8/24/09 14:02:10:501 CEST] 00000017 SchedulerServ I SCHD0077I: The Scheduler Service is starting the Schedulers. [8/24/09 14:02:10:540 CEST] 00000017 SchedulerServ I SCHD0078I: The Scheduler Service has completed starting the Schedulers. [8/24/09 14:02:10:742 CEST] 0000000a RMIConnectorC A ADMC0026I: The RMI Connector is available at port 9810 [8/24/09 14:02:11:451 CEST] 0000001a UserManagemen I CWWIM60021 Received notification that the server has finished starting. [8/24/09 14:02:11:515 CEST] 0000001a UserManagemen I CWWIM6003I Initialization of the dynamic reload manager completed successfully. [8/24/09 14:02:16:557 CEST] 00000030 ServletWrappe I SRVE0242I: [DMS WebApp] [/dmserver] [EDMSTPMManagementService]: Initialization successful. [8/24/09 14:02:21:501 CEST] 0000002f Serv]etWrappe I SRVE0242I: [CDS] [/DownloadGrid] [MCServices]: Initialization successful. [8/24/09 14:02:22:728 CEST] 00000036 DiscoveryMBea I ADMD0023I: The system discovered process (name: nodeagent, type: NodeAgent, pid: 368830) [8/24/09 14:02:25:727 CEST] 0000000a WsServerImp] A WSVR0001I: Server MXServer open for e-business

You can now access the Tivoli Provisioning Manager Version 7.1.1 Graphical User Interface by using this URL:

https://<fully_qualified_hostname>:9443/maximo

The Start Center page is displayed, as shown in Figure 17-13.

🥹 Start Center - Mozilla Firefox					<u>_ ×</u>
Eile Edit View History Bookmarks Iools Help					
C 🗙 🟠 🚺 🔀 🔀	🔇 🔀 🗶 🏡 🚺 🕅 com https://risc40pa.rot.it.ibm.com:9443/maximo/ui/login				
🙍 Most Visited 🔆 Firefox Help 📰 Firefox Support 🤌 Windows	Live Hotmail 💹 Plug-in FAQ	😂 playonline.html 💩 Riepilogo de 1	ll mio eBay 🧐 Canon EOS 400D /	Di 📄 Contact Reference Fil	e »
Start Center					
Welcome, MAXADMIN		O Web Replay Pulletins: (0)	r <mark>¢ <u>G</u>o To IIII <u>R</u>eports III Start <u>C</u>e</mark>	enter 🔺 <u>P</u> rofile 🎽 <u>Si</u> gn Out	? Help IEM. 🖻
Automation Package Developer Compliance Analyst D	eployment Specialist Pr	ocess Management Requester Pr	ovisioning Administrator Prov	visioning Configuration Librarian	
	Change C	ontent/Layout 🔤 Display Settings	Create New Template	Modify Existing Template	28 Update Start Center
Automation development applications	Status of my recent prov	visioning workflows 🛛 🔻 Filter > 🕅	2 @		/ = 1
Provisioning Workflows	Deployment Request ID		Workflow Name	Error Message	
	10.000				
Provisioning Workflow Status	Set Graph Options		No_operation		1 - 1 of 1
Provisioning Computers	Status of my recent prov	visioning tasks i 🔻 Filter > 🚜 i 🖄 i	\$		/
	Provisioning Task			Status	Start Date
Virtualization Management	Run provisioning workflow	No_operation submitted at August 24, 2	009 2:19:40 PM CEST	Success	8/24/09 2:19 PM
Provisioning Task Tracking	Graphical View				1 - 1 of 1
• M	Data model object finder	r 🔝 Filter > 🚯 🗊 🏟			2 = 1
Provisioning Task Definitions	Object ID	Object		Object Type	
	1,009	Windows Computers		Computer Group	
Provisioning administration applications 🥒 🗆 🗊	1,010	AIX Computers		Computer Group	
	1,011	Red Hat Linux Computers		Computer Group	
Other configuration and development applications 🥒 🗖 🛊	1,012	HPUX Computers		Computer Group	
	1,013	Envorite Computers		Computer Group	
	1,014	Eavorite Computers		Group	
	41.024	TPC SANFabric		Device Driver	
	41,026	TPC StorageSubsystem		Device Driver	
	41,028	TPC StoragePool		Device Driver	
	Set Graph Options			1 - 10	of 1200 <u>Next Page</u> »
x					7
					<u>}</u>

Figure 17-13 Tivoli Provisioning Manager Version 7.1.1 Start Center

Important: Before starting to use Tivoli Provisioning Manager Version 7.1.1, ensure that the __master_tc_driver_update_ workflow task completes.

To check the status, click Go To \rightarrow Task Management \rightarrow Provisioning Tasks \rightarrow Provisioning Workflow Status.

Figure 17-14 shows the page you get after the foregoing selection.

Provisioning Workflow Sta	atus - Mozilla Firefox								
<u>File Edit View History I</u>	<u>B</u> ookmarks <u>T</u> ools <u>H</u> elp								
	🕜 🕞 🕈 🔥 📄 bm.com https://risc40pa.rot.it.ibm.com:9443/maximo/ui/login					☆ • 👔	Google		P
应 Most Visited 👯 Firefox Hel	p 🔚 Firefox Support 🧦 Windows Live Hotn	nail <u> I</u> Plug-in FAQ	Ø playonline.html 💇 Riep	ilogo de Il mio eBay	🕖 Canon EC	05 400D / Di 📄 Conta	ict Reference F	File	**
Provisioning Workflow	status 🔶								-
Provisioning Workflo	w Status		🕑 Web Replay 🛛 👂 <u>B</u> ulleti	ns: (0) 🛛 🧖 <u>G</u> o To	Int Reports	Start Center & Profile	Sign Out	? Help	RM. 🖻
Find:	n 🔫 Select Action	🦳 🖌 🍐 📢	0						
List Execution Logs	3								
🖄 Advanced Search 🔻 🔒	Save Query 👻 🥔 Bookmarks								
Deployment Dequeete	111							R. Download	2: 6
Deployment Request	Workflow Name		Start Date		Status			E/ Downood	
		1							
<u>13,200</u>	No_operation	1	8/24/09 2:19 PM		Success		1		×
<u>12,800</u>	master_tcdriver_update_]	1	8/11/09 1:38 AM		Success		,		×
<u>12,404</u>	MS_SDI_Config_Offline	1	8/4/09 11:02 PM	8	Failed				×
12,403	TivoliCommonAgent_Upgrade	:master_todriver_	update/4/09 11:01 PM		Success		1		×
12,402	YUM_Configure_TCDriver	1	8/4/09 10:54 PM		Success				×
12,401	TCAupgrade_CreateSPBs	1	8/4/09 10:50 PM		Success				×
12,400	UnzipSWDCLI	1	8/4/09 10:48 PM		Success		1		×
12,020	TCA_PingAgent	1	7/31/09 7:06 PM		Success		1		×
12,005	Install_CDS_Depot	8	7/31/09 2:27 PM		Success		1		×
12,004	Discovery.OnDevice	1	7/31/09 1:34 PM		Success		2		×
12,003	InitialDiscovery	1	7/31/09 12:06 PM		Success		1		×
12,002	InitialDiscovery	1	7/31/09 9:37 AM		Success		1		×
12,001	InitialDiscovery	1	7/31/09 9:15 AM		Success		1		×
<u>11,664</u>	Install_Agent	1	7/30/09 9:18 PM	8	Failed		1		×
<u>11,663</u>	InitialDiscovery	1	7/30/09 9:17 PM		Success		1		×
12,000	Discovery.OnDevice	7	7/30/09 7:58 PM		Success		1		×
11.662	Discovery.OnDevice	P	7/30/09 5:33 PM		Success		1		×
<u>11,661</u>	Discovery.OnDevice	1	7/30/09 5:33 PM		Success		1		×
<u>11,660</u>	Discovery.OnDevice	1	7/30/09 4:41 PM		Success		1		×
11,721	Discovery.OnDevice	1	7/30/09 3:44 PM	8	Failed		1		×
Select Records									×1
र									Þ

Figure 17-14 ____master_tc_driver_update_ workflow status

Validating the migration

The migration guide suggests some operations to be executed to validate the migration.

For details about this task, refer to *Tivoli Provisioning Manager Version 7.1.1 Migration Guide* at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ibm.t ivoli.tpm.ins.doc/tpm_migrate_guide.pdf

We tried to run a workflow called No_operation to verify the deployment engine functionality and checked that the computers from our 5.1.1.2 environment were listed in the 7.1.1 provisioning server, navigating the Start Center by clicking:

Go To \rightarrow IT Infrastructure \rightarrow Provisioning Inventory \rightarrow Provisioning Computers.

We then filtered the Computer name to vmachine* as shown in Figure 17-15.

🥙 Provisioning Computers - Mozilla Fir	efox			
Eile Edit View History Bookmarks	<u>T</u> ools <u>H</u> elp			
🔇 🔊 • C 🗙 🏠 🔝	ibm.com https://risc40pa.rot.it.ibm.com:9443/maximo/ui/	(login	☆ •]	👌 Google
🙋 Most Visited 👯 Firefox Help 🔚 Firef	ox Support 🧦 Windows Live Hotmail 🗾 Plug-in FAQ ،	🖑 playonline.html 🛛 💇 Riepilogo de Il	mio eBay 🕐 Canon EOS 400D / Di 📄 Cor	tact Reference File >>
Provisioning Computers	*			
Provisioning Computers		C Web Replay Pulletins: (0)	▶ <u>G</u> o To Lut <u>R</u> eports III Start <u>C</u> enter III Profi	le [×] Sign Out ?Help IBM.
Find:	n v Select Action v 💽 🕄] @ \$ \$ \$		
List Computer Hardware	Software Compliance Recommendati	ions Credentials VVorkflov	vs Variables Deployment Properti	es
🖄 Advanced Search 🔻 🔒 Save Query	🔻 🛷 Bookmarks			
Computers 🛛 🔻 Filter > 🕅 🕴 🛊 🐐	⇔1-3 of3 →			Ely Download
Computer +	Operating System Glob	ally Unique Identifier	Agent	Compliance Status
vmachine*				
<u>vmachine4.rot.it.ibm.com</u>	Red Hat Enterprise Linux AS release 4 (Update 6)		TCA-1.3.2.29	No compliance checks configured
vmachine5.rot.it.ibm.com	Red Hat Enterprise Linux Server release 5.1		TCA-1.3.2.29	No compliance checks configured
vmachine8.rot.it.ibm.com	Windows Server 2008 Enterprise Edition		TCA-1.3.2.29	No compliance checks configured
Select Records				
-				
T				Þ

Figure 17-15 Provisioning Computers

Those system were Tivoli Common Agent installed in the Tivoli Provisioning Manager Version 5.1.1.2 server and now migrated into the Tivoli Provisioning Manager Version 7.1.1 provisioning database.

Restoring the 5.1.1.2 LDAP information to 7.1.1

This task is used to restore the 5.1.1.2 directory server user information to the 7.1.1 directory server.

Example 17-22 details the steps executed to perform this task.

Example 17-22 Restoring 5.1.1.2 directory server user information to the 7.1.1 directory server

Having configured the properties file to use a new LDAP by setting the ldapUseNew=new property, two files have been created by the tpm5112backup.sh script:

```
creation_LdapBackupNew.ldif
LdapBackupNew.ldif
```

Run these commands to migrate the 5.1.1.2 user information to the 7.1.1 directory server:

[tioadmin@risc40pa][/]> /opt/IBM/ldap/V6.2/bin/ldapmodify -a -D cn=root -w <password> -i /opt/IBM/tivoli/tpm/migration/backup/ldap/creation_LdapBackupNew.ldif

```
Operation O adding new entry cn=tioappadmin,ou=users,ou=SWG,o=IBM,c=US
```

Operation 1 adding new entry cn=sample:all-permissions,ou=groups,ou=SWG,o=IBM,c=US

```
[tioadmin@risc40pa][/]> /opt/IBM/ldap/V6.2/bin/ldapmodify -a -D cn=root
-w <password> -i
/opt/IBM/tivoli/tpm/migration/backup/ldap/LdapBackupNew.ldif
Operation 0 modifying entry cn=TPADMIN,ou=groups,ou=SWG,o=IBM,c=US
```

Changing user password

The tioappadmin has now been added to the 7.1.1 directory server database, but for security reasons, user passwords are not stored in the LDIF files.

The directory server Web interface cannot be used to change user passwords; Tivoli Directory Server provides a Web Administration Tool so that users can change their passwords. It is not installed by default.

Follow this link for details about how to install the Web Administration Tool:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic= /com.ibm.IBMDS.doc/install27.htm

Follow this link for details about how to use the Web Administration Tool:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic= /com.ibm.IBMDS.doc/install18.htm We used the Web Administration Tool installed on a different directory server in the same network, therefore we added a server from **Manage control servers**, and then provided to the Web Administration Tool the correct LDAP hostname and credential as shown in Figure 17-16.

🕹 IBM Tivoli Directory Serv	ver Web Administration - Mozilla Firefox
<u>File E</u> dit <u>V</u> iew Hi <u>s</u> tory	Bookmarks Iools Help
C ×	Ittp://timfive.rot.it.ibm.com:9080/IDSWebApp/IDSjsp/Login.jsp
🔎 Most Visited 🔅 Firefox He	elp 🔚 Firefox Support 🧳 Windows Live Hotmail У Plug-in FAQ 🖑 playonline.html 🖤 Riej
Start Center	🖂 😵 IBM Tivoli Directory Server Web 🔯 🔗
Tivoli Tivoli Director	ry Server Web Administration Tool
Directory server log	jin and a second se
Enter user name an	d password
LDAP Hostname:	risc40pa.rot.it.ibm.com:389
User DN:	cn=root
Password:	
Login	Login to Console admin

Figure 17-16 Web Administration Tool

To change the tioappadmin user password:

- 1. Expand Directory management.
- 2. Click Manage entries.
- 3. Expand the RDN o=ibm,c=us.
- 4. Expand the RDN ou=SWG.
- 5. Expand the RDN ou=users.
- 6. Select the tioappadmin used and click **Edit attributes**, as shown in Figure 17-17.



Figure 17-17 Changing tioappadmin user password

7. Then click **Next** and scroll down the attributes list until userPassword; insert the new password and click **Finish**.

Migrating access groups

To complete this task, synchronize the provisioning server and the LDAP server for the user and group information, and then run the TPM711Migration_Security workflow.

Here are the detailed steps:

- 1. From the provisioning server Web interface, click **Go To** → **System** Configuration → Platform Configuration → Cron Task Setup.
- 2. In the Cron Task field type VMMSYNC and press enter.
- 3. Click VMMSYNC.
- 4. To activate the synchronization select **Active** in the Cron Task Instances and save the changes, as shown in Figure 17-18.

e Edit View History Bookmarks Tools Help		
🕢 🕞 C 🗙 🏠 🚺 ibm.com https://risc40pa.rot.il	ibm.com:9443/maximo/ui/login	🟠 🔹 🎦 🖥 Google
Most Visited 🔆 Firefox Help 🔚 Firefox Support 🧳 Windows Live I	Hotmail 💆 Plug-in FAQ 🦃 playonline.html 🐠 Riepilogo de Il mio 🕫	aBay 🐵 Canon EOS 400D / Di 📄 Contact Reference File
Cron Task Setup		
🗊 Cron Task Setup	🕑 Web Replay 🛛 🕴 Bulletins: (0) 🖗 💁	To Lut Reports P Start Center Profile Sign Out ? Help IE
Y Find: Select Action		
ist Cron Task		
	Save Cron Task Definition CTRL+ALT+5	
Cron Task VMMSYNC Invokes Web	Sphere VMM APIs to populate dat	
Class psdi.security.vmm.VMMSyncCronT	ask	
Access Level FULL		
on Task Instances i Eilter Millia a i a 1, 1 of 1 a		Ri Download 12
Cron Task Instance Name Schedule	Run as User	Active Keep History Max Number of History Records
VMMSYNC01 5m.********	MAXADMIN 2	
		Duplicate New Row
Derometere		
Cron Task Parameters 🛛 🕨 Filter > 🚳 🛛 😂 🍦 🔶 🔶 🔶 🕹 🕹		E9 Download ?
Parameter ≑	Value	Description
Credential		VMM admin credentials.
GroupMapping	xml version="1.0" encoding="UTF-8" ? DO</td <td>The USER XML used by the VMM task.</td>	The USER XML used by the VMM task.
GroupSearchAttribute	cn	VMM search attribute to query group records.
Principal	cn=wasadmin,ou=users,ou=SWG,o=IBM,c=US	VMM admin principal.
SynchAdapter	psdi.security.vmm.DefaultVMMSyncAdapter	VMM synchronization adapter.

Figure 17-18 Activate VMM synchronization

5. Add this line in the maximo.properties file:mxe.crontask.donotrun=ALL Example 17-23 details the steps to modify the file.

Example 17-23 maximo.properties file modification

Save the current maximo.properties file by running:

[root@risc40pa][/opt/IBM/SMP/maximo/applications/maximo/properties]> mv
maximo.properties maximo.properties.090824

Copy the /opt/IBM/SMP/etc/maximo.properties_orig file into the /opt/IBM/SMP/maximo/applications/maximo/properties as maximo.properties by running:

[root@risc40pa][/opt/IBM/SMP/etc]> cp maximo.properties_orig
/opt/IBM/SMP/maximo/applications/maximo/properties/maximo.properties

Add the following line to the maximo.properties file:

mxe.crontask.donotrun=ALL

Encrypt the file by running:

[root@risc40pa][/opt/IBM/SMP/maximo/tools/maximo]> encryptproperties.sh

Copy the encrypted file into
\$TIO_HOME/lwi/runtime/tpm/eclipse/plugins/tpm_pmp/properties by
running:

[root@risc40pa][/opt/IBM/SMP/maximo/applications/maximo/properties]> cp
maximo.properties
\$TI0 HOME/lwi/runtime/tpm/eclipse/plugins/tpm pmp/properties

Stop and restart the Tivoli Provisioning Manager Version 7.1.1 by running **tio.sh stop wasadmin <password>** followed by **tio.sh start**.

- 6. To run the TPM711Migration_Security workflow, click Go To \rightarrow Administration \rightarrow Provisioning \rightarrow Provisioning Workflows.
- 7. In the Provisioning Workflow field search for the TPM711Migration_Security workflow.
- 8. Click the TPM711Migration_Security workflow.
- 9. From the Workflow tab in the Select Action list select Run Workflow.
- 10. From the Run Workflow tab select Run.

11.Click Yes in the System Message tab.

You can check the workflow task execution by looking at the Provisioning Task Tracking, as shown in Figure 17-19.

Provisioning Task Tracking - Mozilla	Firefox							- 1012
<u>File Edit View History Bookmarks</u>	Tools Help							
🚱 🖓 • C 🗙 🔬 🔯	ibm.com https://risc40pa.rot	.it.ibm.com:9443/maximo/ui/lo	ogin			ជ	Soogle	P
🔎 Most Visited 👯 Firefox Help 🔚 Firef	iox Support 🏘 Windows Live	e Hotmail 🗾 Plug-in FAQ 🦑	🖇 playonline.html 🛯 💩 Riepil	ogo de Il mio eBay Ø	Canon EOS 400D	/ Di 🎽 Con	itact Reference File	>
Provisioning Task Tracking	÷							
Provisioning Task Tracking							<u> <u> </u> - <u> </u> <u> </u> <u> </u> - </u>	IEM.
Find:	🔥 🤜 Select Action	× 🕄 🗟 🖉	4					
Provisioning Task Run provisioning we Type Provisioning Workfle Created By MAXADMIN Changed By	arkflow TPM711Migration_S aw	Run provisioning workflov	w TPM711Migration_S	Base S	Definition R Start Date 8/ End Date 8 Status S Services Task	un provisioning /24/09 6:19 PM /24/09 6:20 PM juccess	workflow TPM711Migration_	
Provisioning Workflows 🕴 Filter > 🚳	1214 4141.1 of 1 + 1				_		Status: Success	load ? =
Provisioning Workflow	Status		Start Date	End Date	Conc	surrency Level	Subtask	
TPM711Migration_Security	Succeeded	/	8/24/09 6:19 PM	8/24/09 6:20 PM		5	TPM711Migration_Secur	ity
Notification								-
Recipients Filter > A 2 + + + + +	**							010 3 5
Neupieni			No rows to display					
Events > Filter > A 2 + + + + +							Down	ioad ? 📼
Event Type								
			No rows to display					
Provisioning Workflows > Provisioning Task	Tracking							

Figure 17-19 TPM711Migration_Security workflow task status

You can now log into the provisioning Web interface using the tioappadmin user.

🖏 Start Center - Mozilla Firefox						_ [0] :
Eile Edit View History Bookmarks Tools Help						
	Dpa.rot.it.ibm.com;9443/maximo/ui/login			<u>ح</u> ر ،	Google	L.
	epan ocnenen noon in Proprio anino papagan		-		loogo	
🖉 Most Visited 🔅 Firefox Help 🔚 Firefox Support 🧳 Wind	ows Live Hotmail 💆 Plug-in FAQ 🤌 p	olayonline.html 🐠 Riepilogo d	e Il mio eBay 😢 Canon	EOS 400D / Di 🔄 C	iontact Reference File	
Start Center						
Welcome, tioappadmin		Web Replay 🤚 <u>B</u> ulletins: (0)	🥐 <u>G</u> o To 🕮 <u>R</u> eports	ta Start <u>C</u> enter ▲ Pro	ofile × Sign Out ? <u>H</u> el;) IRM.
	🔡 Change Content/L	ayout 📲 Display Settings	Reate New Temp	late 🛛 🔏 Modify Existi	ing Template 🛛 🖓 🖓 Upda	te Start Center 📥
Inbox / Assignments 🥒 🗖 👔	🔒 Bulletin Board 🛛 🔻 Filter 🖓 🌍					T
Refrest	Subject Messag	e Post Date	Expira	ation Date	Viewed?	
Description Due Date Route					N	
No Assignments found for tioappadmin		These are concerned	ku na kullatin kanad wana	ana ta ulaur		
F	3	There are curren	uy no bulletin board niess	ages to view.		
ravorite applications 70 a	My favorite reports 🛛 🔻 Filter > 🚜	12 10				/01
Provisioning Computers						
	Successful, failed and in-progres	ss provisioning tasks				
Virtualization Management						
•••	All recent provisioning tasks 🛛 🔻	Filter>d 🛍 🔝 🖗				
Software Products	Agents status					/00
Patches	Software distribution infrastruct	ure communication status				200
Brouisioning Task Tracking	Denot status					
	Data model object finder 💎 Filter	()@a [⊅ [@				/ = @
Provisioning administration applications 🛛 🖉 🗖 👔	Object	Contractory of the second s		Object Type		
H Provisioning Groups						
	Default Device Model			Device Driver		
Station in the second s	AIX Computers			Computer Group		
Provisioning Permission Groups	Red Hat Linux Computers			Computer Group		
c = 1	HPUX Computers			Computer Group		
Provisioning Global Settings	Set Graph Options				1 - 5 of 1200	Next Page >>
Provisioning Workflows						
w anic content beivery configuration						
Work Order Tracking						
Activities and Tasks						-
а а					*//	· F

Figure 17-20 shows the tioappadmin user Start Center after a successful login.

Figure 17-20 tioappadmin user Start Center

Backing up the database

Now that the installation has completed successfully, you might want to back up the 7.1.1 database.

You can use your own backup tool or use the information provided in this link:

https://www.ibm.com/developerworks/wikis/display/tivoliprovisioningmana
ger/Backing+up+the+database+and+important+data

Migrating dynamic groups

When you migrate the dynamic groups from 5.1.1.2 to version 7.1.1, the dynamic groups are available, in the Provisioning Groups application, and have all of their parameters but they have no content because they have lost the query that they were originally linked to.

You can list them by navigating the provisioning Web interface, clicking Go To \rightarrow Deployment \rightarrow Provisioning Groups.

The Group Type column reports Dynamic or Static based on the group type. As you can see in Figure 17-21, the Query field is empty.

🥙 Provisioning Groups - Mozilla Firefox			>	×
<u>File Edit View History Bookmarks Tools H</u> elp				
C 🗙 🔂 陆 C 🔀	40pa.rot.it.ibm.com:9443/maximo/ui/login		🔝 🗸 🔀 Google 🖉	j
🔊 Most Visited 🔆 Firefox Help 🔚 Firefox Support 🧳 Wind	dows Live Hotmail 💆 Plug-in FAQ 🦑 playonline.html	🐠 Riepilogo de Il mio eBay 🕐 Canon EOS 400D /	Di 📋 Contact Reference File 3	»»
Provisioning Groups				-
Provisioning Groups	C Web Replay	Bulletins: (0) A Go To LA Reports A Start Go	enter ² Profile ^X Sign Out ? Help <u>IBM</u> ,	-
Find:	ct Action 🔽 👀 🚺 🗟 🗶 🍬 💠			
List Group Compliance Recommendation	is Variables			
Group * AIX Computers	Computers running the AIX operating system	Member Type Computer	Is Untyped Group?	
Group Type Dynamic Query *	D	Source Local Group		
Members i Filter i + + i ++			🕞 Counicas ? 🗖	
Name	Member Type			
	No rows to dis	play		
			Copy Members to Static Group	
Groups				
AIX Computers Group Me	embership 🕨 Filter > 🙈 🗊 🛉 🛊 🚸 🌩	Manchasa Tuna	ix Download ? 🖻	
Dem Object		No rows to display		

Figure 17-21 Dynamic groups

The structure of dynamic groups in version 5.1.1.2 changed with the version 7.1.1 where the dynamic groups rely on the base services queries that embed the SQL needed to retrieve the data dynamically. The base services queries are based on the application object so, the queries can only be created for objects that have an associated application.

After a query is created, it is available for the dynamic group through the Provisioning Groups application. Dynamic groups can only be associated to these queries; they can no longer be associated to any SQL-based queries, as they were in version 5.1.1.2. The 5.1.1.2 QUERY table was renamed to QUERY5112 during the migration and all of the content was saved.

Example 17-24 shows how to retrieve the query information by using the content of QUERY5112 table in the database.

Example 17-24 Retrieving 5.1.1.2 dynamic group query

You can retrieve the query information by runnig an sql as described below:

```
- su - tioadmin
```

- db2 connect to maxdb71 user maximo using <password>

Create an SQL file containing these lines:

```
SELECT CASE
WHEN Q.EDITED_QUERY is not null then Q.EDITED_QUERY
ELSE Q.QUERY_STRING
END query
FROM QUERY5112 Q, DCM_OBJECT 0, BASIC_GROUP G
WHERE 0.NAME='<dynamic_group_name>'
AND Q.QUERY_ID=G.QUERY_OBJECT_ID and G.GROUP_ID=0.ID;
```

```
We substituted the 0.NAME='<dynamic_group_name>' with 0.NAME='Windows
Computers'.
The query returns:
```

```
SELECT server_info_view.SERVER_NAME
FROM server_info_view
WHERE (server_info_view.OS_NAME LIKE '%Win%')
ORDER BY server info view.SERVER NAME
```

```
so the query uses server_info_view.OS_NAME LIKE '%Win%' to populate the dynamic groups where:
server_info_view corresponds to the Provisioning Computers application and OS_NAME LIKE '%Win%' identifies the filter information.
```

After you have identified the filter information, you can create the query:

- 1. To navigate the Web interface, click Go To \rightarrow Deployment \rightarrow Provisioning Computers.
- 2. In the Operating System field insert the filter (Win%) identified in Example 17-24 on page 654.
- 3. The Windows Computers are listed.

- 4. Click **Save Query** to store the filter as a query. You have to provide a query name.
- 5. Associate now the saved query to the Provisioning Group Windows Computers. See Figure 17-22.

😢 Provisioning Groups - Mozilla Firefox					<u>- 0 -</u>
Eile Edit View History Bookmarks Tools Help					
C X 🟠 🖿 Ktps:/	/risc40pa.rot.it.ibm.com:9443/maximo/	/ui/login		☆ ·	Soogle 🔎
应 Most Visited 🔆 Firefox Help 🔚 Firefox Support 🧳	Windows Live Hotmail 💹 Plug-in FAC	Q 🖉 playonline.html 🐠 Riej	pilogo de Il mio e	eBay 🙋 Canon EOS 400D / Di 📔 Co	ntact Reference File >
Provisioning Groups					
Provisioning Groups		🕞 Web Replay 🛛 🔒 <u>B</u> ullet	ins: (0) 🛛 🧖 <u>G</u> o	To IIII Reports 🏶 Start Center 🌲 Pro	file X Sign Out ? Help IRM.
Find:	Select Action 🛛 🔽 🚯 🗍				
List Group Compliance Recommenda	ations Variables	Save Provisioning Group	CTRL+ALT+S		
Group · Windows Computers	Computers running the Windo	ows operating sys	Member Type	Computer	Is Untyped Group?
Group Type Dynamic			0	Local One	
Query Vindows_Computers	P		Source	Local Group	
Members > Filter > 3% 🔤 + + + + + + + + + + + + + + + + + +					E→ <u>Download</u> ? =
Name vmachine8.rot.it.ibm.com				Computer	
					Copy Members to Static Group
Groups					
🖬 Windows Computers	Group Membership 🗄 🕨 Filter 🔊				🗈 Download 🔅 📼
	Dcm Object		Membe	ers Type	
			No rows t	to display	
I					

Figure 17-22 Windows Computers dynamic group

The query is now associated to the dynamic group and it contains the Windows Provisioning Computers.

17.9 Post-migration tasks

This section provides a list of post-migration tasks that must be executed on the Tivoli Provisioning Manager Version 7.1.1 provisioning server.

The task list includes:

- Backing up the administrative workstation
- Configuring SSL with IBM HTTP Server
- Using the Tivoli Monitoring agent

These tasks are described next.

17.9.1 Backing up the administrative workstation

The administrative workstation is not required to be active for the Tivoli Provisioning Manager Version 7.1.1 operations.

It is used to install:

- Product patches or upgrades
- New applications
- New process managers
- Additional language packs

We recommend that you back up the administrative workstation so that the settings can be restored if needed.

In the environment used for this Redbooks publication, we installed the administrative workstation on the same system as the Tivoli Provisioning Manager Version 7.1.1 server, having used an Operating System that supported the local administrative workstation installation, AIX 6.1.

Example 17-25 details the steps you have to run to back up an administrative workstation on AIX 6.1.

Example 17-25 Backing up the administrative workstation

To backup the administrative workstation, you have to backup the Web components and base services by running the de_backupdb script as detailed below:

[root@risc40pa][/usr/ibm/common/acsi/bin]> de_backupdb -bfile /adm_wks_backup/DE_BACKUPS/AFTER_INSTALL_PMP_7.1.1.0

Backing up database to

/adm_wks_backup/DE_BACKUPS/AFTER_INSTALL_PMP_7.1.1.0; please wait ... Request completed successfully.

You should now backup the deployment directory. In the following example we created a tar archive of the /opt/IBM/SMP directory.

[root@risc40pa][/opt/IBM/SMP]> tar cvf /adm_wks_backup/opt_IBM_SMP.tar
./*

17.9.2 Configuring SSL with IBM HTTP Server

After Tivoli Provisioning Manager installation, IBM HTTP Server SSL is not configured, and on UNIX installations, the root user runs the HTTP server. You can optionally configure the server to run as tioadmin user on UNIX and configure SSL communication with IBM HTTP Server. After this configuration, you can use an external HTTP server to access the provisioning server Web user interface.

To configure the HTTP server to run as tioadmin user, follow the steps outlined in Example 17-26.

Example 17-26 Running HTTP server as tioadmin

To configure IBM HTTP Server to run as tioadmin user, make sure the user has access to these directories:

/usr/IBM/HTTPServer/Plugins/config/webserver1
/usr/IBM/HTTPServer/logs

Set these directories permisison to 777 by running these commands:

[root@risc40pa][/usr/IBM/HTTPServer]> chmod -R 777 Plugins logs

Considering the listening port must be greater than 1024 for a non-root user to bind, change the default non-secure port 80 to 8080 (or any other value greater than 1024 and not used by other processes) by commenting the Listen 80 and adding a Listen 8080 entry in the /usr/IBM/HTTPServer/conf/httpd.conf file

You can now restart the HTTP server as tioadmin user and verify from the ps output the succesfull startup:

[tioadmin@risc40pa][/usr/IBM/HTTPServer/bin]> apachectl start [tioadmin@risc40pa][/usr/IBM/HTTPServer/bin]> ps -ef|grep HTTP tioadmin 159788 741552 0 11:17:00 - 0:00 /usr/IBM/HTTPServer/bin/httpd -d /usr/IBM/HTTPServer -k start tioadmin 647406 741552 0 11:17:00 - 0:00 /usr/IBM/HTTPServer/bin/httpd -d /usr/IBM/HTTPServer -k start tioadmin 741552 1 0 11:16:59 - 0:00 /usr/IBM/HTTPServer/bin/httpd -d /usr/IBM/HTTPServer -k start

```
tioadmin 770230 741552 0 11:17:00 - 0:00
/usr/IBM/HTTPServer/bin/httpd -d /usr/IBM/HTTPServer -k start
tioadmin 778446 741552 0 11:17:00 - 0:00
/usr/IBM/HTTPServer/bin/sidd
tioadmin 786440 790748 0 11:17:43 pts/1 0:00 grep HTTP
```

Now that the HTTP server is configured to run as tioadmin user, you have to configure SSL and perform these steps on the HTTP server side:

- 1. Create an HTTP Server CMS keystore file.
- 2. Enable SSL directives in the IBM HTTP Server httpd.conf configuration file.
- 3. Restart the HTTP server.
- 4. Configure the Web server plug-in for Secure Sockets Layer.

Other steps need to be executed on the WebSphere Application Server side:

- 5. Add HTTP port to maximo host virtual host.
- 6. Modify CTG_MAXIMO_SERVLET_URL variable.
- 7. Restart the MXServer application server.

In the following sections we describe these steps in detail.
Create an HTTP Server CMS keystore file

Before creating the CMS keystore, you can create a path on the provisioning server to store both the keystore and the self-signed certificate (/opt/IBM/tivoli/tpm/cert/keys in our example)

To create the CMS keystore:

- 1. Open the HTTP server ikeyman utility from /usr/IBM/HTTPServer/bin directory
- 2. Click Key Database File \rightarrow New.
- 3. Select **CMS** as **Key database type** and enter the **File Name** and the **Location**, as shown in Figure 17-23. We called it TPM711.kdb.

B-Type:			
le Name:			
oken Lab	dt		
	Key database content		
ersonal (ertificates	Rec	eive
		De	elete
		View	//Edit
		Im	port
	● Untitled	Recreate	Request
	Key database type CMS 💌		
	File Name: TPM711.kdb Browse		
	Location: /opt/IBM/tivoli/tpm/cert/keys/		
	OK Cancel		

Figure 17-23 Creating the keystore

4. Provide the keystore password and select **Stash the password to a file?** check box in the next panel.

Note: The password you specify in this step must match the Tivoli Provisioning Manager Keystore that was used at 5.1.1.2 installation time.

Enable SSL directives in the IBM HTTP Server httpd.conf

To configure the IBM HTTP Server to enable SSL, follow the steps outlined in Example 17-27.

Example 17-27 enable SSL directives in the IBM HTTP Server httpd.conf file

Add these lines into the /usr/IBM/HTTPServer/conf/httpd.conf file: LoadModule ibm_ssl_module modules/mod_ibm_ssl.so <IfModule mod_ibm_ssl.c> Listen 1976 <VirtualHost *:1976> SSLEnable </VirtualHost> </IfModule> SSLDisable KeyFile "/opt/IBM/tivoli/tpm/cert/keys/TPM711.kdb"

The listening port is greater than 1024 to allow tioadmin or any other non-root user to start the IBM HTTP Server.

Stop and start the Web server by running:

/usr/IBM/HTTPServer/bin/apachectl stop /usr/IBM/HTTPServer/bin/apachectl start

Configure the Web server plug-in for Secure Sockets Layer

The following link to the WebSphere Application Server documentation details the whole procedure to follow to successfully configure the Web server plug-in for Secure Sockets Layer:

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/ com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/tsec_httpserv.html

Some of the steps described in the foregoing documentation were not necessary for the environment used for this Redbooks publication, because the Tivoli Provisioning Manager performs them at installation time.

All the steps are listed next, following the same order as described in the WebSphere documentation. Comments are added for those steps that you are not required to perform:

1. Create a self-signed personal certificate.

In this step you are required to create a CMS keystore, but it has been already created in the previous step and it is called TPM711.kdb.

Note: You do not need to create the self-signed certificate and extract it. These operations were performed by the Tivoli Provisioning Manager installation.

2. Generate a self-signed certificate for the Web container.

Note: You do not need to run this step. The Web container, referenced as WasWebContainer.jks, was created by the Tivoli Provisioning Manager installation and it is called tpmTrustStore.jks.

The self-signed certificate, referenced as WASWebContainer, was created by the Tivoli Provisioning Manager installation and it is called tpmui.cer

3. Exchange public certificates.

This step is not required if the WebSphere Application Server and the Web server are installed on the same system.

- 4. Import the certificate into the Web server plug-in key file.
 - a. Open the CMS keystore previously created.
 - b. Select Signer Certificate from Key Database content frame and click Add.
 - c. Select Base64-encoded ASCII data as Data type and enter tpmui.cer in the **Certificate file name** and /opt/IBM/tivoli/tpm/cert in the **Location** fields as shown in Figure 17-24.

		Key database information	
DR Turner CMC I	a databasa fila	,	
DB-Type. CM3 K	ey uatabase me	- 77047344 ().	
ne Name: 70pt/1	BM/tivoli/tpm/tert/key	SYTEM / II. Kub	
loken Label:			
		Key database content	
Signer Certificates			▼ Add
Entrust net Global	Secure Server Certific	ation Authority	Delate
Entrust.net Global	Client Certification A	uthority	Delete
Entrust.net Client (Certification Authority		View/Edit
Entrust.net Certific	ation Authority (2048		
Entrustinet Secure	Server Certification A	uthority	Extract
VeriSign Class 3 St	uhlic Primary Certifica	tion Authority	
VeriSign Class 2 Pu	ublic Primary Certifica	tion Authority	
VeriSign Class 1 Pu	ublic Primary Certifica	tion Authority	
VeriSign Class 4 👔	Untitled		1 E
VeriSign Class 3	Data tura		
VeriSign Class 2	Data type	Baseb4-encoded ASCII data	
VeriSign Class 4	Certificate file name:	tpmui.cer	Browse
VeriSign Class 3			
VeriSign Class 2	Location:	/opt/IBM/tivoli/tpm/cert/	
VeriSign Class 1			
Thawte Personal		OK Cancel	
Thawte Personal R	asic CA		
Thawte Premium S	erver CA		
Thousan Common CA			
Thawle Server CA	Certification Authority	/	
RSA Secure Server			
RSA Secure Server			
RSA Secure Server			

Figure 17-24 import tpmui.cer

- d. Enter a label for the certificate. We used WASWebContainer. This represents the trusted signer public certificate.
- 5. Import the certificate into the Web container keystore file.

Note: This step is not required. It was performed by the Tivoli Provisioning Manager installation, but you have to associate the Web container tpmTrustStore.jks to the CMS keystore TPM711.kdb

- 6. To associate the tpmTrustStore.jks to the CMS keystore TPM711.kdb:
 - a. Open the CMS keystore previously created.
 - b. Import the self-signed certificate by selecting **Personal Certificate** from **Key Database content** frame and click **Import**.
 - c. Select **JKS** as **Key database type** and enter tpmTrustStore.jks in the **File Name** and /opt/IBM/tivoli/tpm/cert in the Location, as shown in Figure 17-25.

-			Nev database information	
I-Type: CMSK	ey database file		,	
e Name: /opt/l	BM/tivoli/tpm/cen	t/keys/TPM711.kdb		
ken Label:				
			Key database content	
ersonal Certificat	25			 Receive
				Delete
				Delete
				View/Edit
				Export/Import
				Recreate Request
	Untitled			<u>ف</u>
	Key file type	JKS 🔻		
	File Name:	tomTrustStore_iks		Browse
	Location:	/opt/IBM/tivoli/tpm/cert/	·	
			OK Cancel	

Figure 17-25 Import Web Container truststore

- d. Provide the password that was used at 5.1.1.2 installation time.
- e. Select **tpmuicert** from the key list and click **OK**. We changed the label to WASplugin.
- 7. Modify the Web container to support Secure Socket Layer (SSL):

The steps for the JSSE repertoire were already completed during Tivoli Provisioning Manager installation.

The next steps are performed in the WebSphere Application Server administrative console.

8. Logon to the console by opening this URL:

http://<your_was_hostname>:9060/ibm/console

Provide wasadmin user and password credentials to log in.

Continue the procedure with the following steps.

- 9. Modify the Web server plug-in:
 - Click Servers \rightarrow Web servers \rightarrow webserver1.
 - Under Additional Properties select Plug-in properties → Custom Properties.
 - Click New, enter KeyringLocation in the Name field and/opt/IBM/tivoli/tpm/cert/keys/TPM711.kdb in the Value field and click OK.
 - Click New, enter StashfileLocation in the Name field and /opt/IBM/tivoli/tpm/cert/keys/TPM711.sth in the Value field and click OK.
 - Click Save to save the changes. Figure 17-26 shows the final result of this step.

Provisioning Groups	EINECO: Conto, Inves		Ston Internal Server Error	WebSohere Application S	Integrated S
Integrated Calutions Cancels	I INCCO. Conto, Inves	Incip system		webspilere Application 5	
integrated Solutions Console w	veicome wasadmin			Help Logout	
View: All tasks					Ŀ
Welcome Mu Startup Dages	Web	servers			
FI Guided Activities	Wel	servers			? – Help
Servers					Field
Application servers		Veb servers > webserver1 > Pi	ug-in properties > Custom Properties		For f
Generic servers	F	roperties.	te pair. The value is a soring that can set	ncernal system comgoration	mark
Proxy Servers Version 5 IMS servers	В	Preferences			curse
Web servers		Nev Delete			Page
Clusters		D D # 9			this
Generic Server Clusters			Value O	Description O	
WebSphere MQ servers		E Kowiel ocation	/opt/TRM/twoll/tors/cost	Description C	
H Core groups	1		/keys/TPM711.kdb		
Applications		StashfileLocation	/opt/IBM/tivoli/tpm/cert /keys/TPM711.sth		
Resources		Total 2			00005
E Security					
Environment		~			
System administration					
Osers and Groups					
Traublachasting					
Service integration					
E bervice integration					
CE LIDDI					

Figure 17-26 Modify Web server plug-in

10. Access the Web server plug-in from the Web Server:

This step is not required if the WebSphere Application Server and the Web server are installed on the same system.

Note: Steps 9 and 10 can be delayed because other changes need to be performed on the WebSphere Application Server.

- 11.Restart the application server.
- 12. Test the connection.
- 13. Import the correct certificate with public and private keys into the browser. This step is optional; it has not been performed because we skipped step 6.

Add HTTP port to maximo_host virtual host

With this step you add the HTTP server SSL port defined before (port 1976) to the WebSphere Application Server.

- 1. Click Environment \rightarrow Virtual Hosts \rightarrow maximo_host \rightarrow Host Aliases.
- 2. Click **New** and specify * in the **Host Name** field and 1976 in the **Port** filed to match the HTTP server SSL configuration. The panel in Figure 17-27 is shown.

Provisioning Groups Frovisioning Groups Provisioning Groups Provisioning Groups Provisioning Groups Provisioning Provisio	p, jrvestm	seo of the system (DNS) alias by which the virtual host is known.	Integrated Solutions
Integrated Solutions Console Welcome weardmin Views [All tasks Welcome My Startup Bages G Guide Activities G Sarvers Applications Resources Security E Environment	Virtual Hosts Virtual Hosts Virtual Hosts > maximo_host > Host Ali Use bis page to add, create, or delete a Preferences	Help Logout	Help Field help
Walcome My Starup Page Goided Activities Sarvers Applications Resources Security Environment	Virtual Hosts Virtual Hosts > maximo host > Host Ali Use this page to edit, create, or delete a Preferences	ases • domain name system (DNS) alias by vhich the virtual host is known.	Help Field help
My Startup Pages () Guided Activities () Applications () Resources () Security E Environment	Virtual Hosts Virtual Hosts > maximo_host > Host Ali Use this page to adit, create, or delete a Preferences	ases • domain name system (DNS) alias by vhich the virtual host is known.	- Help Field help
Severs Severs Severs Security	Virtual Hosts > maximo_host > Host Ali Use this page to edit, create, or delete a ☐ Preferences	ases 1 domain name system (DNS) alias by which the virtual host is known.	Field help
Applications Resources Security Exervity	Virtual Hosts > maximo host > Host Ali Use this page to edit, create, or delete a	ases a domain name system (DNS) alias by which the virtual host is known.	rield help
Resources Security Environment	Preferences	a uomani name system (UNS) allas by which the virtual host is known.	For field help in
Environment			select a field lab marker when the
Environment	New Neise		cursor appears.
	Nev Delete		Page help More informatio
Virtual Hosts	00 # 2		this page
 Update global Web server plug-in configuration 	Select Host Name 🗢	Port 🗘	
WebSphere Variables		9443	
Shared Libraries		1976	
 Replication domains URI Groups 	Total 2		
⊞ Naming			
System administration			
E Users and Groups	ľ		
Monitoring and Tuning			
Troubleshooting			
E Service integration			
I UDDI			
Settings			

Figure 17-27 Host Aliases

Modify CTG_MAXIMO_SERVLET_URL variable

The last step in the procedure before the Application server restart is the modification of the *CTG_MAXIMO_SERVLET_URL* variable:

- 1. Click Environment → WebSphere Variables → CTG_MAXIMO_SERVLET_URL.
- 2. Fill the Value field with http://<your_host_name>:1976/maximo/ui/.

Restart the MXServer

To restart the Application server:

- 1. Click Servers \rightarrow Application servers.
- 2. Select the MXServer, then Stop and Start.

You can now test the connection using the SSL port 1976 by opening this URL:

http://<your_host_name>:1976/maximo

You are first asked to trust the certificate. After it is trusted, you have to provide the credentials: You can use the default maxadmin user and maxadmin password.

🖏 Integrated Solutions Console - Mozilla Firefox _ 🗆 🗵 File Edit View History Bookmarks Tools Help 🔇 🔊 - C 🗙 🏠 🗋 ibm.com https://risc40pa.rot.it.ibm.com:9043/ibm/console/secure/securelogon.do ☆ • 🚷 Google ø 🧕 Most Visited 🔆 Firefox Help 🔚 Firefox Support 🧳 Windows Live Hotmail 💁 Plug-in FAQ 😓 playonline.html 💇 Riepilogo de Il mio eBay 🗶 Canon EOS 400D / Di... 🗋 Contact Reference File Provisioning Groups FINECO: Conto, Investim... 🗵 help system 300 Internal Server Error 📧 🚥 WebSphere Application S... Integrated Solutions Integrated Solutions Console Welcome wasadmin Help Log IBM View: All tasks -Welcome Virtual Hosts Close page My Startup Pages 🗄 Guided Activities Virtual Hosts + Servers Field help <u>Virtual Hosts</u> > <u>maximo_host</u> > Host Aliase For field help information select a field label or list marker when the help cursor appears. + Applications Use this page to edit, create, or delete a domain name system (DNS) alias by which the virtual host is known Resources Preferences F Security New Delete Page help Environment More information about this page 00 # 4 Virtual Hosts Update global Web server plug-in Select Host Name 🛟 Port () configurat WebSphere Variables □ 1 9443 Shared Libraries □ ± 1976 Replication domains LIRI Groups Total 2 Naming System administration R I Users and Groups H Monitoring and Tuning Troubleshooting H Service integration UDDI 🕀 Settings × Find: 🐥 Next 👚 Previous 🖌 Highlight all 🔲 Match case 🕚 🔿 5 Now: Mostly Sunny, 29 °C 🖄 Tue: 29 °C 🥙 Wed: 30 °C 🖄 Thu: 29 °C 🖄 Fri: 30 °C 🏩 Sat: 29 °C 🖄 Sun: 27 °C 🧞 Done

The Start Center is shown in Figure 17-28.

Figure 17-28 Start Center using the SSL port 1976

Other post-migration tasks can be executed based on the Tivoli Provisioning Manager Version 5.1.1.2 provisioning server customization. Not all of them have been executed in our environment, therefore they are only mentioned here for completeness.

Important: For details about any of the following tasks, refer to the *Tivoli Provisioning Manager Version 7.1.1 Migration Guide* at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ib m.tivoli.tpm.ins.doc/tpm_migrate_guide.pdf Here is a complete list of the tasks:

Restoring WebSphere Application Server settings.

This step is only required if you customized any configuration in the 5.1.1.2 application server.

• Configuring the provisioning server for integration with other products.

This step is only required if you want to integrate Tivoli Provisioning Manager Version 7.1.1 with Service Request Manager or Change and Configuration Management Database (CCMDB). If so some configurations are required.

We did not perform this step.

Recreating custom roles.

This step is only required if you created custom roles for you 5.1.1.2 provisioning server

 Recreating Tivoli Provisioning Manager for OS Deployment Embedded Edition images.

There is no migration for the images created with Tivoli Provisioning Manager for OS Deployment Embedded Edition 5.1.1.2. If you recaptured the 5.1.1.2 images using a 7.1.1 test provisioning server before the migration, you can clone them to the 7.1.1 production server. We did not have any image created at 5.1.1.2, therefore we did not perform this task.

Migrating TADDM GUIDs.

This step is only required if you imported TADDSM data in your 5.1.1.2 provisioning server.

Importing the SSL certificates for VMware.

This step is only required if you discovered host platform servers and virtual servers in your 5.1.1.2 provisioning server.

Restoring and removing automation packages.

This step is only required if you created custom automation packages in 5.1.1.2 that you backed up before the migration. Also, if there are 5.1.1.2 automation packages that were deprecated during the migration, download them from OPAL, and install them on the 7.1.1 provisioning server.

Restoring local file repositories.

This step is required to recreate the 5.1.1.2 file repositories on the 7.1.1 provisioning server

► Recreating compliance information.

Compliance checks, and the related scheduled scans, are migrated to version 7.1.1. The compliance status and the information about the last scan is not migrated. After the migration, run compliance checks on the target computers, or groups or target computers, to populate the recommendations and update the compliance state in the 7.1.1 provisioning server.

Recreating custom reports.

This step is only required if you created custom reports in your 5.1.1.2 provisioning server. Tivoli Provisioning Manager Version 7.1.1 replaced Alphabox technology with Business Intelligence and Reporting Tools (BIRT) designer, the new reporting technology used by Tivoli. The BIRT Report Engine is embedded in the Tivoli Process Automation Platform. All Tivoli Process Automation Platform products share an instance of the BIRT runtime. Reports in BIRT are created using the BIRT Report Designer and then imported into the Tivoli Process Automation Platform.

Migrating inventory extensions.

This step is only required if you created custom inventory reports in your 5.1.1.2 provisioning server.

Activity plan and endpoint tasks.

This step is only required if you created activity plans and endpoint tasks in your 5.1.1.2 provisioning server. These might be migrated to the MAXADMIN user.

Note: For a comparison of GUI differences between Tivoli Provisioning Manager Version 5.1.1.2 and Tivoli Provisioning Manager Version 7.1.1, you can refer to 6.7, "Overview of the GUI differences" on page 167.

670 IBM Tivoli Provisioning Manager V7.1.1: Deployment and IBM Service Management Integration Guide

Α

Miscellaneous upgrade scenarios

In this appendix, you can find information about the following topics:

- "Upgrade to Tivoli Provisioning Manager V7.1.1 and Tivoli CCMDB V7.1.1.5" on page 672
- "Upgrade to Tivoli Provisioning Manager V7.1.1 and Tivoli Service Request Manager V7.1.0.4" on page 674
- "Integration between Tivoli Provisioning Manager V7.1.1 and IBM Tivoli Asset Management for IT V7.1.0.5" on page 678

Important: The information listed here does not replace that available in the official documentation. To get detailed instructions for installing and using each Tivoli product involved in the integration scenarios, refer to the Tivoli Provisioning Manager V7.1.1 InfoCenter at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp

Upgrade to Tivoli Provisioning Manager V7.1.1 and Tivoli CCMDB V7.1.1.5

In this topic you can find the sequence of steps to upgrade a pre-existing Tivoli Provisioning Manager and Tivoli CCMDB integration to Tivoli Provisioning Manager 7.1.1 and Tivoli CCMDB V7.1.1.5

We are assuming the following conditions:

- Tivoli Provisioning Manager V7.1 and Tivoli CCMDB 7.1.1.3 are installed on the same Windows system.
- The integration between the two products is operational.
- The product fix packs to install are available on the system.

Step 1: Upgrade preparation steps

Follow these steps:

1. Stop Tivoli Provisioning Manager as follows:

%TI0_HOME%\tools\tio.cmd stop <wasadmin> <wasdmin_password>

2. Start WebSphere Application Server as follows:

startManager.bat
startNode.bat

Attention: Keep the MXServer stopped.

- 3. Run these steps to ensure that configuration changes are applied to the Maximo database and to drop any temporary table.
 - a. Open a command prompt on the CCMDB administrative system and issue the following commands:

cd C:\IBM\SMP\maximo\tools\maximo configdb.bat restorefrombackup.bat dropbackup.bat dropbackup.bat

Attention: The **dropbackup.bat** is run twice to ensure that there are no more changes to apply.

b. Optionally you can restart the MXServer by running:

%WAS_HOME%\profiles\ctgAppSrv01\bin\startServer.bat MXServer and log into Tivoli Provisioning Manager user interface to check that all steps were correctly run up to this point.

4. Check if the non-SSL port is enabled by trying to connect to:

http://<fully qualified hostname>/maximo

If you cannot connect using that URL, run the following steps to enable the non-SSL port:

a. Log on as wasadmin to the WebSphere Application Server console at the URL:

https://<fully qualified_hostname>:9043/ibm/console

- b. Navigate to Environment \rightarrow Virtual Hosts \rightarrow maximo_host \rightarrow Host Aliases.
- c. Click New.
- d. Specify the following values:

Host Name: * Port: 80

- e. Click OK.
- f. Click Save.
- g. Restart Tivoli Provisioning Manager as follows:

```
%TIO_HOME%\tools\tio.cmd stop <wasadmin> <wasdmin_password>
%TIO_HOME%\tools\tio.cmd start
```

h. Verify that you can connect to the Tivoli Provisioning Manager user interface using a non-secure connection:

http://<fully qualified_hostname>/maximo

Step 2: Upgrade CCMDB V7.1.1.3 to fix pack 5

Follow these steps:

1. Stop Tivoli Provisioning Manager as follows:

%TIO_HOME%\tools\tio.cmd stop <wasadmin> <wasdmin_password>

2. Follow the instructions provided in the fix pack readme file and run the installation.

Note: In this sample we have assumed that you have installed on a server with a Windows operating system.

If you installed on a UNIX machine, then you have to run the following steps at this stage on the Windows administrative workstation from which you installed the Base Services:

- 1. Log in as root on the UNIX system.
- 2. Start the WebSphere Application Server Manager, Node, and MXServer.
- 3. On the Windows administrative workstation modify the file C:\IBM\SMP\etc\install.properties by replacing:

WAS.RemoteAccessUserName=root

with:

WAS.RemoteAccessUserName=tioadmin

Now you can the upgrade from the Windows administrative workstation.

Step 3: Upgrade WebSphere Application Server to fix pack 23

You must upgrade the WebSphere Application Server if the version installed is lower than 6.1.0.23.

Follow the instructions provided in the fix pack readme file and run the installation.

Step 4: Upgrade Tivoli Provisioning Manager to V7.1.1

Upgrade Tivoli Provisioning Manager V7.1 to V7.1.1 following the instruction provided in *Tivoli Provisioning Manager Version 7.1.1 Upgrade Guide* at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ibm.t ivoli.tpm.ins.doc/tpm_upgrade_guide.pdf

Upgrade to Tivoli Provisioning Manager V7.1.1 and Tivoli Service Request Manager V7.1.0.4

In this topic you can find the sequence of steps to upgrade a pre-existing Tivoli Provisioning Manager and Tivoli Service Request Manager integration to Tivoli Provisioning Manager 7.1.1 and Tivoli Service Request Manager V7.1.0.4. We are assuming the following conditions:

- Tivoli Provisioning Manager V7.1 and Tivoli Service Request Manager 7.1.0.2 are installed on the same Windows system.
- The integration between the two products is operational.
- The product fix packs to install are available on the system.
- ► The level of Service Request Manager V7.1 install is March 2009 or later.

Note: Only if you installed a level of Service Request Manager V7.1 sooner than March 2009, you must have run the following steps before installing Tivoli Provisioning Manager V7.1:

1. Open a DB2 command window:

db2cmd

2. Set the DB2 instance:

set db2instance=ctginst1

3. Connect to the maxdb71:

db2 connect to maxdb71 user maximo using password <maximo password>

4. Update the CTRLCONDITION table as follows:

update CTRLCONDITION set CTRLCONDITIONID=99999200 where CTRLCONDITIONID=200;

```
update CTRLCONDITION set CTRLCONDITIONID=99999201 where
CTRLCONDITIONID=201;
```

Step 1: Install Service Request Manager fix pack 4

Follow the instructions provided in the fix pack readme file and run the installation.

Step 2: Upgrade WebSphere Application Server to fix pack 23

You must upgrade the WebSphere Application Server if the version installed is lower than 6.1.0.23.

Follow the instructions provided in the fix pack readme file and run the installation.

Step 3: Upgrade Tivoli Provisioning Manager to V7.1.1

Make sure that you review and run the following steps before starting to install Tivoli Provisioning Manager V7.1.1.

1. Stop Tivoli Provisioning Manager as follows:

```
%TI0_HOME%\tools\tio.cmd stop <wasadmin> <wasdmin_password>
```

- 2. Run these steps to ensure that configuration changes are applied to the Maximo database and to drop any temporary table.
 - a. Stop the MXServer by running this command:

```
%WAS_HOME%\profiles\ctgAppSrv01\bin\stopServer.bat MXServer
-username wasadmin -password <wasadmin password>
```

b. Open a command prompt on the CCMDB system and issue the following commands:

cd C:\IBM\SMP\maximo\tools\maximo configdb.bat restorefrombackup.bat dropbackup.bat dropbackup.bat

Attention: The dropbackup.bat is run twice to ensure that there are no more changes to apply.

c. Restart the MXServer by running:

%WAS_HOME%\profiles\ctgAppSrv01\bin\startServer.bat MXServer

- 3. Stop the base services applications as follows:
 - a. Log on to the WebSphere Application Server console at the URL:

http://<fully qualified_hostname>:9060/ibm/console

- b. Navigate to Applications \rightarrow Enterprise Applications.
- c. Select MAXIMO and MAXIMOHELP, and click the Stop button.
- d. Log out from the WebSphere Application Server console.
- 4. To upgrade the product, follow the *Tivoli Provisioning Manager Version 7.1.1 Upgrade Guide* at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ib
m.tivoli.tpm.ins.doc/tpm_upgrade_guide.pdf

Step 4: Post-upgrade steps

Run the following steps to complete the setup:

- 1. Verify the configuration settings in the WebSphere Application Server Console:
 - a. Log on as wasadmin to the WebSphere Application Server console at the URL:

http://<fully qualified_hostname>:9060/ibm/console

b. Navigate to:

Applications \rightarrow Enterprise Applications \rightarrow MAXIMO \rightarrow Class loading and update.

- c. Ensure **Single class loader for application** is checked under WAR class loader policy.
- d. Ensure **Classes loaded with parent class loader first** is checked under Class loader order.
- e. If you applied any change, click Save.
- f. Restart WebSphere Application Server.
- 2. If non-SSL port is required, you can optionally enable it as follows:
 - a. Log on as **wasadmin** to the WebSphere Application Server administration console:

http://<fully_qualified_hostname>:9060/admin

- b. Select Environment \rightarrow Virtual Hosts \rightarrow maximo_host \rightarrow Host Aliases.
- c. Select the Host Alias with Port Number: 80.
- d. Click Delete.
- e. Click Save.
- f. Restart Tivoli Provisioning Manager as follows:

%TIO_HOME%\tools\tio.cmd stop <wasadmin> <wasdmin_password>
%TIO_HOME%\tools\tio.cmd start

g. Verify you can connect to the Tivoli Provisioning Manager user interface using a non-secure connection:

http://<fully_qualified_hostname>:80/maximo

3. Ensure Maximo business objects are in sync. Do the following if Tivoli Provisioning Manager DE is not started properly:

Integration between Tivoli Provisioning Manager V7.1.1 and IBM Tivoli Asset Management for IT V7.1.0.5

This topic provides high level instructions for installing Tivoli Provisioning Manager V7.1.1 to coexist with IBM Tivoli Asset Management for IT V7.1.0.5 on one WebSphere Application Server.

These steps do not replace the Tivoli Asset Management for IT documentation, but provide guidance for installing the product in the same environment as Tivoli Provisioning Manager.

Installing Tivoli Asset Management for IT on top of Tivoli Provisioning Manager V7.1.1

After having installed Tivoli Provisioning Manager V7.1.1 following the instructions provided in the Installation Guide, run the following steps.

Step 1: Run Tivoli Asset Management for IT pre-installation steps

Run the following steps on the system where you installed Tivoli Provisioning Manager:

1. Stop Tivoli Provisioning Manager as follows:

%TI0_HOME%\tools\tio.cmd stop <wasadmin> <wasdmin_password>

2. Start WebSphere Application Server as follows:

startManager.bat
startNode.bat

Attention: Keep the MXServer stopped.

3. As Administrator, run these steps in a command prompt shell on the administrative workstation to ensure that configuration changes are applied to the Maximo database and to drop any temporary tables:

```
cd C:\IBM\SMP\maximo\tools\maximo
configdb.bat
restorefrombackup.bat
dropbackup.bat
dropbackup.bat
```

Attention: The dropbackup.bat is run twice to ensure that there are no more changes to apply.

Step 2: Install Tivoli Asset Management for IT V7.1

Tivoli Asset Management for IT installation is run on the administrative workstation. In this sample, because we are assuming to install on a server with a Windows operating system, the administrative workstation is the server itself.

If you installed Tivoli Provisioning Manager on a UNIX machine, then you have to run the steps to install Tivoli Asset Management for IT on the Windows administrative workstation from where you installed the Base Services and the Web Components.

We assume that the version of Tivoli Asset Management for IT to install is V7.1 image from March 2009 release:

- 1. Start the Tivoli Asset Management for IT launchpad.
- 2. Because Base Services V7.1.1.5 have already been installed during Tivoli Provisioning Manager installation, only license enablement is required.
- 3. Enable license for usage.
- 4. No IBM Tivoli Management for IT V7.1.0.5 fix pack application is required.

Step 3: Run Tivoli Asset Management for IT post- installation steps

Run the following steps to complete the setup.

- 1. Verify the configuration settings in the WebSphere Application Server Console:
 - a. Log on as wasadmin to the WebSphere Application Server console at the URL:

http://<fully qualified_hostname>:9060/ibm/console

b. Navigate to:

Applications \rightarrow Enterprise Applications \rightarrow MAXIMO \rightarrow Class loading and update.

- c. Ensure that **Single class loader for application** is checked under WAR class loader policy.
- d. Ensure that **Classes loaded with parent class loader** first is checked under Class loader order.
- e. If you applied any changes, click Save.
- f. Restart WebSphere Application Server.
- 2. Optionally you can run the following steps to enable also the non-SSL port:
 - a. Log on to the WebSphere Application Server console at the URL:

https://<fully qualified_hostname>:9043/ibm/console

as userid wasadmin.

- b. Navigate to Environment \rightarrow Virtual Hosts \rightarrow maximo_host \rightarrow Host Aliases.
- c. Click New.
- d. Specify the following values:

```
Host Name: *
Port: 80
```

- e. Click OK.
- f. Click Save.
- g. Restart Tivoli Provisioning Manager as follows:

%TIO_HOME%\tools\tio.cmd stop <wasadmin> <wasdmin_password> %TIO_HOME%\tools\tio.cmd start

- 3. Ensure Maximo business objects are in sync. Do the following if Tivoli Provisioning Manager DE is not started properly:
 - a. In a command shell run the following commands:

```
cd "C:\ibm\SMP\maximo\deployment\default"
unzip maximo.ear businessobjects.jar
```

b. Copy the businessobjects.jar file into the following directories:

%TIO_HOME%\eclipse\plugins\tpm_pmp\maximoLibs
%TIO_HOME%\lwi\runtime\tpm\eclipse\plugins\tpm_pmp\maximoLibs

c. Restart Tivoli Provisioning Manager as follows:

```
%TIO_HOME%\tools\tio.cmd stop <wasadmin> <wasdmin_password>
%TIO_HOME%\tools\tio.cmd start
```

Installing Tivoli Provisioning Manager on top of Tivoli Asset Management for IT V7.1.0.5

After having installed:

IBM Tivoli Management for IT V7.1 March 2009 release following the instructions provided in Tivoli Provisioning Manager V7.1.1 Installation Guide:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ib m.tivoli.tpm.ins.doc/tpm_install_guide.pdf

- IBM Tivoli Management for IT V7.1 fix pack 5 following the instructions provided in the readme file
- ► Then run the following steps to complete the overall installation.

Step 1: Run Tivoli Provisioning Manager V7.1.1 pre-installation steps

Make sure you run the following steps before starting to install Tivoli Provisioning Manager V7.1.1.

- 1. Run these steps to ensure that configuration changes are applied to the Maximo database and to drop any temporary table.
 - a. Stop the MXServer by running this command:

```
%WAS_HOME%\profiles\ctgAppSrv01\bin\stopServer.bat MXServer
-username wasadmin -password <wasadmin password>
```

b. Open a command prompt on the system and issue the following commands:

cd C:\IBM\SMP\maximo\tools\maximo configdb.bat restorefrombackup.bat dropbackup.bat dropbackup.bat

Attention: The dropbackup.bat is run twice to ensure that there are no more changes to apply.

c. Restart the MXServer by running:

%WAS_HOME%\profiles\ctgAppSrv01\bin\startServer.bat MXServer

- 2. Stop the base services applications as follows:
 - a. Log on to the WebSphere Application Server console at the URL:

http://<fully qualified_hostname>:9060/ibm/console

- b. Navigate to Applications \rightarrow Enterprise Applications.
- c. Select MAXIMO and MAXIMOHELP, and click the Stop button.
- d. Log out from the WebSphere Application Server console.

Step 2: Upgrade WebSphere Application Server to fix pack 23

You must upgrade the WebSphere Application Server if the version installed is lower than 6.1.0.23.

Follow the instructions provided in the fix pack readme file and run the installation.

Step 3: Install Tivoli Provisioning Manager V7.1.1

Refer to 4.3, "Tivoli Provisioning Manager V7.1.1 installation" on page 68. to install the following Tivoli Provisioning Manager parts:

- Only the Web Replay component among the Base Services
- Core Components
- Web Components

After the installation completes, you can do the following steps to double-check that Tivoli Provisioning Manager is properly installed:

1. Log on to the Tivoli Provisioning Manager User Interface at:

https://<fully_qualified_hostname>:9443/maximo

Do this as default administrator userid maxadmin with password maxadmin.

- 2. In the Welcome page you must see the following Start Centers for the Tivoli Provisioning Manager roles added by the Tivoli Provisioning Manager installation:
- Automation Package Developer
- Compliance Analyst
- Deployment Specialist
- Provisioning Administrator
- Provisioning Configuration Librarian

Step 4: Run Tivoli Provisioning Manager V7.1.1 post-installation steps

Run the following steps to complete the setup:

1. When Tivoli Provisioning Manager installation completes, by default the SSL port is enabled.

Optionally you can run the following steps to enable also the non-SSL port:

a. Log on to the WebSphere Application Server console at the URL:

https://<fully qualified_hostname>:9043/ibm/console

as userid wasadmin.

- b. Navigate to Environment \rightarrow Virtual Hosts \rightarrow maximo_host \rightarrow Host Aliases.
- c. Click New.
- d. Specify the following values:

Host Name: * Port: 80

e. Click OK.

- f. Click Save.
- g. Restart Tivoli Provisioning Manager as follows:

```
%TIO_HOME%\tools\tio.cmd stop <wasadmin> <wasdmin_password>
%TIO_HOME%\tools\tio.cmd start
```

h. Verify that you can connect to the Tivoli Provisioning Manager user interface using a non-secure connection:

http://<fully qualified hostname>/maximo

- 2. Ensure Maximo business objects are in sync. Do the following if Tivoli Provisioning Manager DE is not started properly:
 - a. In a command shell run the following commands:

```
cd "C:\ibm\SMP\maximo\deployment\default"
unzip maximo.ear businessobjects.jar
```

b. Copy the businessobjects.jar file into the following directories:

%TIO_HOME%\eclipse\plugins\tpm_pmp\maximoLibs %TIO_HOME%\lwi\runtime\tpm\eclipse\plugins\tpm_pmp\maximoLibs

c. Restart Tivoli Provisioning Manager as follows:

%TIO_HOME%\tools\tio.cmd stop <wasadmin> <wasdmin_password>
%TIO_HOME%\tools\tio.cmd start

684 IBM Tivoli Provisioning Manager V7.1.1: Deployment and IBM Service Management Integration Guide

Β

Tivoli Provisioning Manager Version 7.1.1 pre-installation checks

This appendix provides the pre-installation prerequisite checks performed on the AIX 6.1 system used to install part of the components of Tivoli Provisioning Manager Version 7.1.1 for the subsequent migration process from 5.1.1.2 version as described in 17.5, "Tivoli Provisioning Manager Version 7.1.1 pre-installation tasks" on page 558.

Compared to the same steps described in the Installation Guide or Migration Guide, we focused on the creation of a predefined filesystem structure, and we detailed all the commands, for AIX 6.1, required to perform the checks.

This appendix covers the following topics:

- "File systems creation" on page 686
- "Required packages" on page 688
- "openssl and openssh" on page 690
- "Operating System checks" on page 692
- "Environment checks" on page 695
- "Prepare the installation media" on page 697

File systems creation

The hardware configuration described next allows you to create a separate logical volume grouping (volume group) dedicated to the creation of all the filesytems, with the required mount points for the installation of the various components.

All the filesystems created use the mount point matching the default installation location of the various products.

Example B-1 shows the final structure created on our system for the installation.

Note: The default allocation size of a filesystem is determined by the volume group physical partition size (PP size) value.

If you do not specify the PP size at volume group creation, AIX will calculate its size automatically based on the size of the physical volume you add to the volume group. You cannot have more than 1016 physical partitions per each physical volume. The physical volume used on our AIX system is 300 GB and the calculated PP size at volume group creation was 512 MB.

With 512 MB being the PP size for our volume group, the creation of a smaller filesystem (for example, 100 MB) allocates the default size of 512 MB.

Example B-1 Filesystem structure

The volume group created is called tpmvg. The following command shows the logical volumes belonging to the tpmvg volume group:

[root@risc550a][/]> lsvg -l tpmvg	
-----------------------------------	--

ТҮРЕ	LPs	PPs	PVs	LV STATE	MOUNT POINT
jfs2log	1	1	1	open/syncd	N/A
jfs2	1	1	1	open/syncd	/home/maximo
jfs2	120	120	1	open/syncd	/tpm_images
jfs2	12	12	1	open/syncd	/opt/IBM/SMP
jfs2	2	2	1	open/syncd	/tmp/mwi
jfs2	12	12	1	open/syncd	/tmp/swrepos
jfs2	12	12	1	open/syncd	/opt/IBM/tivoli/tpm
jfs2	1	1	1	open/syncd	/opt/IBM/tpmfos
jfs2	1	1	1	open/syncd	/opt/tpmfosd_files
jfs2	1	1	1	open/syncd	/opt/IBM/AgentManager
jfs2	1	1	1	open/syncd	/opt/IBM/DeviceManager
jfs2	1	1	1	open/syncd	/opt/IBM/tivoli/CDS
jfs2	1	1	1	open/syncd	/usr/ibm/tivoli/common/COP/logs
jfs2	1	1	1	open/syncd	/opt/IBM/tivoli/ITM
	TYPE jfs2log jfs2 jfs2 jfs2 jfs2 jfs2 jfs2 jfs2 jfs2	TYPELPsjfs2log1jfs21jfs2120jfs212jfs212jfs212jfs21jfs21jfs21jfs21jfs21jfs21jfs21jfs21jfs21jfs21jfs21jfs21jfs21jfs21jfs21jfs21	TYPELPsPPsjfs2log11jfs211jfs2120120jfs21212jfs21212jfs21212jfs211jfs211jfs211jfs211jfs211jfs211jfs211jfs211jfs211jfs211jfs211jfs211jfs211	TYPELPsPPsPVsjfs2log111jfs2111jfs21201201jfs212121jfs212121jfs212121jfs2111jfs2111jfs2111jfs2111jfs2111jfs2111jfs2111jfs2111jfs2111jfs2111jfs2111	TYPELPsPPsPVsLV STATEjfs2log111open/syncdjfs2111open/syncdjfs21201201open/syncdjfs212121open/syncdjfs212121open/syncdjfs212121open/syncdjfs212121open/syncdjfs21211open/syncdjfs21 <td< td=""></td<>

fslv25	jfs2	5	5	1	open/syncd	/opt/IBM/db2
fslv26	jfs2	20	20	1	open/syncd	/home/ctginst1
fslv27	jfs2	2	2	1	open/syncd	/opt/IBM/ldap
fslv28	jfs2	3	3	1	open/syncd	/home/idsccmdb
fslv29	jfs2	1	1	1	open/syncd	/opt/IBM/AgentController
fslv30	jfs2	7	7	1	open/syncd	/usr/IBM/WebSphere/AppServer
fslv31	jfs2	1	1	1	open/syncd	/usr/IBM/WebSphere/UpdateInstaller
fslv04	jfs2	3	3	1	open/syncd	/usr/IBM/HTTPServer
fslv32	jfs2	1	1	1	open/syncd	/usr/ibm/common/acsi
fslv02	jfs2	1	1	1	open/syncd	/opt/tivoli/cit
fslv03	jfs2	1	1	1	open/syncd	/usr/ibm/tivoli/common/CIT/logs
fslv05	jfs2	1	1	1	open/syncd	/usr/ibm/tivoli/common/ctgde/logs
fslv06	jfs2	1	1	1	open/syncd	/opt/IBM/ITM
fslv08	jfs2	1	1	1	open/syncd	/home/dasusr1
fslv09	jfs2	1	1	1	open/syncd	/home/db2fenc1
fslv11	jfs2	1	1	1	open/syncd	/home/db2inst1
fslv12	jfs2	1	1	1	open/syncd	/home/idsldap
fslv33	jfs2	1	1	1	open/syncd	/home/tioadmin
fslv34	jfs2	2	2	1	open/syncd	/ibm/tivoli/mwi/workspace

The following command shows the space utilization details of the filesystems:

[root@risc550a]	[/]> df -k					
Filesystem 1	LO24-blocks	Free	%Used	Iused	%Iused	Mounted on
/dev/hd4	262144	64376	76%	2303	14%	/
/dev/hd2	1835008	552772	70%	35919	23%	/usr
/dev/hd9var	131072	86524	34%	401	3%	/var
/dev/hd3	2228224	2175336	3%	74	1%	/tmp
/dev/fwdump	393216	392828	1%	4	1%	/var/adm/ras/platform
/dev/hd1	131072	130680	1%	16	1%	/home
/dev/hd11admin	131072	130708	1%	5	1%	/admin
/proc	-	-		-	-	/proc
/dev/hd10opt	524288	268092	49%	5464	9%	/opt
/dev/livedump	262144	261776	1%	4	1%	/var/adm/ras/livedump
/dev/fslv01	67108864	10523444	85%	13041	1%	/tivoli_images
/dev/fs1v07	2097152	205764	91%	21591	31%	/opt/IBM/ITM_Backup
/dev/fslv10	157286400	113319252	28%	29	1%	/beta3
/dev/fs1v00	524288	523880	1%	4	1%	/home/maximo
/dev/fslv13	62914560	13452424	79%	4733	1%	/tpm_images
/dev/fslv14	6291456	6290168	1%	4	1%	/opt/IBM/SMP
/dev/fslv15	1048576	1048088	1%	4	1%	/tmp/mwi
/dev/fslv16	6291456	6290168	1%	4	1%	/tmp/swrepos
/dev/fslv17	6291456	6290168	1%	4	1%	/opt/IBM/tivoli/tpm
/dev/fslv18	524288	523880	1%	4	1%	/opt/IBM/tpmfos
/dev/fslv19	524288	523880	1%	4	1%	/opt/tpmfosd files
/dev/fslv20	524288	523880	1%	4	1%	/opt/IBM/AgentManager
/dev/fslv21	524288	523880	1%	4	1%	/opt/IBM/DeviceManager
/dev/fslv22	524288	523880	1%	4	1%	/opt/IBM/tivoli/CDS
/dev/fslv23	524288	523880	1%	4	1%	/usr/ibm/tivoli/common/COP/logs

/dev/fslv24	524288	523880	1%	4	1% /opt/IBM/tivoli/ITM
/dev/fslv25	2621440	2620712	1%	4	1% /opt/IBM/db2
/dev/fslv26	10485760	10483828	1%	5	1% /home/ctginst1
/dev/fslv27	1048576	1048088	1%	4	1% /opt/IBM/ldap
/dev/fslv28	1572864	1572296	1%	4	1% /home/idsccmdb
/dev/fslv29	524288	523880	1%	4	1% /opt/IBM/AgentController
/dev/fslv30	3670016	3669128	1%	4	1% /usr/IBM/WebSphere/AppServer
/dev/fslv31	524288	523880	1%	4	1% /usr/IBM/WebSphere/UpdateInstaller
/dev/fslv04	1572864	1572296	1%	4	1% /usr/IBM/HTTPServer
/dev/fslv32	524288	523880	1%	4	1% /usr/ibm/common/acsi
/dev/fslv02	524288	523880	1%	4	1% /opt/tivoli/cit
/dev/fslv03	524288	523880	1%	4	1% /usr/ibm/tivoli/common/CIT/logs
/dev/fslv05	524288	523880	1%	4	1% /usr/ibm/tivoli/common/ctgde/logs
/dev/fslv06	524288	523880	1%	4	1% /opt/IBM/ITM
/dev/fslv08	524288	523880	1%	4	1% /home/dasusr1
/dev/fslv09	524288	523880	1%	4	1% /home/db2fenc1
/dev/fslv11	524288	523880	1%	4	1% /home/db2inst1
/dev/fslv12	524288	523880	1%	4	1% /home/idsldap
/dev/fslv33	524288	523880	1%	4	1% /home/tioadmin
/dev/fslv34	1048576	1021572	3%	1281	1% /ibm/tivoli/mwi/workspace

Required packages

The following RPMs must be installed on the AIX system before installing Tivoli Provisioning Manager Version 7.1.1:

- ► glib
- expect
- bash-doc
- ► bash
- ► gtk2
- ► tar
- perl
- ► tk
- ► tcl
- wget
- unzip

They can be downloaded from the IBM AIX Toolbox download page at:

http://www-03.ibm.com/systems/power/software/aix/linux/toolbox/download
.html

For details about the required versions, refer to *Tivoli Provisioning Manager Version 7.1.1 Installation Guide* at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ibm.t ivoli.tpm.ins.doc/tpm_install_guide.pdf

We downloaded the latest versions available at the IBM AIX Toolbox download page, as shown in Example B-2.

Example B-2 Prerequisites RPMs

Follows the version of the RPM's downloaded from the IBM AIX Toolbox download page:

glib-1.2.10-2.aix4.3.ppc.rpm expect-5.42.1-3.aix5.1.ppc.rpm bash-doc-3.2-1.aix5.2.ppc.rpm gtk2-2.8.3-9.aix5.1.ppc.rpm tar-1.14-2.aix5.1.ppc.rpm tk-8.4.7-3.aix5.1.ppc.rpm tcl-8.4.7-3.aix5.1.ppc.rpm wget-1.9.1-1.aix5.1.ppc.rpm unzip-5.51-1.aix5.1.ppc.rpm

We installaed them using **rpm** command, increasing first the /opt disk space to 500MB:

rpm -ivh *.rpm

bash	****
bash-doc	#######################################
expect	#######################################
glib	*****
gtk2	****
perl	****
tar	#######################################
tcl	#######################################
tk	***
unzip	*****
wget	***

We then set the *PATH* variable to include the GNU tar at first place as shown below: [root@risc550a][/opt/freeware/bin]> export PATH=/opt/freeware/bin:\$PATH [root@risc550a][/]> tar --version tar (GNU tar) 1.14 Copyright (C) 2004 Free Software Foundation, Inc. This program comes with NO WARRANTY, to the extent permitted by law. You may redistribute it under the terms of the GNU General Public License; see the file named COPYING for details. Written by John Gilmore and Jay Fenlason.

openssl and openssh

These two packages are required for all supported AIX systems. They can be downloaded from the following locations:

openssh can be download from:

https://sourceforge.net/projects/openssh-aix

openssl can be downloaded from the IBM AIX Toolbox download page at:

http://www-03.ibm.com/systems/power/software/aix/linux/toolbox/downl
oad.html

Example B-3 shows the detailed steps to install these packages.

Example B-3 openssl and openssh

The following directory listing shows the packages needed for the openssl and openssh installation:

```
[root@risc550a][/tpm_images/openssl-ssh]> 1s -la
total 23384
drwxr-xr-x  2 root  system   256 Jul 06 15:47 .
drwxr-xr-x  6 root  system   256 Jul 06 17:40 ..
-rw-r----  1 root  system   1555 Jul 06 15:46 Readme.0.9.8.840-AIX-5.3_6.1.txt
-rw-r----  1 root  system   0 Jul 06 15:46 openssh_5.0.0.5302_61.tar.Z
-rw-r----  1 root   system   6710648 Jul 06 15:46 openssl.0.9.8.840-AIX5.3_6.1.tar.Z
```

We used a script run from the Command Line Interface (CLI) to perform the installation after uncompressed and extracted the packages:

OPENSSL INSTALLATION

/usr/lib/instl/sm_inst installp_cmd -a -l -d '.' -f 'openssl.base ALL @@I:openssl.base _all_filesets,openssl.license ALL @@I:openssl.license _all_filesets,openssl.man.en_US ALL @@I:openssl.man.en_US _all_filesets' '-c' '-N' '-g' '-X' '-Y'

The result of the installation was:

Finished processing all filesets. (Total time: 38 secs).

++ Summaries:								
++								
Installation Summary								
Name	Level	Part	Event	Result				
openssl.man.en_US openssl.license openssl.base openssl.base	0.9.8.840 0.9.8.840 0.9.8.840 0.9.8.840 0.9.8.840	USR USR USR ROOT	APPLY APPLY APPLY APPLY	SUCCESS SUCCESS SUCCESS SUCCESS				

OPENSSH INSTALLATION

/usr/lib/instl/sm_inst installp_cmd -a -l -d '.' -f 'openssh.base ALL @@I:openssh.base _all_filesets,openssh.license ALL @@I:openssh.license _all_filesets,openssh.man.en_US ALL @@I:openssh.man.en_US _all_filesets,openssh.msg.EN_US ALL @@I:openssh.msg.EN_US _all_filesets,openssh.msg. en_US ALL @@I:openssh.msg.en_US _all_filesets' '-c' '-N' '-g' '-X' '-Y'

The result of the installation was:

Finished processing all filesets. (Total time: 12 secs).

+			 +
	Summari	Δς •	·
	Julillari	E3 .	

Installation Summary

Name	Level	Part	Event	Result
openssh.license	5.0.0.5302	USR	APPLY	SUCCESS
openssh.base.client	5.0.0.5302	USR	APPLY	SUCCESS
openssh.base.server	5.0.0.5302	USR	APPLY	SUCCESS
openssh.base.client	5.0.0.5302	ROOT	APPLY	SUCCESS
openssh.base.server	5.0.0.5302	ROOT	APPLY	SUCCESS
openssh.msg.en US	5.0.0.5302	USR	APPLY	SUCCESS
openssh.msg.EN_US	5.0.0.5302	USR	APPLY	SUCCESS
openssh.man.en_US	5.0.0.5302	USR	APPLY	SUCCESS

File /etc/group has been modified.

----------+

File /etc/passwd has been modified.

One or more of the files listed in /etc/check_config.files have changed. See /var/adm/ras/config.diff for details.

TESTING SSH INSTALLATION

```
[root@risc550a][/tpm images/openssl-ssh/openssh]> ssh risc550a.rot.it.ibm.com
The authenticity of host 'risc550a.rot.it.ibm.com (9.168.47.14)' can't be
established.
RSA key fingerprint is 57:7b:a0:2f:82:9e:7e:2a:c7:40:52:f3:66:da:a9:8c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'risc550a.rot.it.ibm.com,9.168.47.14' (RSA) to the list of
known hosts.
root@risc550a.rot.it.ibm.com's password:
Last unsuccessful login: Mon Jul 6 14:13:49 DFT 2009 on ftp from
L3ARA8X-6474B84.rot.it.ibm.com
Last login: Tue Jul 7 11:25:48 DFT 2009 on /dev/pts/1 from
ICON-9-164-169-78.megacenter.de.ibm.com
* Welcome to AIX Version 6.1!
 Please see the README file in /usr/lpp/bos for information pertinent to
*
* this release of the AIX Operating System.
*
*
[root@risc550a][/]>
```

Operating System checks

The Operating System checks include these:

- Verify 64-bit cpu/kernel configuration.
- Verify the automount daemon status.
- Check the required paging space.
- Check the required maxuproc setting.
- Check the required ulimit settings.
- ► Check the /tmp permission.
- Check umask setting.

These checks are detailed in Example B-4:

Example B-4 Operating System checks

```
Verify 64-bit cpu/kernel configuration
This can be verified by running these commands:
[root@risc550a][/]> prtconf -c
CPU Type: 64-bit
[root@risc550a][/]> prtconf -k
Kernel Type: 64-bit
Verify the automount daemon is disabled
This can be verified by running this command:
[root@risc550a][/dev]> lssrc -a grep mount
                  nfs
                                   303140
                                                 active
 rpc.mountd
automountd
                  autofs
                                                 inoperative
Check the required Paging Space
This can be verified by running these commands:
[root@risc550a][/dev] > lsps -a
Page Space
                Physical Volume
                                  Volume Group Size %Used Active Auto Type Chksum
hd6
                hdisk0
                                  rootvg
                                                  512MB
                                                            2
                                                                yes
                                                                      yes
Not being the default 512MB paging space enough, we created an addition paging space
to meet the requirement of at least 4GB. In our system we increased the paging space
to 8GB:
[root@risc550a][/dev]> lslv hd6
LOGICAL VOLUME:
                    hd6
                                           VOLUME GROUP:
                                                            rootva
                    00c56f5d00004c0000001223c19459d.2 PERMISSION:
                                                                        read/write
LV IDENTIFIER:
VG STATE:
                    active/complete
                                                            opened/syncd
                                           IV STATE:
TYPE:
                    paging
                                           WRITE VERIFY:
                                                            off
MAX LPs:
                    512
                                           PP SIZE:
                                                            128 megabyte(s)
COPIES:
                    1
                                           SCHED POLICY:
                                                            parallel
IPs:
                    4
                                           PPs:
                                                            4
STALE PPs:
                    0
                                           BB POLICY:
                                                            non-relocatable
INTER-POLICY:
                    minimum
                                           RELOCATABLE:
                                                            yes
INTRA-POLICY:
                    middle
                                           UPPER BOUND:
                                                            32
MOUNT POINT:
                    N/A
                                           LABEL:
                                                            None
MIRROR WRITE CONSISTENCY: off
EACH LP COPY ON A SEPARATE PV ?: yes
Serialize IO ?:
                    NO
```

1v

0

The above command shows the partition size in the PP SIZE: value

```
[root@risc550a][/dev]> mkps -s'60' -n'' -a'' rootvg hdisk0
paging00
```

The above command added another paging space to the rootvg volume group to reach the 8GB value.

```
[root@risc550a][/dev]> lsps -a
Page Space
               Physical Volume
                                 Volume Group Size %Used Active Auto Type Chksum
                                                          1
paging00
               hdisk0
                                 rootvg
                                               7680MB
                                                             yes
                                                                            1v
                                                                                   0
                                                                     yes
hd6
               hdisk0
                                 rootvg
                                                 512MB
                                                           2
                                                              ves
                                                                     yes
                                                                            1v
                                                                                   0
[root@risc550a][/dev]> lsps -s
Total Paging Space Percent Used
     8192MB
                          1%
Check the required maxuproc setting
This can be verified by running this command:
[root@risc550a][/dev]> lsattr -El sys0 grep maxuproc
maxuproc
               128
                                  Maximum number of PROCESSES allowed per user
True
The requirement is to have at least 2048 maxuproc. We increased them to 4096 by
running this command:
[root@risc550a][/dev] > chdev -1 sys0 -a maxuproc='4096'
sys0 changed
```

[root@risc550a][/dev]> lsattr -El sys0|grep maxuproc maxuproc 4096 Maximum number of PROCESSES allowed per user True

Check the required ulimit settings

Check these entries in the /etc/security/limits file. If the limits for root are not se to unlimited, change them as follows:

```
root:
```

```
fsize = -1
cpu = -1
data = -1
rss = -1
nofiles = 8192
stack = -1
```
```
stack hard = -1
```

Logout and login again for the change to be effective:

```
[root@risc550a][/]> ulimit -a
time(seconds)
                    unlimited
file(blocks)
                    unlimited
data(kbytes)
                    unlimited
stack(kbytes)
                   unlimited
memory(kbytes)
                    unlimited
coredump(blocks)
                    unlimited
nofiles(descriptors) 8192
threads(per process) unlimited
processes(per user) unlimited
```

Check the /tmp permission is set to 1777
This can be verified by running ls -la /tmp command:

drwxrwxrwt 8 bin bin 4096 Jul 07 13:25 tmp

The above output shows correct permissions.

Check umask setting

The required umask value is 002.

```
[root@risc550a][/etc/security]> grep umask /etc/security/user
* umask Defines the default umask for the user.
umask = 022
```

Set the default to umask = 002 Logout and login again for the change to be effective

Environment checks

The environment checks include:

- hostname requirements
- /etc/hosts file requirements
- sshd_config configuration
- prepare the installation media

These checks are detailed in Example B-5.

Example B-5 Environment checks

Hostname requirements

[root@risc550a][/etc]> hostname
risc550a

[root@risc550a][/]> nslookup risc550a
Server: 9.64.162.21
Address: 9.64.162.21#53

Name: risc550a.rot.it.ibm.com Address: 9.168.47.14

The hostname is succesfully configured and resolved on a DNS server

/etc/hosts file requirements

#IP address	Fully Qualified Domain Name	Short name	
127.0.0.1	localhost.localdomain	loopback localhost	# loopback
(loO) name/addr	ess		
9 168 47 14	risc550a rot it ibm com	risc550a	

Moved the loopback at the second row.

sshd_config configuration

[root@risc550a][/etc/ssh]> grep PermitRootLogin sshd_config
#PermitRootLogin yes
the setting of "PermitRootLogin without-password".

Set PermitRootLogin to yes removing the # in the sshd_config file. Stop and start the sshd service by running these commands:

```
[root@risc550a] [/etc/ssh]> stopsrc -s sshd
0513-044 The sshd Subsystem was requested to stop.
[root@risc550a] [/etc/ssh]> startsrc -s sshd
0513-059 The sshd Subsystem has been started. Subsystem PID is 426004.
```

Prepare the installation media

Before starting the installation, place all of these installation images in the same location (/tpm_images has been used for this Redbooks publication):

- ► TPM_V711_Install_UNIX.tar
- ► TPM_V711_CoreComp_AIXPPC64.tar
- ► TPM_V711_Midlwr_AIXPPC64.tar

Note: For AIX, you must use the gtar command to extract the images.

After they are extracted, change the image location permission to 775 with this command:

chmod -R 775 /tpm_images

After you have verified all of these checks, the system is ready for the installation.

698 IBM Tivoli Provisioning Manager V7.1.1: Deployment and IBM Service Management Integration Guide

С

tpm5112backup.sh script

In this appendix you can find the tpm5112backup.sh script, which is referenced in in 17.8.1, "Migration tasks for the Tivoli Provisioning Manager Version 5.1.1.2 system" on page 591. You can also download this script using the instructions provided in Appendix D, "Additional material" on page 711.

tpm5112backup.sh script

Example C-1 displays the tpm5112backup.sh script.

```
Example C-1 tpm5112backup.sh script
```

```
#!/bin/bash
# Licensed Materials - Property of IBM
# 5724-F75
# (C) Copyright IBM Corp. 2003 - 2009
# All Rights Reserved
# US Government Users Restricted Rights -Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
##
# tpm5112backup performs basic checks on the original TPM 5.1.1.2
environment
# for readiness and then backup all the crucial data needed for
migration to
# TPM 7.1.1. The data includes database content backup, Agent Manager
# configurations backup, and directory server (i.e. LDAP) related data.
#
                         _____
   _____
 environment checks & initialization
      CURRENTDIR=`dirname $0`; CURRENTDIR=`cd $CURRENTDIR && pwd`
LaunchTitle=`basename $0`
. $CURRENTDIR/.script/progressTracker.sh
. $CURRENTDIR/.script/scriptUtil.sh
# Note that it is assumed DCM configuration information are available
through dcm.xml file defined
# under $TIO HOME/config directory.
# Steps to run through this script includes:
# 1) PRE CHECK ENV
# 2) VALIDATE INPUT
```

```
# 3) INITIAL_CONFIG
# 4) CREATE_LDIF
# 5) BACKUP_CAS
# 6) REMOVE_AUDIT
# 7) BACKUP_DB
# 8) COLLECT_FILES
#
```

setupLogs MarkScriptBegin

checkTpmEnv 5112

Once TIO_LOGS is defined, logs should be dumped to \$TIO_LOGS
useTpmLogs

```
confirmStart backup
```

MarkStepEnd

```
# Allow tpmmigrate.properties file to override
readAndMapVariable OPT_REMOVE_AUDIT removeAuditData noMissingCheck
{flag_to_remove_audit_before_backup}
readAndMapVariable OPT_OUT_DIR outputDir failMissing {output_directory}
readAndMapVariable OPT_BASE_DN baseDN failMissing {base-dn}
readAndMapVariable OPT_USR_DN userBaseDN failMissing {user-base-dn}
readAndMapVariable OPT_GRP_DN groupBaseDN failMissing {group-base-dn}
readAndMapVariable OPT_LDAP_TYPE ldapType noMissingCheck {ITDS_or_MSAD}
readAndMapVariable OPT_LDAP_USENEW ldapUseNew noMissingCheck
{new_or_exist}
readAndMapVariable OPT_DB_REMOTE dblsRemote noMissingCheck
{flag_is_database_on_tpm_server}
readAndMapVariable OPT_ORACLE_OSUSER orclOSUser noMissingCheck
{Oracle software owner OS user}
```

```
readAndMapVariable OPT ZIP FILES zipBackupFiles noMissingCheck
{Automatically zip backup files default to no}
readAndMapVariable OPT WAS USER wasUser noMissingCheck
{Websphere username}
# Add any other password parameter description. Note passwords should
always be prompted and thus no missing checks.
readAndMapVariable OPT DB PWD dbPass noMissingCheck {Database Password}
readAndMapVariable OPT ORACLE SYS PWD orclSysPass noMissingCheck
{Oracle Sys User Password}
# Force default behavior if option does not exist
if [ -z "$OPT REMOVE AUDIT" ]; then
    export OPT REMOVE AUDIT=no
fi
if [ -z "$OPT ZIP FILES" ]; then
    export OPT ZIP FILES=no
fi
EXPECTING=option
if [ $# -ne 0 ]; then
    while [ $# -gt 0 ]; do
        echo "$1" | $EGREPCMD "^($CMD OPTIONS)$" >/dev/null
        RESULTCODE=$?
        if [ "$EXPECTING" = "option" ]; then
            if [ $RESULTCODE -ne 0 ]; then
                # If current parameter token is not a known command
option
                CheckUsage
                ErrorExit $MC 16011 INVALID OPTION $*
            fi
            if [ $# -1t 2 ]; then
                CheckUsage
                ErrorExit $MC 16012 MISS OPTION VALUE $*
            fi
           EXPECTING=$1
        else
            if [ $RESULTCODE -eq 0 ]; then
                # If current parameter token is not a value
                CheckUsage
                ErrorExit $MC_16014_MISS_PROP_VALUE
```

```
fi
            fillInVariableValue $EXPECTING $1
            EXPECTING=option
        fi
        shift
    done
fi
# check whether directory is valid
if [ ! -d $OPT_OUT_DIR ]; then
    DEST DIR=$OPT OUT DIR
    ErrorExit $MC 16045 DIRECTORY NOT EXIST
else
    createDirectory $OPT OUT DIR/1dap
    createDirectory $OPT OUT DIR/tca
    createDirectory $OPT OUT DIR/database
    createDirectory $OPT OUT DIR/guid
    createDirectory $OPT OUT DIR/config
fi
checkMissingParameters
$DOT_SCRIPT_DIR/ldapOSQuery.sh -e "$TIO_HOME" -q
EXITCODE=$?
if [ $EXITCODE -eq 0 ]; then
    OPT LDAP OS=true
    promptMissingVar OPT LDAP TYPE "Enter the type of LDAP for 7.1.1
(ITDS or MSAD): " "ITDS MSAD"
    EXITCODE=0
else
    if [ $EXITCODE -eq 1 ]; then
        OPT LDAP OS=false
        promptMissingVar OPT LDAP USENEW "Are you using a new or
existing LDAP server for 7.1.1 (new or exist): " "new exist"
       if [ "$OPT LDAP USENEW" = "exist" ]; then
           promptMissingVar OPT WAS USER "Enter the name of the
WebSphere Application Server user: "
       fi
    else
        ErrorExit $EXITCODE
    fi
fi
EXITCODE=0
# Check for unrecognized database type
```

```
export DB TYPE=`$DOT SCRIPT DIR/getdbinfo.sh TYPE | tail -1 | tr
'[a-z]' '[A-Z]'`
if [ "$DB TYPE" != "DB2JCC" -a "$DB TYPE" != "ORACLE" ];then
    ErrorExit $MC 16025 UNSUPPORTED DATABASE
fi
# Read database information
export DB RUNTIME USER=`$DOT SCRIPT DIR/getdbinfo.sh USER | tail -1`
if [ -z "$DB RUNTIME USER" ]; then
    ErrorExit $MC 16027 FAIL GET DB USERNAME
fi
export DB NAME=`$DOT SCRIPT DIR/getdbinfo.sh NAME tail -1
if [ -z "$DB NAME" ]; then
    ErrorExit $MC 16028 FAIL GET DB NAME
fi
promptMissingVar OPT DB PWD "Enter the password for the database user
'$DB RUNTIME USER': "
if [ "$DB TYPE" = "ORACLE" ]; then
   promptMissingVar OPT ORACLE OSUSER "Enter the operating system user
name for the Oracle administrator: "
   promptMissingVar OPT ORACLE SYS PWD"Enter the password for Oracle
user SYS : "
fi
promptMissingVar OPT DB REMOTE "Is the database remote, yes or no? "
"yes no"
if [ "$OPT DB REMOTE" = "yes" ]; then
    promptMissingVar OPT DB BACKUPED "Have you backed up the database
on the remote database server, yes or no? " "yes no"
    if [ "$OPT DB BACKUPED" = "no" ]; then
        ErrorExit $MC 16043 DB NOT BACKUP
    fi
fi
confirmVariableValues
MarkStepEnd
# **********************
export STEP NAME=INITIAL CONFIG
# **********************
MarkStepBegin
```

```
# Check root user
if [ `$IDCMD -u` -ne 0 ]; then
    export runasuser=root
    ErrorExit $MC_16002_RUNAS_ERROR
fi
# Check user has administrative priviledges
TIOADMIN GRP=`$IDCMD -gn $TIOADMIN USER`
. $TIO HOME/.TCprofile
# use -L, since using -v will cause the >/dev/null to be interpreted as
a "zip from stdin" command
if [ "$OPT ZIP FILES" = "yes" ]; then
  zip -L >/dev/null
  if [ $? != 0 ];then
       ErrorExit $MC 16020 ZIP NOT FOUND
   fi
fi
# Check setupcmdline environment
SETUPCMD=$TI0 HOME/tools/setupCmdLine.sh
if [ ! -f $SETUPCMD ]; then
    ErrorExit $MC 16005 INVALID SETUPCMD
fi
if [ ! -x $SETUPCMD ]; then
    ErrorExit $MC 16019 FAIL SCRIPT EXEC
fi
. $SETUPCMD
#REM Ignore APPSERVER NAME, only WAS install needs it
#REM VPD file is not needed
#REM Backup does not require VPD paths for CAS, CDS, DMS
#REM TPM.product file is not crucial for determining packages
# Load values into other useful variables
BUILD VERSION PROP=$TIO HOME/config/build-version.properties
if [ ! -f $BUILD VERSION PROP ]; then
    ErrorExit $MC 16006 FAIL GET PROD VERSION
fi
VERSION=`grep 'current.version' $BUILD VERSION PROP | cut -d= -f2`
if [ -z "$VERSION" ]; then
    ErrorExit $MC 16007 FAIL SET PROD VERSION
fi
```

```
MIGRATE_FROM_VERSION=5.1.1.2
if [ "$VERSION" != "$MIGRATE_FROM_VERSION" ]; then
    ErrorExit $MC_16008_INCORRECT_FROM_VERSION
fi
```

#REM WAS_HOME and wsadmin.sh checks are ignore because not used #REM APPSRV_PROFILE and WAS_PROFILE_HOME checks are ignore because not used

```
SetTIOPermissions $TIO_HOME/eclipse/tpmconfig
SetTIOPermissions $TIO_HOME/migration
SetGlobalPermissions $OPT OUT DIR
```

#TPDO Remove Ignore access to CAS & CDS logs files which requies VPD access

```
MarkStepEnd
```

```
# *****************************
export STEP NAME=CREATE LDIF
MarkStepBegin
if [ $? -eq 0 ]; then
   echoAlreadyDone
else
    if [ -z "$OPT_WAS_USER" ]; then
     unset MINUS W OPT
    else
       MINUS W OPT="-w $OPT WAS USER"
  fi
   if [ "$OPT LDAP OS" = "true" ]; then
      RunScript $DOT SCRIPT DIR/1dapBackup.sh -e $TIO HOME -u
$0PT USR DN -g $0PT GRP DN -o $0PT OUT DIR/1dap -t $0PT LDAP TYPE -b
$OPT BASE DN 2>&1 | tee -a $unixUpgradeLog
   else
      if [ -z "$OPT GRP DN" ]; then
     RunScript $DOT SCRIPT DIR/1dapBackup.sh -e $TIO HOME -m
$OPT LDAP USENEW -o $OPT OUT DIR/ldap $MINUS W OPT 2>&1 | tee -a
$unixUpgradeLog
      else
      RunScript $DOT SCRIPT DIR/1dapBackup.sh -e $TIO HOME -m
$0PT LDAP USENEW -u $0PT USR DN -g $0PT GRP DN -o $0PT OUT DIR/1dap
$MINUS W OPT 2>&1 | tee -a $unixUpgradeLog
      fi
```

```
fi
   CheckScriptResult
  MIGRATION ERRORCODE=$((17920+$EXITCODE))
   if [ $EXITCODE -ne 0 ]; then
      ErrorExit $MIGRATION ERRORCODE
   fi
fi
MarkStepEnd
# **********************
export STEP NAME=BACKUP CAS
MarkStepBegin
if [ $? -eq 0 ]; then
    echoAlreadyDone
else
    # Store agent manager installation location into CAS HOME
    CAS VPD KEY=4886af1c5eb4f6c75d84991853b6aa2f
    CAS SUN PKG=IS4886af1
  if [ "$PLATFORM" = "solaris" ]; then
      CAS_HOME=`pkginfo -1 $CAS_SUN_PKG | grep "BASEDIR" | tr -d " " |
cut -d ":" -f 2
  else
      CAS HOME=`grep ^$CAS VPD KEY $VPD FILE | cut -d "|" -f13`
  fi
  if [ ! -d $CAS HOME ]; then
       ErrorExit $MC 16026 INVALID CAS HOME DIR
  fi
    # Move old getConfig.py to getConfig.py.old
    [ -f "$CAS HOME/toolkit/resources/getConfig.py" ] && rm -f
"$CAS HOME/toolkit/resources/getConfig.py"
    # Copy getConfig.py from TIO HOME/migration/resources to
CAS HOME/toolkit/resources
    cp "$TIO HOME/migration/resources/getConfig.py"
"$CAS HOME/toolkit/resources/getConfig.py"
    EXITCODE=$?
   if [ $EXITCODE -ne 0 ]; then
       ErrorExit $MC 16080 FAIL COPY GETCONFIGPY
    fi
    # Config proper permission
    SetTIOPermissions "$CAS HOME/toolkit/resources/getConfig.py"
```

```
REMPATH=`pwd`
    cd $CAS HOME/toolkit/bin
    RunScript ./backupTool.sh tca5112backup.zip 2>&1 | tee -a
$unixUpgradeLog
    CheckScriptResult
    ERRLEVEL=$EXITCODE
    cd $REMPATH
    unset REMPATH
    if [ $ERRLEVEL -ne 0 ]; then
       MIGCMD=backupTool.sh
        ErrorExit $MC 16033_FAIL_COMPLETE_CMND $ERRLEVEL
    fi
    mv $CAS HOME/toolkit/bin/tca5112backup.zip $OPT OUT DIR/tca
    ERRLEVEL=$?
    if [ $ERRLEVEL -ne 0 ]; then
        ErrorExit $MC 16029 FAIL MOVE FILE
    fi
fi
MarkStepEnd
if [ "$OPT REMOVE AUDIT" = "yes" -a "$OPT DB REMOTE" = "no" ]; then
export STEP NAME=REMOVE AUDIT
# ******************************
  MarkStepBegin
  if [ $? -eq 0 ]; then
      echoAlreadyDone
  else
        if [ "$DB TYPE" = "DB2JCC" ]; then
            RunScript su - $DB RUNTIME USER -c ".
$TIO HOME/.TCprofile; $DOT SCRIPT DIR/db2DeleteAudit.sh $DB NAME
$DB RUNTIME USER $OPT DB PWD 2>&1" | tee -a
$TIO LOGS/migration/removeaudit.log
            CheckScriptResult
            # Ignore Error
          if [$EXITCODE -ne 0]; then
              echoCK "Warning: Audit records removal returns with
value $EXITCODE. Please check $TIO LOGS/migration/removeaudit.log for
details."
          fi
            EXITCODE=0
        elif [ "$DB TYPE" = "ORACLE" ]; then
              RunScript su - $OPT ORACLE OSUSER -c ".
$TIO HOME/.TCprofile; $DOT SCRIPT DIR/oracleDeleteAudit.sh $DB NAME
```

```
$DB RUNTIME USER $OPT DB PWD 2>&1" | tee -a
$TI0 LOGS/migration/removeaudit.log
             CheckScriptResult
            # Ignore Error
          if [ $EXITCODE -ne 0 ]; then
              echoCK "Warning: Audit records removal returns with
value $EXITCODE. Please check $TIO LOGS/migration/removeaudit.log for
details."
          fi
            EXITCODE=0
        fi
  fi
  MarkStepEnd
fi
# *********
export STEP NAME=BACKUP DB
# *****************
MarkStepBegin
if [ $? -eq 0 ]; then
  echoAlreadyDone
else
  if [ "$OPT DB REMOTE" = "yes" ]; then
     echoCK The database is assumed to be already backed up through
manual steps, thus skipping step BACKUP DB.
  else
      if [ "$DB TYPE" = "DB2JCC" ]; then
          RunScript $SCRIPT DIR/runDb2Backup.sh $DB NAME
$DB RUNTIME USER $OPT DB PWD $OPT OUT DIR/database 2>&1 | tee -a
$unixUpgradeLog tee -a $TIO LOGS/migration/db2backup.log
          CheckScriptResult
          ERRLEVEL=$EXITCODE
      else
          if [ "$DB TYPE" = "ORACLE" ]; then
              RunScript $SCRIPT DIR/runOracleBackup.sh
$OPT ORACLE OSUSER $DB NAME $OPT ORACLE SYS PWD $OPT OUT DIR/database
2>&1 | tee -a $unixUpgradeLog | tee -a
$TI0 LOGS/migration/orclbackup.log
              CheckScriptResult
              ERRLEVEL=$EXITCODE
          fi
      fi
      if [ $ERRLEVEL -ne 0 ]; then
          ErrorExit $EXITCODE
```

```
fi
  fi
fi
MarkStepEnd
# **********************
export STEP NAME=COLLECT FILES
# ********
MarkStepBegin
# Do not skip even if done before
# Store Tivoli GUID
$TIVGUID FILE -Show > $OPT OUT DIR/guid/tivguid.txt
ERRLEVEL=$?
if [ $ERRLEVEL -ne 0 ]; then
    ErrorExit $MC 16030 FAIL TIVOLI GUID
fi
# Copy all the files from configuration directory
cp -R $TIO HOME/config $OPT OUT DIR
if [ $ERRLEVEL -ne 0 ]; then
    ErrorExit $MC 16031 FAIL COPY CFG FILES
fi
#zip command
if [ "$OPT ZIP FILES" = "yes" ]; then
   cd $OPT OUT DIR
  zip -r $OPT OUT DIR/tpm5112backup */*
  if [ $ERRLEVEL -ne 0 ]; then
      ErrorExit $MC 16032 FAIL PACKAGE BACKUP
  fi
fi
echoCK Backup process completed.
MarkStepEnd
MarkScriptEnd
finalizeLogs
exit 0
```

D

Additional material

This book refers to additional material that can be downloaded from the Internet as described next.

Locating the Web material

The Web material associated with this book is available in softcopy on the Internet from the IBM Redbooks publications Web server. Point your Web browser at:

ftp://www.redbooks.ibm.com/redbooks/SG247773

Alternatively, you can go to the IBM Redbooks Web site at:

ibm.com/redbooks

Select the **Additional materials** and open the directory that corresponds with the IBM Redbooks publications form number, SG247773.

Using the Web material

The additional Web material that accompanies this book includes the following files:

File nameDescriptiontpm5112backup.zipZipped tpm5112backup.sh script. This script is referenced
in 17.8.1, "Migration tasks for the Tivoli Provisioning
Manager Version 5.1.1.2 system" on page 591.

System requirements for downloading the Web material

The following system configuration is recommended:

Operating System: Windows/Linux/UNIX

How to use the Web material

Create a subdirectory (folder) on your workstation, and unzip the contents of the Web material zip file into this folder.

Abbreviations and acronyms

ACL	access control list	DOS	disk operating system
ADS	architecture description	DVD	digital video disc
	specification	EAR	enterprise archive
AM	Agent Manager	FIPS	Federal Information
APDE API	Automation Package		Processing Standard
		FQDN	fully qualified domain name
	application programming interface	FTP	File Transfer Protocol
BIOS	Basic Input/Output System	GB	gigabyte
BIRT	Business Intelligence and	GL	Graphics Library
	Reporting Tool	GUID	globally unique identifier
CAS	Common Agent Services	HADR	high availability disaster recovery
CCMDB	Configuration Management	HAL	hardware abstraction layer
	Database	НМС	Hardware Management
CD-ROM	compact-disc read-only		Console
	memory	HTML	Hypertext Markup Language
CDS	Content Delivery Service	HTTP	Hypertext Transfer Protocol
CI	callable interface	HTTPS	HTTP over SSL
СІТ	Common Inventory	I/O	input/output
DB	detabase	IBM	International Business
	database		Machines
DBWS	database management system	IP	Internet Protocol
DCD	Dynamic Content Delivery	ISM	IBM Service Management
DCM	data center model	ISO	International Organization for Standardization
DDS	Dynamic Depot Selection	ITIC	IBM Tivoli Integration
DE	deployment engine		Composer
DHCP	Dynamic Host Configuration Protocol	ITIL	Information Technology Infrastructure Library
DLL	dynamic link library	ІТМ	IBM Tivoli Monitoring
DMI	Desktop Management	JDBC	Java Database Connectivity
	Interface	JES	Job Entry Subsystem
DMS	Device Management Service	JIT	Just-In-Time
DNS	Domain Name System	JMS	Java Message Service

JRE	Java Runtime Environment	RXA Remote Execution and	
JVM	Java virtual machine		Access
LAN	local area network	SAN	storage area network
LDAP	Lightweight Directory Access Protocol	SAP	service access point
		SCM	software configuration
LDO	The Logical Device Operation	000	management
		SCP	System Control Process
LMO	Logical Management Operations	SDI	scalable distribution
MAC	Medium Access Control	SIE	Software Installation Engine
MB	megabyte	SMB	Server Message Block
MSU	message signal unit	SOA	service-oriented architecture
NFS	Network File System	SOAP	Simple Object Access
NIC	Network Information Center	SDR	software nackage block
NIS	Network Information Service	SPD	sorvice provider equipment
NIST	National Institute of Standards	SPE	Setware Peakage Editor
ODAL		SPE	Soliware Package Editor
OFAL	Automation Library	SQL	
os	operating system	SRM	system resources manager
PCI	Peripheral Component	<u>зэп</u>	Secure Snell
	Interconnect	SSL	Secure Sockets Layer
РМР	process manager product	IADDM	I Ivoli Application Dependency Discovery
PTF	program temporary fix		Manager
PXE	Preboot eXecution	ТСА	task control area
	Environment	ТСР	Transmission Control Protocol
RAID	Redundant Array of Independent Disks	TCP/IP	Transmission Control Protocol/Internet Protocol
RAM	random access memory	TLS	Transport Layer Security
RDBMS	relational database management system	UI	unique identifier unnumbered information frame
RFC	Request for Comments	URL	Uniform Resource Locator
ROM	read-only memory	VLAN	virtual local area network
RPC	remote procedure call	VMM	Virtual Member Manager
RPM	RPM Package Manager	WAN	wide area network
RTLM	IBM Rational Test Lab Manager	WAS	WebSphere Application Server

Web Services Description Language
Web Services Resource Framework
Microsoft Windows Server Update Services
Windows Update Agent
Extensible Markup Language
Extensible Stylesheet Language Transformation



Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this book.

IBM Redbooks

For information about ordering these publications, see "How to get Redbooks" on page 719. Note that some of the documents referenced here might be available in softcopy only.

 End-to-End Service Management Using IBM Service Management Portfolio SG24-7677

Online resources

These Web sites are also relevant as further information sources:

- Tivoli Provisioning Manager V7.1.1 Infocenter: http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp
- ► Tivoli Provisioning Manager V7.1.1 Installation Guide:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ib
m.tivoli.tpm.ins.doc/tpm_install_guide.pdf

► Tivoli Provisioning Manager V7.1.1 Administration Guide:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ib m.tivoli.tpm.scenario.doc/tpm_admin_guide.pdf

Cygwin website:

http://www.cygwin.com

Tivoli Provisioning Manager V7.1: Capacity Planning Cookbook:

http://www-01.ibm.com/software/brandcatalog/portal/opal/details?cata log.label=1TW101070

► Tivoli Application Dependency Discovery Manager Infocenter:

http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/index.jsp?to
pic=/com.ibm.ccmdb.doc_7.1.1/ccmdb_welcome.htm

 IBM Tivoli Change and Configuration Management Database Version 7 Release 1.1 Infocenter:

http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/index.jsp?to
pic=/com.ibm.ccmdb.doc_7.1.1/ccmdb_welcome.htm

 Tivoli Change and Configuration Management Database Version 7 Release 1.1 - Integration Adapter for Tivoli Application Dependency Discovery Manager Implementation Guide:

http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/index.jsp?to
pic=/com.ibm.ccmdb.doc_7.1.1/ccmdb_welcome.htm

Tivoli Provisioning Manager V7.1.1 User Guide:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ib
m.tivoli.tpm.scenario.doc/tpm_user_guide.pdf

► Tivoli Provisioning Manager for OS Deployment V7.1.1 User Guide:

http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm .tivoli.tpm.osd.doc/osd_install_guide.pdf

InfoSphere Federation Server link on IBM website:

http://www.ibm.com/shop/publications/order

► IBM website, Service Delivery Solutions:

http://www-01.ibm.com/software/tivoli/solutions/service-delivery/

Novell website for SuSe Linux patches:

http://www.novell.com/products/opensuse/downloads/ftp/int_mirrors.ht
ml

 Document for using SSL security certificate in Tivoli Provisioning Manager V7.1.1:

http://tioid2.torolab.ibm.com:8888/help/index.jsp?topic=/com.ibm.tiv
oli.tpm.scenario.doc/spe/septb1_1.html

▶ Web Services Resource Framework (WSRF) services overview:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/index.jsp?to
pic=/com.ibm.tivoli.tpm.soa.doc/wsrf/cwsr_wsrfsv.html

► IBM Tivoli Integration Composer overview:

http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/topic/com.ib m.srm.doc_7.1/installing/src/c_ccmdb_icoverview.html

► IBM ServerGuide Scripting Toolkit WinPE 2.x download link:

http://www-947.ibm.com/systems/support/supportsite.wss/docdisplay?ln docid=SERV-TOOLKIT&brandind=5000008

• Details on how to install the Web Administration Tool:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?top ic=/com.ibm.IBMDS.doc/install27.htm

Details on how to use the Web Administration Tool:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?top ic=/com.ibm.IBMDS.doc/install18.htm

► Tivoli Provisioning Manager Version 7.1.1 Migration Guide:

http://publib.boulder.ibm.com/infocenter/tivihelp/v28r1/topic/com.ib
m.tivoli.tpm.ins.doc/tpm_migrate_guide.pdf

► Document for configuring the Web server plug-in for Secure Sockets Layer:

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topi
c=/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/tsec_httpserv.h
tml

How to get Redbooks

You can search for, view, or download Redbooks, Redpapers, Technotes, draft publications and Additional materials, as well as order hardcopy Redbooks publications, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

720 IBM Tivoli Provisioning Manager V7.1.1: Deployment and IBM Service Management Integration Guide

Index

Α

Activities and Tasks application 275 Actual Configuration Items 286, 293 Add Object actions 241 administrative workstation 39, 44-46, 89 AES (Advanced Encryption Standard) 109 Agent Manager (AM) 30, 33, 39, 49-53, 75, 84, 88, 107, 116, 700, 707 AIX environment 397 AIX Fix Center 396 AIX patch scan 401 update 401 Alert At 153 Apache server instance 191 Application 5 Application Cluster 5 Application Designer 166 application tier structure 201 Apply Configuration Changes 284 authentication 10 authorization 10 Authorized Configuration Items 286 automatic binding rules. 420 automation package 27, 29, 32, 216, 222, 225, 376, 381, 395, 399, 522, 524 Automation Package Development Environment (APDE) 32, 65, 228, 352 Automation Packages 4

В

baremetal 18 baremetal install 18 Base Services Installer (BSI) 516 batchSize 206 BEA home 212 Bill of Material (BOM) 412 BIRT reports 141 Bitvise 199 Bulletins 141 Business Intelligence and Reporting Tools (BIRT) 15 business process workflows 352

С

Capacity Planning Cookbook 34, 48 casprofile 603 casprofile profile password 616 CASservice.zip 528 Caution At 153 ccexport 363 ccimport 363 CCMDB middleware 61-62, 80 CCMDB V7.1.1.5 59, 95, 325, 328 CDS depot creating 113 implementation 115 server 53 CDS_Depot_Stack 112 CDS Set Parameter 118 centralized control 39, 109 Change Management 23-24, 193, 326, 329-330, 333 Change Management integration IBM Tivoli Change and Configuration Management Database (CCMDB) 326 Change Management process 326 overview 326 Types of Changes Emergency Change 327 Pre-approved Change 327 Standard Change 327 IBM Tivoli Release Process Manager 327 ITIL based Change Management 326 Problem Management 328 scenario 328 scenario users 330 users and groups definition 330 Change Manager 187 Classification 307 client.JobM anagementServiceClient 533 CMDB 196-197, 275-276, 278, 285-287, 289, 292-294, 362 Command Line Interface (CLI) 115, 359, 525 Common Agent Service (CAS) 43, 75

common agent services code 32 Common Data Subsystem (CDS) 25 Common Inventory Technology (CIT) 33, 255 common PMP 70 company sets 279 Compliance Analyst 65, 227, 239, 243, 257, 374, 387, 391, 394, 400, 402-403 compliance check 219-220, 222, 224-227, 237, 241, 243, 245-246, 248, 252-255, 261, 265, 276, 376, 388, 400-401 Compliance Management 29, 217-219, 223, 237, 246, 531 typical scenario 217 Compliance Management with TADDM built-in auto-remediation 220 security 222 software and patch 221 software configuration 221 compliance and remediation process 223 compliance checks 219 security 219 software configuration 220 software installation 219 features 218 scenario 225 scenario implementation 231 compliance recommendation 374, 376, 378, 385, 391 compliance scan 254-255, 257, 265, 377, 385, 390, 394, 401, 403 ComplianceRecommendation.Remediate 220 ComplianceRecommendationGroup.Remediate 220 configuration change 29–30, 33, 63, 93, 97, 282-284 configuration examiner 523 Configuration Item (CI) 12, 23, 182, 197, 224, 226, 240, 250, 261, 276-278, 285-288, 293-296, 298, 310, 318, 320, 326, 343 183 actual state 286 extended attributes 12 Import 286 Configuration Librarian 254 configuration management 12, 20, 23, 27, 29, 184-185, 276-277, 283-288, 295 Configuration Management Database (CCMDB) 26 configuration setting 44, 95, 99, 102, 220, 224, 231, 243, 250, 263

configuration template 112, 117–118 connection parameter 289–291, 365 Console.log 538 consolefile 521 copy file 8 cron task 154 execution process 331 field 106 Setup Application 331 Cron Task Application 331 CTG_MAXIMO_SERVLET_URL 666

D

data center model (DCM) 5, 7 data center model objects 7 data integration 349-351, 362-366 environment 365 other IBM solutions 365 data model 12, 23, 29, 31, 38, 114, 196-197, 200, 211, 214, 224, 350, 362, 364, 374–376, 380, 383, 387-388, 390-391, 396, 399, 401, 407 database heap size 284 dbgw.exe 412 DCMQuery 352-353 default insert site 282 default service access point 50 demilitarized zone (DMZ) 54 deployment engine (DE) 26, 29-31, 56, 360, 376, 398, 511, 516, 520, 531, 536, 540 Deployment Specialist 65, 193, 228, 261, 301-302, 305, 314, 316, 318-320, 322-323, 329-330, 342, 349, 351, 374, 392, 402-403 new activity 318 depot server 39, 108, 110, 112-114, 121, 131, 381, 391, 393, 529, 531-532 IP address 114 Device Management Service (DMS) 33 Device manager federated agents 120 Device manager federator 120 device manager service (DMS) 31, 120, 533 Device.CopyFile 50 Device.ExecuteCommand 50, 352, 355, 357-358 DHCP server 351, 412 directory server 32, 38-39, 41, 46-47, 49, 700 user authentication 32 Discovery Library Adapter (DLA) 11, 13, 364 Discovery Library Adapter workflow 363 download plan 109, 534

dummy password 215 Dynamic Content Delivery (DCD) 33 dynamic content delivery (DCD) 109 management center 109 regions 110 zones 110 Dynamic Depot Server Selection (DDSS) 109 Dynamic Host Configuration Protocol (DHCP) 411

Ε

Eclipse environment 122 emulate PXE 413 Enterprise Java Beans (EJB) 4 execute command 8

F

Federal Information Processing Standard (FIPS) 11–12 File and Printer Sharing 385 file repository 121, 126, 128–129, 395, 533, 537 Firefox 354 fully qualified domain name (FQDN) 114, 529

G

gateway agent 55 gateway manager 55 gateway service 56 gateway.private 56 Global Issue 313 globally unique identifier (GUID) 197, 210 Go To menu 141 golden master image 416 gtar command 697

Η

Hardware Abstraction Layer (HAL) 445 Hardware Discovery 204 heartbeat function 33 HMC (Hardware Management Console) 12 host name 30, 66, 92, 99, 213, 283, 289, 291, 383, 407

I

IBM Autonomic Deployment Engine 562
IBM HTTP Server 38, 191, 221, 226, 231, 248–250, 257–258, 262–263, 268
Version 1.3 201

IBM Key Management application 56 IBM Open Process Automation Library (OPAL) 32 IBM Rational Test Lab Manager (RTLM) 18 IBM Redbooks Web site 711 IBM Service Management Products 26 IBM Tivoli Application Dependency Discovery Manager 136 IBM Tivoli Asset Management 58 IBM Tivoli common agent 519, 526 IBM Tivoli Integration Composer 67, 197, 277, 286-288, 362, 365 7.1.1 199 server 288 IBM Tivoli Monitoring agent 369 IBM Tivoli Monitoring Agent for Tivoli Provisioning Manager 503 configuring 498 documentation 503 functions 498 installing support files 502 overview 498 predefined workspaces 503 sample workspaces data 503 IBM Tivoli Monitoring documentation 502 IBM Tivoli Monitoring infrastructure 502 IBM Tivoli Provisioning Manager V7.1.1 3, 11, 371-372 components 35, 68 InfoCenter 57 installation 68, 101 Base Services install 70 core components 75 pre-install Cygwin 68 pre-installation steps 63 Web components 89 interface 327 post-installation step 65 user interface 65 workflow 309, 354, 360-361 IBM Tivoli Release Process Manager 327 IBM Tivoli Service Request Manager 136, 271 IBM Tivoli Service Request Manager V7.1.0.4 58 IBM Tivoli Software Support team 523 IBM WebSphere Application Server Version 6.0 202 Version 6.1 202 ikeyman.bat 56 ikeyman.sh 56

Incident Analyst 187, 301-302, 312, 314, 316, 338 Incident Management integration 271-272, 275, 277, 294, 300-301, 303.309 integration scenario 271, 278, 294, 300 process 271, 273, 294, 300 scenario 271, 276-278, 285-286, 296, 300-301, 330 Incident Management integration 271 ITIL based Incident Management Continual Service Improvement 273 Incident Management process 273 Service Design 272 Service Operation 273 Service Strategy 272 Service Transition 273 lab environment 276 posts-installation tasks for CCMDB 278 create a general ledger account 280 create a general ledger account component 280 create currency codes 278 create default insert site 282 define an organization 279 define item and company sets 279 prerequisites steps 277 Tivoli Service Request Manager 274 overview 274 Service Catalog management 274 Service Desk functionality 274 Service Desk management 274 incident owner 301, 307, 312, 322-323, 329-330, 335-336 Incident Specialist 187 Incident Template 301, 303–304, 307, 313–317 Information Technology Infrastructure Library (ITIL) 272, 326-328 Install common agent task 519 install.log 519 installed Configuration Item authorized Configuration Items 218 InstallShield program 241 Instance Administration Tool 103 Integrated Solutions Console (ISC) 103 integration scenario 57, 59, 271–272, 275, 277, 279, 289, 291–293, 300–301, 303, 305, 309, 313, 347 Integration with non-IBM solutions 347 data federation

considerations 366 IBM InfoSphere Federation Server 367 integration types data federation 350 data integration 349 considerations 362 data importing and exporting 363 DCMExport 363 Discovery Library Adapter 364 IBM Tivoli Integration Composer (ITIC) 365 XMLImport 363 data integration summary 365 functional integration 349 summary 361 overview 349 Internal priority field 307 IPv6 enablement 14 IPv6 support 14 ISBN 0113310455 326 ISBN 0113310463 326 ISBN 0113310471 326 ISBN 011331048X 326 ISBN 0113310498 326 item sets 279 **ITIL** framework 274 ITIL processes 273 **Continual Service Improvement** Improvement Planning 273 Measurement and Control 273 Process Assessment and Analysis 273 Service Assessment and Analysis 273 Service Level Management 273 Service Measurement 273 Service Design Availability Management 272 Capacity Management 272 Information Security Management 272 Service Catalog Management 272 Service Continuity Management 272 Service Level Management 272 Service Portfolio Management 272 Supplier and Contract Management 272 Service Operation Access Management 273 Incident Management 273 Monitoring and Event Management 273 Problem Management 273 Request Fulfillment 273

Service Strategy Demand Management 272 IT Financial Management 272 Market Intelligence 272 Risk Management 272 Service Portfolio Management 272 Strategy Generation 272 Service Transition Acquire, Build, Test Release 273 Change Management 273 Deployment, Decommission, and Transfer 273 Knowledge Management and Service Knowledge System 273 Performance and Risk Evaluation 273 Service Asset and Configuration Management 273 Service Release and Deployment Planning 273 Service Release, Acceptance, and Test and Pilot 273 Testing 273 Continual Service Improvement 326

ITIL V3

Service Design 326 Service Operation 326 Service Strategy 326 Service Transition 326

J

Java Runtime Environment (JRE) 122, 126 javaplugin.TCACopyFile 538 Job Management Service (JMS) 39, 88 job plan 187, 193, 304–308, 313, 317–318, 329, 339, 342

Κ

KeepAlive 258 Key Performance Indicators (KPIs) 153 KPICronTask 154 Korn shell 42

L

lab environment 57, 68, 196-197, 226, 271, 276, 284, 289, 291-293, 295 Idapadd command 60 Lightweight Directory Access Protocol (LDAP) 38, 43, 103-104, 107 log file 123, 521–522, 525, 528, 531 initial log4j.log level configuration 521 log4j.appender 521 log4j.prop file 520, 522 log4j-util.prop 522 log4j-util.prop file 520 log-details position 537–539 logical device 8 Logical Device Operation (LDO) 4, 8, 354, 379 Logical Management Operations (LMO) 354 logical operation 4 LogPackagetimestamp.zip 523

М

mail.smtp.host 283 managed target computer provisioning workflows 31 manager.Stat usUpdateProcessor 539 maxadmin 227 maxadmin user 304 Maximo database 63, 66, 93, 97, 282-284, 289, 292 Maximo products 20 MaxKeepAliveRequests 258, 269 maxuproc 692 MD5 (Message-Digest algorithm 5) 109 messagefile 521 metadata 23 Microsoft Active Directory discovery 30 Microsoft Automated Deployment Services (ADS) 413 Microsoft Setup program 241 Microsoft Windows Server Update Services (WSUS) 372-373 migration 543 artifacts migration 544 assigning the host names 625 backing up the LDAP server 554 backing up Tivoli Provisioning Manager Version 5.1.1.2 591 complete the property file 577 configuring SSL with IBM HTTP Server 657 core components installation 567 creating the database and database server user 565 environment used 545 gradual phased migration 543

installing the base services and the Web components 616 installing the middleware 560 migrating access groups 649 migrating file repositories 556 migration tasks for the Tivoli Provisioning Manager Version 5.1.1.2 system 591 migration tasks for the Tivoli Provisioning Manager Version 7.1.1 system 596 objectives 543 overview 548 pre-migration tasks 550 pre-migration tasks for Tivoli Directory Server 554 prerequisites for migrating automation packages 555 restoring the 5.1.1.2 LDAP information to 7.1.1 645 Tivoli Provisioning Manager Version 7.1.1 installation 559 upgrading the common agent to version 1.3.2.29 552 upgrading the provisioning server to version 5.1.1.2 551 validating the migration 645 multipath I/O function 17 multiple network interface card 52 multi-server topology 46 MXServer 64, 70, 93, 95, 97-98

Ν

N-1 principle 543 NetBIOS over TCP/IP 50 network interface cards (NICs) 52 noncompliance issue 29, 219–220, 222, 225, 257, 261 non-SSL port 65, 92, 96, 99

0

Open Process Automation Library (OPAL) 32, 34, 48 Open Services Gateway Initiative (OSGI) 32 openssh 690 operating system (OS) 18, 29, 39, 41–42, 58, 113, 121–122, 130, 189–191, 199, 202, 208, 343, 375–376, 381–382, 385, 388, 393, 395, 399, 401, 403, 513, 528

official patches catalogs 343 system accounts 41 operating system provisioning 409 AIX platforms 451 bindings 454 automatic binding rules 454 manual bindings 459 cloning computers 489 deployment basics 415 deployment from CD/DVD 419 DHCP configuration options 413 Options 1, 6, and 15 415 Options 60 and 43 413 Options 66 and 67 414 golden master image 416 hardware configuration 417, 460 Linux platforms 451 parent-child boot servers 423 point-in-time snapshot image 416 software modules 417, 426 Solaris platforms 451 Tivoli common agent software modules 452 Tivoli Provisioning Manager for OS Deployment architecture 411 unattended image 416 unattended setup 469 AIX 487 golden master image 490 Linux 483, 489 Solaris 488 Windows 2003 469 Windows Vista/2008 476 Windows platforms custom action on the target computer 438 including a Windows driver in a deployment 430 Microsoft Installer (MSI) 427 Windows HAL 445 Windows Vista/2008 436 Operational Management Product (OMP) 25 Oracle Database 38, 47, 120, 201, 589 9i 201 Oracle updateDCM workflow 190 Oracle WebLogic Server 196 10g Release 3 211 8.1 201 9.2 199, 201, 211, 215 9.2 installation 211 Oracle WebLogic Server 10.3 199, 201

organization 279 OSGi environment 359

Ρ

package size 524 packagelog 523 packageLogs 523 packageLogs tool 523 packageLogs.cmd 523 packageLogs.sh 523 patch catalogue 374, 376, 380 Patch Management 11, 15, 369, 371-372, 374-377, 380-381, 384, 392, 396-397, 402, 405-406.408 AIX environments 396 acquiring patches 399 approving compliance recommendations 401 distributing patches 402 installing patches 402 scanning for missing patches 401 setting up compliance 400 uninstalling patches 403 verifying compliance results 403 basic steps 404 big picture 381 important enhancements 369 in large Windows environments 380 acquiring patches 385 approving compliance recommendations 391 generating patch compliance reports 394 patch approval 387 scan for missing patches 388 setting up compliance check 388 verification of compliance results 394 in small Windows environments 376 approval of recommendations 378 ComplianceRecommendationGroup.Remed iate 379 Default Compliance Recommendation Gr oup_Remediate 379 flow 376 installation of missing patches 379 verification of patch installation 379 predefined roles 374 requirements 374 solution 372

SUSE Linux Enterprise environments 404 SUSE Linux patch server 405 SUSE Linux update site model 406 patch name 387 physical partition size (PP size) 686 PMP (process manager product) 70 Point-in-Time Snapshot 496 PollingInterval parameter 112 Preferred upload server check box 114 Priority Matrix 275 Problem Analyst 187, 329–330, 337 Problem Specialist 187 process workflow runtime 20-21, 23 Program actions 241 Provisioning Group 373 proxy relay 55 proxy server 373, 405, 407 default port 383 PXE boot ROM chip 413 PXE network boot 413 PXE remote-boot capability 412 Python 69

R

Rational Test Lab Manager (RTLM) 18 rbagent.linux process 412 reboot time 500 recommendation workflows 262-263 Red Hat Enterprise Linux 202 Red Hat Linux operating system 381-382 release 7.3 202 Redbooks Web site 719 Contact us xxiii Redbooks-Inc 185 rembo 412 rembo.exe 412 Remediation action 221-222, 224-225, 237, 261, 265 Remote Execution and Access (RXA) 50 remote procedure call (RPC) 50 Remove Object actions 241 Request For Change (RFC) 193 resource pool 5 ReturnCode 355 RPM package 241

RXA protocol 378, 385, 537

S

sample KPI 154 sample-compliance-validation automation package 222 Sarbanes-Oxley 218, 223 scalability statement 34 scalable distribution infrastructure (SDI) 11, 26, 30-31, 107, 113, 116, 133, 197, 237, 519, 531 scriptlet 358 SdiTaskDispatcher 532-533 Secure Shell (SSH) 50 Secure Sockets Layer (SSL) 55, 75 Secure SSL 51-53 Security Compliance Manager (SCM) 33, 255 Security Compliance Manager collectors technology (SCM) 255 security group 16, 102-103, 227-228, 230, 302-303 Select Action drop-down menu Authorized Configuration Item 295 GL Account Configuration 280 GL Component Maintenance 280 Server Message Block (SMB) 50 Servers definition 5 Service Access Point (SAP) 5 service access point (SAP) 116, 189, 214, 237-238, 383, 398, 407 service access points (SAP) 50 Service Catalog management 274 Service Desk management 274 service level agreements (SLAs) 18 service level priority 5 Service Request 182-184, 186, 188, 274-276, 286, 296, 298, 300-301, 310-313, 320, 325, 327-330, 333-335, 337-338, 346 corporate service desk 274 Service Update Management Assistant (SUMA) 396 setup.ini 69 simple multicast protocol (MTFTP) 412 simple power application 139 sles-operating-system 408 SOAP commands 31 SOAP Service 350, 359-361 decentralized and stateless request model 360 SOAPCli 359

Software Assistant (SWA) 372 software catalog 126-127 software catalogue 112 software configuration 18, 197, 218, 220-221, 224, 226, 243, 248-253, 256, 265 check 12, 226, 250-253 compliance 220, 251 information 249 template 12, 224, 248-249 software definition 126, 130, 221, 380, 387 installable files 130 Software Discovery 204 software distribution 30, 39, 101, 107, 121, 131, 182, 198, 509, 511, 520, 531, 536 software installation 13, 189, 192, 211, 219, 221, 243.355-356 software compliance rules 192 Software Installation Engine (SIE) 33 software module 131, 221, 226, 241, 243-245 software package 4, 113, 121-122, 125, 129, 228, 241-243, 327, 519, 531, 535, 537, 540 local build 129 software package block (SPB) 101, 121, 128-129, 132 software package definition (SPD) 128-129 software package distribution 531 Software Package Editor (SPE) 122–129, 241–242 environment 122 folder 123 main window 129 preference 125 tree view display 129 software product 5, 126-127, 131, 208-209, 219, 225, 243, 377, 384 software resource template 6, 211-212, 215 software stack 4-5, 379 SoftwareInstallable DCM object 7 SoftwareInstallation.Install 221 SoftwareInstallation.Uninstall 221 SoftwareModule.Install 352, 355, 537 SPB_Synch_Install 539 SPB TCA Install 537 SPBHandler 535 ssh connection 196 sshd config 695 SSL port 65, 92, 96, 99 standard navigation bar 140 standard power application 140 Start Center 11, 16, 136, 141, 228, 334, 339, 387,

389 Portlets Chart Options 155 Column Display 155 Display Options 155 stateful Web services 359 Sun Update Connection Enterprise 372 SUSE Linux Enterprise Server 10 404 8 202 SUSE Linux Enterprise Server (SLES) 404, 407 SUSE Linux patch server communicate 405 model 405 suse patch 408 SyncTADDMLaunchEntries.xml 95 Sysprep 491 Sysprep tool 491 System actions 241 system reboot 500

Т

TADDM APIs 197 TADDM collection objects 201 TADDM Discovery 188-189, 191-192, 195-197, 200, 202-215, 220, 224, 233-234, 236, 249-250, 253, 256, 264, 268, 276–277, 297, 350 configuration 206-207 hardware 201, 208 information 207 mechanism 201 scope 207 TADDM discovery method 197 TADDM integration 196 configuring communication to discovered computers and applications 213 configuring discovery 206 controlling software applications 215 creating a discovery 204 defining discovery scope 207 discovering applications 203 installed components 198 life cycle 199 running the discovery 207 supported applications 201 viewing application configuration data 210 working with discovered applications 209 TADDM sensor 199, 203

TADDMDiscovery automation package 202 target CI 340 target computer 29, 31, 50-51, 108, 112-113, 116, 122, 209, 226, 231, 237, 240, 253, 372-375, 377-378, 380-381, 384, 398-402, 409, 420, 441, 450 common agent 385 compliance scan task 390, 401 compliance state 388 compliance status 395 concurrent compliance scan tasks 390, 401 different groups 408 large numbers 531 service command 528 target system 44, 241, 309 automation activities 309 Task Configuration 331 Task Management 11, 16, 26 task status 238, 378, 386, 389, 392-393, 399, 401-402, 404, 519 Tasks Information Time Range 498 TCA.Create.EO.SAP 116 TCA PingAgent 526 TCP-to-ODBC/JDBC gateway service 412 temporary directory 212, 288 Ticket Templates 275, 308 Ticket Templates application 275 Tivoli Change and Configuration Management Database (CCMDB) 196 Tivoli common agent 31-32, 39, 107, 112, 115-117, 197, 199, 224, 237, 374, 418, 426, 452, 454, 519, 526–528, 531, 533, 548, 645 log level 527 multiple firewalls 55 polling activity 197 Tivoli common agent log file collector 528 Tivoli Enterprise Monitoring Server 502 Tivoli Enterprise Portal 502, 507 Tivoli Enterprise Portal Server desktop client 502 Tivoli process automation engine 10–11, 17, 20, 23, 25-27, 135, 352, 365 benefits 20 Common Configuration Services 23 Common Data Subsystem 23 Common Process Workflow Runtime and Services 23 Common User Interface 22 core capabilities 21

overview 20 platform 20, 25, 135 portfolio of applications 24 security framework 102 Service Management 23 Tivoli Provision Manager V7.1.1 Core Components Installer 517 Data Center Model 249 database 224 PMP 517 server 233 Tivoli Provisioning Manager Discovery Library Adapter (DLA) 13 Tivoli Provisioning Manager External Wiki 512 Tivoli Provisioning Manager for OS Deployment architecture 411 product components 411 Tivoli Provisioning Manager for OS Deployment Embedded Edition 557 Tivoli Provisioning Manager V7.1.1 27 architecture 19 components architecture 27 automation 29 Automation Package Developer Environment (APDE) 32 compliance and remediation 29 data model 29 deployment infrastructures 30 discovery 30 external management applications 32 Open Process Automation Library 32 Operator and administrator console 31 Provisioning database 29 Provisioning server 29 reporting 30 Tivoli common agent 32 user directory 32 Web Services interface 31 client value 17 compliance and remediation with TADDM 217 components automation package 29 Automation Package Developer Environment (APDE) 32 compliance and remediation 29 data model 29 deployment engine (DE) 31 deployment engine infrastructure 31 deployment infrastructures 30

discovery 30 External management applications 32 IBM Open Process Automation Library (OPAL) 32 Operator and administrator console 31 provisioning database 29 provisioning server 29 reporting 30 Scalable Distribution Infrastructure (SDI) 30 Tivoli common agent 32 User directory 32 Web Services interface 31 concepts 4 Application 5 Application tier 5 Automation package 4-5 Capability 5 Customer 5 data center model (DCM) 5 Logical operation 4 Requirement 5 Resource pool 5 Servers 5 Service Access Point 5 Software Configuration Template 6 Software product 5 software stack 5 Transition 5 Workflow 4 data center model (DCM) 224 documentation 219 enhancements compliance 12 discovery 12 Discovery Library Adapter (DLA) 13 Federal Information Processing Standard 140-2 12 installation 13 IPv6 addressing 14 migration 14 operating systems management 14 Patch Management 15 reporting 15 security 16 Start Centers 16 target computers 16 task management 16 virtualization 17 groups 159
TPADMIN 159 TPCOMPLIANCEANALYST 162, 164 TPDEPLOYMENTSPECIALIST 161 **TPDEVELOPER** 165 GUI differences with V5.1.1.2 167 high availability and data integrity 34 IBM Tivoli Monitoring Agent for Tivoli Provisioning Manager 497 Incident Management integration with Tivoli Service Request Manager 271 installation 57 installation considerations 38 installation planning 37 integrated Service Management 181 integration installation 57 assumptions and rules 58 install CCMDB V7.1.1 middleware 60 install Service Request Manager fix pack 4 63 install Tivoli Application Dependency Discovery Manager V7.1.2 60 install Tivoli Integration Composer V7.1.1 66 install Tivoli Provisioning Manager V7.1.1 65 installing CCMDB on top of Tivoli Provisioning Manager V7.1.1 92 installing Tivoli Service Request Manager on top of Tivoli Provisioning Manager 7.1.1 97 other samples of integrated environments 92 run Tivoli Provisioning Manager V7.1.1 pre-installation steps 63 steps to install 59 upgrade CCMDB to fix pack 5 62 upgrade the WebSphere Application Server 63 upgrade Tivoli Integration Composer to fix pack 4 67 integration with non-IBM solutions 347 migration 541 operating system provisioning 409 overview 3 authentication 10 Provisioning 4 security 10 Patch Management 371 Problem and Change Management integration 325

scalability 34 Start Center overview 139 Bulletins 141 configuring 143 Field Buttons 142 Find 141 Go To menu 141 Help 141 Profile 141 Query 141 Reports 141 Select Action 142 Sign Out 141 simple power application 139 standard navigation bar 141 standard power application 140 Web Replay 141 Start Center templates 138, 159 Automation Package Developer 165 Compliance Analyst 162 Deployment Specialist 161 Provisioning Administrator 159 Provisioning Configuration Librarian 164 TADDM Discovery 195 Tivoli process automation engine based user interface 137 troubleshooting 511 user interface customization 138 Tivoli Provisioning Manager Version 5.1.1.2 541 Tivoli Provisioning Manager Version 7.1.1 installation 559 migration 543 upgrade 543 Tivoli Release Process Manager V7.1.1 328 V7.1.1.5 328 Tivoli Service Request Manager 17, 58, 92, 183, 186-187, 271, 274-275, 277, 301, 327-328, 330, 347, 349, 351, 365 Configuration Item 286 Fix Pack 5 328 Incident Management process 273 integration capabilities 271 overview 271, 274 V7.1.0.4 59 V7.1.1 92 Tivoli Storage Productivity Center (TPC) 18 Tivoli System Automation for Multiplatforms 34 Toolbox Web Replay

7.1.1 198 V7.1.1 70 TOPCICLASS 287 TPDEVELOPER role 241 tpm5112backup.sh 592 TpmAuthenticator 51 TPM-ITM agent 43 transitions 5

U

ulimit 692 umask 42, 692 unzip command 554 upgrade 543 uploading 39 Urlgrabber 69 user interface 20–24, 38, 62, 65–66, 93–94, 96, 98, 100 UUID (Universal Unique Identifier) 421

V

Virtual Member Manager (VMM) 16, 106–107 Virtualization capabilities 26 virtualization management 17 virtualization technology 18 VLAN 7 VMMSync 106 VMMSYNC crontask 144 VVMSYNC cron task 331

W

wasadmin 103. 228 Web interface 22, 30-31, 115, 377, 384, 519, 521, 525 export capabilities 30 workflow log 525 Web Replay 141 Web Services Description Language (WSDL) 360 Web Services Resource Framework (WSRF) 31, 359 WebLogic instance 212 WebLogic Server 199, 201, 209, 211, 215 WebSphere Application Server 38, 41, 47–49, 60, 62-65, 67, 70, 75, 81, 92-95, 97-99, 187, 190, 198, 201-202, 208, 285, 354 administration 96 appropriate patch 187

MXServer application 285 user 703 Windows Antivirus 222 Windows Power-On Password 222 Windows screen saver 222 Windows Services 519 Windows Update Agent (WUA) 373 Windows User Password policy 222 Windows XP 385 workflow 56, 118, 128, 133, 222, 255–256, 261–263, 268, 356, 376, 378–379, 384, 386, 391, 398, 519, 524–526, 528, 537, 539 workflow definition 4 workflow log 524

Х

xIC.rte 6.0 runtime code 399 xml file 115, 386, 390, 393

Y

Yum Update Proxy (YUP) 406 YUP Package Manager 405

Z

ZENworks 405 zone 110



(1.5" spine) 1.5"<-> 1.998" 789 <->1051 pages

IBM Tivoli Provisioning Manager V7.1.1: Deployment and IBM Service Management Integration Guide



Learn how to implement Tivoli Provisioning Manager V7.1.1 in your environment

Experiment with IBM Service Management integration scenarios

Learn TPM troubleshooting and how to migrate from V5.1.2 troubleshooting This IBM Redbooks publication is a complete reference for the recently available Tivoli Provisioning Manager V7.1.1 product. This document provides information valuable to those who want to plan for, customize, and use the IBM Tivoli Provisioning Manager V7.1.1 product to automate and manage IT provisioning and integrated IT service management processes in their environments. It includes five parts:

Concepts and architecture: Provides an overview of provisioning concepts and introduces Tivoli Provisioning Manager V7.1.1 concepts and architecture, in perspective with the overall Tivoli process automation engine platform.

Planning for deployment and implementation: Discusses planning considerations for deploying Tivoli Provisioning Manager V7.1.1 in a production environment, installation and initial customization of product components, and a sample software deployment scenario to verify the successful deployment of the product.

The new GUI and IBM Service Management integration scenarios: Covers value added integration scenarios with several IBM Service Management products such as TADDM, IBM Tivoli Service Request Manager, and CCMDB. Also included is a section explaining the Start Center based new GUI, and a section on implementing Tivoli Provisioning Manager V7.1.1 with a non-IBM configuration management database.

Patch Management, Operating System Deployment, and IBM Tivoli Monitoring Agent for Tivoli Provisioning Manager: Introduces several scenarios on Patch Management and Operating System Deployment, Also provided is an overview of the IBM Tivoli Monitoring Agent for Tivoli Provisioning Manager.

Troubleshooting and migration from Tivoli Provisioning Manager V 5.1.2: Discusses troubleshooting tips and migration from V 5.1.2.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information: ibm.com/redbooks

SG24-7773-00