HiCommand® Storage Services Manager Installation Guide

Version 5.1
MK-93AI001-07

First Edition

Table of Contents

Preface *About This Guide* . . . . . ***xxix***

Intended Audience xxix
Where to Find Additional Information xxx

Chapter 1 *Overview* ***1***

About this Product 4
Storage Management Terms *5*
Key Benefits *5*
Key Features *5*
Software Requirements *6*
Web Browser Configuration Requirements 6

Chapter 2 *Installing the Management Server on Sun Solaris 9*

Step 1 - Install the Oracle Database (Solaris) 10

Before Installing the Oracle Database 11

Prerequisites 11

Installing the Database on a Secure Shell (SSH) Server with X Forwarding 13

Installing the Database for Configurations Other Than SSH with X Forwarding 18

Installing the Oracle Patch 23

Step 2 - Install the Management Server 27

Step 3 - Verify that Processes Can Start 29

Step 4 - Verify You Can Connect to the Management Server 30

Installing the Java Plug-in on Sun Solaris 32

Configurations Required for Discovering EMC CLARiiON Storage Systems 33

Removing the Management Server 34

Porting the Management Server Across Operating Systems 36

Upgrading the Management Server 38

Step 1 - Stop AppStorManager 39

Step 2 - Export Your Existing Database 39

Step 3 - Upgrade and Start the Windows Proxy 40

Step 4 - Upgrade the Management Server 40

Step 5 - Required Changes for Discovered McDATA and Connectrix Switches 41

Step 6 - Remove and Rediscover Certain Elements 41

Step 7 - Perform Get Details 42

Step 8 - Re-add Remote Sites in Global Reporter 42

Step 9 - Rescan for File Servers 44

Chapter 3 *Installing the Management Server on Microsoft Windows* **.... 45**

Step 1 - Install the Oracle Database (Windows) 46

Installing the Oracle Database 47

Installing the Oracle Patch (Windows) 47

Step 2 - Install the Management Server 49

Step 3 - Verify that Services Can Start 51

Step 4 - Verify You Can Connect to the Management Server 51

Configurations Required for Discovering EMC CLARiiON Storage Systems 53

Removing the Management Server 54

Porting the Management Server Across Operating Systems 55

Upgrading the Management Server 57

Step 1 - Stop AppStorManager 58

Step 2 - Export Your Existing Database 58

Step 3 - Upgrade the Management Server 58

Step 4 - Required Changes for Discovered McDATA and Connectrix Switches 59

Step 5 - Remove and Rediscover Certain Elements 60

Step 6 - Perform Get Details 61

Important Information About Upgrading and Brocade Switches 61

Step 7 - Re-add Remote Sites in Global Reporter 62

Step 8 - Rescan for File Servers 63

Chapter 4 *Discovering NAS Devices, Tape Libraries, Switches and Storage Systems* **. 65**

Discovery Steps 66

Overall Discovery Tasks 66

Overview of Discovery Features 69

Setting Default User Names and Passwords 70

Adding an IP Range for Scanning *72*

Adding a Single IP Address or DNS Name for Discovery *73*

Modifying a Single IP Address Entry for Discovery *75*

Removing Elements from the Addresses to Discover List *76*

Importing Discovery Settings from a File *76*

Saving Discovery Settings to a File *77*

Step 1 - Discover Switches 78

SMI-S Switches Must Be Removed and Rediscovered After Upgrading *81*

Discovering Brocade Switches *81*

Brocade SMI-S Provider Installation Requirements (New Installations of the Management Server) 82

Verifying Brocade Rapid Program Is Set to 1 83

About Brocade Discovery (Specifying Brocade Discovery Using Fabric Access API or SMI-S) 83

Discovering CNT Switches *86*

Discovering Cisco Switches *87*

Discovering Sun StorEdge and QLogic Switches *89*

Changing the SNMP Trap Listener Port for Sun StorEdge Switches *90*

Discovering McDATA and EMC Connectrix Switches *91*

SWAPI Setting Through a Proxy 93

SNMP Setting Through a Proxy 97

Contacting a McDATA or Connectrix Switch Directly 100

Changing the Discovery Settings 102

Excluding McDATA and EMC Connectrix Switches from Discovery *103*

Viewing Log Messages *104*

Viewing the Status of System Tasks *105*

Duplicate Logs for Brocade Switches in Same Fabric 105

Step 2 - Discover Storage Systems, NAS Devices and Tape Libraries106
Discovering 3PAR Storage Systems 109
Discovering EMC Solutions Enabler 5.1 110
Excluding EMC Symmetrix Storage Systems from Discovery 112
Discovering EMC CLARiiON Storage Systems 114
Discovering Engenio Storage Systems 114
Discovering HDS Storage Systems 116
Excluding HDS Storage Systems from Discovery 117
Discovering HP StorageWorks EVA or MSA Arrays 118
Discovering HP StorageWorks XP Arrays 119
Discovering HP XP Arrays by Using Command View XP 120
Discovering HP XP Arrays by Using Command View XP Advanced Edition 121
Discovering HP XP Arrays by using the XP Provider 122
Discovering IBM Storage Systems 122
Discovering Sun StorEdge 3510 Storage Systems 124
Discovering Sun StorEdge 6920 and 6940 Storage Systems 126
Discovering Sun StorEdge 6130 Storage Systems 126
Discovering Xiotech Storage Systems 127
Discovering HP NAS Devices on Windows 128
Discovering HP NAS Devices on Linux 129
Discovering NetApp NAS Devices 130
Discovering Sun NAS Devices 131
Discovering HP and IBM Tape Libraries 132
Step 3 - Build the Topology 133
Building the Topology View 133
Modifying the Properties of a Discovered Address 135

Deleting Elements from the Product *136*
Deleting an Element Using System Explorer or Chargeback 136
Deleting Elements Using Discovery Step 2 (Topology) 137
Step 4 - Get Details 138
Get Details *138*
Stopping the Gathering of Details *140*
Excluding EMC Symmetrix Storage Systems from Force Device Manager Refresh *141*
Excluding HDS Storage Systems from Force Device Manager Refresh . . . *142*
Troubleshooting Mode 143
Managing McDATA and EMC Connectrix Switches 144
About Managing McDATA and EMC Connectrix Switches *145*
Adding McDATA and EMC Connectrix Switches *145*
Removing McDATA and EMC Connectrix Switches *146*
Swapping McDATA and EMC Connectrix Switches *146*
Assigning a File Extension in Netscape 7 147
Filtering Discovery Groups 148
Moving Elements to Another Discovery Group 148
Placing an Element in Quarantine 149
Removing an Element from Quarantine 150
Updating the Database with Element Changes 150
Notifying the Software of a New Element 151

Chapter 5 *Deploying and Managing CIM Extensions* ***153***
About Remote CIM Extensions Management 153
About SSH *154*
Copying the CIM Extensions to the Management Server *155*
Creating Default Logins for Hosts *155*
About the CIM Extensions Management Tool 156

Launching the CIM Extensions Management Tool *156*
Adding Remote Hosts *157*
Managing CIM Extensions on Remote Hosts *157*
Configuring CIM Extensions *158*
Status Icons *159*

Chapter 6 *Installing the CIM Extension for IBM AIX* ***161***

About the CIM Extension for IBM AIX 162
Prerequisites 163
Verifying SNIA HBA API Support 164
Installing the CIM Extension 165
Setting Up Monitoring 166
Starting the CIM Extension Manually 166
How to Determine if the CIM Extension Is Running 167
Configuring CIM Extensions 167
Changing the Port Number *168*
Configuring the CIM Extension to Listen on a Specific Network Card *168*
Additional Parameters *171*
Finding the Version of a CIM Extension 171
Stopping the CIM Extension 172
Fulfilling the Prerequisites 172
Rolling Over the Logs 173
Removing the CIM Extension from AIX 174

Chapter 7 *Installing the CIM Extension for SGI ProPack for Linux* ***175***

About the CIM Extension for SGI ProPack for Linux 176
Prerequisites 176
Verifying SNIA HBA API Support 177

Installing the CIM Extension 178
Starting the CIM Extension 179
How to Determine if the CIM Extension Is Running 181
Configuring CIM Extensions 181
Changing the Port Number 181
Configuring the CIM Extension to Listen on a Specific Network Card 182
Additional Parameters 183
Rolling Over the Logs 184
Stopping the CIM Extension. 185
Removing the CIM Extension from SGI ProPack for Linux 185

Chapter 8 *Installing the CIM Extension for HP-UX **187***

About the CIM Extension for HP-UX 188
Prerequisites 188
HP-UX 11i and 11.0 189
Software Requirements 189
HP-UX 11i 189
Driver Bundle Version 189
Driver Patch 189
HP-UX 11.0 189
Driver Bundle Versions 189
Driver Patch 190
Required Disk Space 190
Network Port Must Be Open 190
Verifying SNIA HBA API Support 190
Installing the CIM Extension 191
Starting the CIM Extension Manually 192
How to Determine if the CIM Extension Is Running 193

Configuring CIM Extensions 193
Restricting the Users Who Can Discover the Host 194
Changing the Port Number 194
If you have already added the host to the discovery list (Discovery > Setup) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports. 196
Configuring the CIM Extension to Listen on a Specific Network Card 196
Additional Parameters 197
Finding the Version of a CIM Extension 198
Combining Start Commands 198
Stopping the CIM Extension 198
Rolling Over the Logs 199
Fulfilling the Prerequisites 199
Removing the CIM Extension from HP-UX 200

Chapter 9 *Installing the CIM Extension for SGI IRIX 201*

About the CIM Extension for SGI IRIX 202
Prerequisites 202
Verifying SNIA HBA API Support 203
Installing the CIM Extension 203
Starting the CIM Extension 204
How to Determine if the CIM Extension Is Running 205
Configuring CIM Extensions 205
Changing the Port Number 205
Configuring the CIM Extension to Listen on a Specific Network Card 206
Additional Parameters 208
Starting the CIM Extension by chkconfig 208
Finding the Version of a CIM Extension 209

Stopping the CIM Extension. 209
Rolling Over the Logs 210
Removing the CIM Extension from SGI IRIX 210

Chapter 10 *Installing the CIM Extension for SUSE and Red Hat Linux* **. . 213**

About the CIM Extension for Red Hat Linux Advanced Server and SUSE Linux. 214
Prerequisites 214
Verifying SNIA HBA API Support 215

Driver Information for Verifying SNIA Emulex Adapters on Red Hat Linux 216

Driver Information for Verifying QLogic SNIA Adapters on Red Hat Linux 216

Driver Information for Verifying QLogic SNIA Adapters on SUSE Linux 216

Installing the CIM Extension 217
Starting the CIM Extension Manually 217
How to Determine if the CIM Extension Is Running 218
Configuring CIM Extensions 219

Changing the Port Number 219

Configuring the CIM Extension to Listen on a Specific Network Card 220

Additional Parameters 221

Finding the Version of a CIM Extension 222

Stopping the CIM Extension. 222
Rolling Over the Logs 222
Removing the CIM Extension from Red Hat or SUSE Linux 223

Chapter 11 *Installing the CIM Extension for Sun Solaris* **. 225**

About the CIM Extension for Solaris 226

Prerequisites 226
Verifying SNIA HBA API Support 227
Driver Information for Verifying SNIA Emulex Adapters 228
Driver Information for QLogic Adapters 228
Driver Information for AMCC/JNI Adapters 228
Driver Information for Sun Leadville branded QLogic or JNI Adapters. 229
Installing the CIM Extension. 229
Starting the CIM Extension Manually 230
How to Determine if the CIM Extension Is Running 231
Configuring CIM Extensions. 231
Restricting the Users Who Can Discover the Host 231
Changing the Port Number 232
Configuring the CIM Extension to Listen on a Specific Network Card 233
Additional Parameters. 234
Finding the Version of a CIM Extension 235
Combining Start Commands 236
Stopping the CIM Extension. 236
Rolling Over the Logs. 236
Removing the CIM Extension from Solaris. 237

Chapter 12 *Installing the CIM Extension for OpenVMS 239*

About the CIM Extension for OpenVMS. 240
Prerequisites 240
Installing the CIM Extension for OpenVMS 242
Installing the CIM Extension on a Standalone Host 242
Installing the CIM Extension on a Cluster 243
Starting the CIM Extension Manually 244

Finding the Status of the CIM Extension 244
Configuring CIM Extensions 245
Restricting the Users Who Can Discover the Host 245
Changing the Port Number 246
Configuring the CIM Extension to Listen on a Specific Network Card 247
Additional Parameters 248
Finding the Version of a CIM Extension 249
Combining Start Commands 249
Stopping the CIM Extension. 249
Rolling Over the Log Files 250
Increasing the Native Logging Level 251
Removing the CIM Extension from OpenVMS 251
Uninstalling the OpenVMS CIM Extension on a Standalone Host 251
Uninstalling the OpenVMS CIM Extension on a Cluster Host 252

Chapter 13 *Installing the CIM Extension for HP Tru64 UNIX* **. 253**

About the CIM Extension for Tru64 UNIX 254
Prerequisites 254
Software Requirements 255
Required Disk Space. 255
Network Port Must Be Open 255
SNIA HBA API Support 256
Installing the CIM Extension 256
Installing CIM Extension on a Standalone Host 256
Installing the CIM Extension on a Cluster. 257
Starting the CIM Extension Manually 258

How to Determine if the CIM Extension Is Running 259
Configuring CIM Extensions 259
Restricting the Users Who Can Discover the Host 259
Changing the Port Number 260
Configuring the CIM Extension to Listen on a Specific Network Card 261
Additional Parameters 262
Finding the Version of a CIM Extension 263
Stopping the CIM Extension 264
Rolling Over the Logs 264
Increasing the Native Logging Level 265
Fulfilling the Prerequisites 265
Removing the CIM Extension from Tru64 265
Removing the CIM Extension from a Standalone Host 266
Removing the CIM Extension from a Cluster 266

Chapter 14 *Installing the CIM Extension for Microsoft Windows* **. 267**

About the CIM Extension for Windows 268
Verifying SNIA HBA API Support 268
Emulex Host Bus Adapters 269
Driver Information for Verifying IBM Branded QLogic Adapters 269
Driver Information for Verifying QLogic Adapters 270
Driver Information for Verifying AMCC/JNI Adapters 270
Upgrading a Host with the Latest CIM Extension 271
Installation Steps 272
Installing the CIM Extension Using the Silent Installation 273
Configuring CIM Extensions 274
Changing the Port Number 274

Additional Parameters *275*
Rolling Over the Logs 276
Configuring the CIM Extension to Listen on a Specific Network Card *276*
Removing the CIM Extension from Windows 277

Chapter 15 *Installing and Discovering the Windows Proxy* ***279***

Installing the Windows Proxy 280
Discovering the Windows Proxy. 281
Configuring Windows Proxy Authentication 282
Decreasing the Maximum Java Heap Size 284
Removing the Windows Proxy 284

Chapter 16 *Discovering Applications and Hosts* ***285***

Step 1 - Discovering Your Hosts 285
Step A - Set Up Discovery for Hosts. *287*
Step B - Build the Topology *291*
(Optional) Step C - View the Topology *291*
Step D - Obtain Details *292*
Step 2 - Setting Up Discovery for Applications. 293
Monitoring Oracle *294*
Step A - Create the APPIQ_USER Account for Oracle 295
Removing the APPIQ_USER Account for Oracle 296
Step B - Provide the TNS Listener Port. 298
Step C - Set up Discovery for Oracle 10g 298
Discovering Oracle Clusters 299
Monitoring Microsoft SQL Server *300*
Switching to Mixed Mode Authentication. 301

Step A - Create the APPIQ_USER for the SQL Server 301
Step B - Provide the Microsoft SQL Server Name and Port Number . 303
Removing the APPIQ_USER Account for SQL Server 305
Deleting SQL Server Information 305
Monitoring Sybase Adaptive Server Enterprise *306*
Step A - Create the APPIQ_USER account for Sybase 306
Removing the APPIQ_USER Account for Sybase 308
Step B - Provide the Sybase Server Name and Port Number 309
Deleting Sybase Information 309
Monitoring Microsoft Exchange *310*
Adding Microsoft Exchange Domain Controller Access 310
Deleting a Microsoft Exchange Domain Controller 311
Step 3 - Discovering Applications 311
Step A - Detect Your Applications *312*
Step B - Obtain the Topology *313*
Step C - Obtain Get Details *313*
Changing the Oracle TNS Listener Port 315
Adding/Modifying Microsoft Exchange Domain Controller Access . . . 316
Changing the Password for the Managed Database Account 317
Obtaining Disk Drive Statistics from Engenio Storage Systems 318

Chapter 17 *Managing Security* ***321***
About the Security for the Management Server 322
About Roles *322*
About Organizations *325*
Planning Your Hierarchy *328*
Naming Organizations *329*
Managing User Accounts 329

Adding Users *330*
Editing a User Account *331*
Changing the Password for a User Account *332*
Changing Your Password *333*
Deleting Users *333*
Modifying Your User Profile *334*
Modifying Your User Preferences *335*
System Explorer and Element Topology Preferences 335
Event Manager Preferences 335
Warnings for Slow Systems Operations 336
Viewing the Properties of a Role *337*
Viewing the Properties of an Organization *337*
Managing Roles 338
Adding Roles *338*
Editing Roles *339*
Deleting Roles *340*
Managing Organizations 341
Adding an Organization *341*
Adding Storage Volumes to an Organization 342
Viewing Organizations *343*
Editing Organizations *343*
Deleting an Organization *345*
Removing Members from an Organization *345*
Filtering Organizations *346*
Changing the Password of System Accounts 349
Using Active Directory/LDAP for Authentication 350

Step 1 - Configure the Management Server to Use Active Directory or LDAP351

Active Directory 352

LDAP 356

Step 2 - Restart the AppStorManager Service and Login as the Designated Admin Account 360

Step 3 - Add Users to the Management Server 361

Step 4 - Provide Login Information to Your Users 361

Chapter 18 *Troubleshooting* **. 363**

"Data is late or an error occurred" Message 364

appiq.log Filled with Connection Exceptions 364

Receiving "HTTP ERROR: 503" When Accessing the Management Server 365

Errors in the Logs 366

Permanently Changing the Port a CIM Extension Uses (UNIX Only) 367

Configuring UNIX CIM Extensions to Run Behind Firewalls 369

Volume Names from Ambiguous Automounts Are Not Displayed 376

Solaris Management Server Suddenly Restarts 376

Installing the Software Security Certificate 377

Installing the Certificate by Using Microsoft Explorer 6.0 377

Installing the Certificate by Using Netscape Navigator 7 378

Changing the Security Certificate to Match the Name of the Server. 378

Troubleshooting After Upgrading 379

SMI-S Switches Must Be Removed and Rediscovered After Upgrading 380

Troubleshooting Discovery and Get Details 380

Names are Changed After Running Get Details for Cisco SMI-S Switches 381

Configuring E-mail Notification for Get Details 382

Increasing the Time-out Period and Number of Retries for Switches in Progress 383

"Connection to the Database Server Failed" Error 385

Using the Test Button to Troubleshoot Discovery 385

DCOM Unable to Communicate with Computer 387

Duplicate Listings for Brocade Switches in Same Fabric 388

Element Logs Authentication Errors During Discovery 388

EMC Device Masking Database Does Not Appear in Topology (AIX Only) 388

Management Server Does Not Discover Another Management Server's Database 389

Microsoft Exchange Drive Shown as a Local Drive 389

Unable to Discover Microsoft Exchange Servers 389

Nonexistent Oracle Instance Is Displayed 389

Requirements for Discovering Oracle 389

Do Not Run Overlapping Discovery Schedules 390

"This storage system uses unsupported firmware. ManagementClassName: ???" Message 390

Troubleshooting Topology Issues 391

About the Topology 391

Undiscovered Hosts Display as Storage Systems 395
Solaris Machines Appear to Have Extra QLogic HBAs 396
No Stitching for Brocade Switches with Firmware 3.2.0. 396
Link Between a Brocade Switch and a Host Disappears from the Topology. 396
Incorrect Topology Sometimes Displayed for CNT Switches 397
Unable to Find Elements on the Network 397
Device Locking Mechanism for Brocade Element Manager Query/Reconfiguration. 397
A Discovered Sun StorEdge A5000 JBOD Does Not Display Its WWN Properly 398
Unable to Monitor McDATA Switches. 398
Unable to Detect a Host Bus Adapter 398
Navigation Tab Displays Removed Drives as Disk Drives 399
Unable to Obtain Information from a CLARiiON Storage System 399
Discovery Fails Too Slowly for a Nonexistent IP Address 399
"CIM_ERR_FAILED" Message 401
Re-establishing Communication with EFCM. 402
Communicating with HiCommand Device Manager Over SSL. 403
Unable to Discover a UNIX Host Because of DNS or Routing Issues 404
Unable to View System Explorer After Upgrade 406
Troubleshooting Provisioning 406
Cannot Access a Resource Owned by Another Controller 406
Error -56 407
"Can't delete this zone" Message 407
Changes in EFC Manager Requiring Get Details. 407
Troubleshooting Hardware 407

About Swapping Host Bus Adapters *408*
"Fork Function Failed" Message on AIX Hosts *408*
Known Driver Issues *408*
Known Device Issues *408*
"mailbox command 17 failure status FFF7" Message *412*
"Process Has an Exclusive Lock" Message *413*

List of Figures

Figure 2-1: */tmp/orainstRoot.sh Script with X Forwarding* ***15***

Figure 2-2: *Do not Create a New Database with X Forwarding* ***16***

Figure 2-3: *Setup Privileges with X Forwarding* ***17***

Figure 2-4: */tmp/orainstRoot.sh Script* ***20***

Figure 2-5: *Do not Create a New Database* ***21***

Figure 2-6: *Setup Privileges* ***22***

Figure 2-7: *Oracle Processes Error Message* ***24***

Figure 4-1: *Setting Default User Names and Passwords* ***71***

Figure 4-2: *Adding an IP Range for Scanning* ***73***

Figure 4-3: *Deleting Elements from the Management Server* ***137***

Figure 17-1: *Parent-Child Hierarchy for Organizations* ***326***

Figure 17-2: *Children in Multiple Organizations* ***327***

Figure 17-3: *Changing Your User Profile* ***334***

Figure 17-4: *Accessing the User Preferences Tab* ***335***

Figure 17-5: *Clicking the Organization Link*. ***347***

Figure 17-6: *Filtering Organizations* ***348***

Figure 17-7: *Active Organization* ***349***

List of Tables

Table 1: *Additional Documentation* . . . . . ***xxx***

Table 1-1: *Roadmap for Installation and Initial Configurations* ***2***

Table 4-1: *Discovery Steps for Switches, NAS Devices, and Storage Systems* ***68***

Table 4-2: *Discovery Requirements for Switches* ***79***

Table 4-3: *Brocade Discovery Methods* ***81***

Table 4-4: *Required Switch Models and InVsn Versions for Discovery* ***86***

Table 4-5: *Discovery Settings for McDATA and Connectrix Switches* ***92***

Table 4-6: *Task Status Descriptions* ***105***

Table 4-7: *Discovery Requirements for Storage Systems, Tape Libraries & NAS Devices* ***107***

Table 5-1: *Status Icons* ***159***

Table 6-1: *Parameters for CIM Extensions* ***171***

Table 7-1: *Parameters for CIM Extensions* ***184***

Table 8-1: *Parameters for CIM Extensions* ***197***

Table 9-1: *Parameters for CIM Extensions* ***208***

Table 10-1: *Parameters for CIM Extensions*. ***221***

Table 11-1: *Parameters for CIM Extensions*. ***235***

Table 12-1: *Parameters for CIM Extensions*. ***248***

Table 13-1: *Parameters for CIM Extensions*. ***263***

Table 14-1: *Parameters for CIM Extensions*. ***275***

Table 16-1: *Making the Management Server Aware of Hosts*. ***287***

Table 17-1: *Default Role Privileges* ***323***

Table 17-2: *Default Role Privileges with Elements*. ***324***

Table 17-3: *Changing User Preferences for Event Manager* ***336***

Table 18-1: *Troubleshooting Firewalls*. ***370***

Table 18-2: *Time-out Properties* ***384***

Table 18-3: *Retry Properties* ***384***

Table 18-4: *Troubleshooting Discovery and Get Details* ***392***

Table 18-5: *Known Device Issues* ***409***

PREFACE

About This Guide

This preface describes the following:

- Intended Audience on page xxix
- Where to Find Additional Information on page xxx

Intended Audience

This document assumes you have a basic understanding of the following:

- Networking
- Storage Area Networks (SANs)
- The Common Information Model (CIM)

To learn out more about:

- **AppIQ** - See www.appiq.com.
- **CIM** - See www.snia.org and www.dmtf.org.

Where to Find Additional Information

The management server ships with the additional documentation:

Table 1: Additional Documentation

Document	Description
Release Notes	Provides late-breaking issues that might impact the usage of the product.
User Guide	Describes how to use the management server. The information in this guide is also accessible from the online help.
Online help	An online help system containing information from the PDFs in HTML format.
File Servers Guide	Describes how to use the file server storage resource management (SRM) functionality in the product.
CLI Guide	Provides information about the CLI commands.
Guide for monitoring applications	Describes how to use the management server to monitor applications.

The documentation listed above, except for the help system, can be found in two locations:

- On the CD-ROM used to install the CIM Extensions.The help system is not accessible from the CD-ROM.
- From the online help system, which is accessible by clicking the **Help** menu in the upper-right corner.

CHAPTER 1

Overview

This chapter describes the following:

- “About this Product” on page 4
- “Software Requirements” on page 6
- “Web Browser Configuration Requirements” on page 6

Table 1-1: Roadmap for Installation and Initial Configurations

Step	Description	Where to Find
1	Install the management server. This step requires you to install third-party software.	■ **Sun Solaris** - See Chapter 2, “Installing the Management Server on Sun Solaris” on page 9. ■ **Microsoft Windows** - See Chapter 3, “Installing the Management Server on Microsoft Windows” on page 45.
2	Perform discovery for switches, filers, and storage systems. This step requires the management server to be connected to the network containing the switches, filers, and storage systems you want to manage.	See Chapter 4, “Discovering NAS Devices, Tape Libraries, Switches and Storage Systems” on page 65.

Table 1-1: Roadmap for Installation and Initial Configurations (Continued)

Step	Description	Where to Find
3	Install a CIM Extension on each host (other than the management server) from which you want the management server to be able to obtain information. The CIM Extension gathers information from the operating system and host bus adapters on the host. It then makes the information available to the management server. **Important**: CIM Extensions are required on UNIX hosts. If you do not install a CIM Extension on a UNIX host, the management server cannot obtain information from the host. On a Microsoft Windows host without a CIM Extension, the management server can only find information that is gathered from Windows Management Instrumentation. The CIM Extension is required to obtain information from the host bus adapter and manage applications on the Microsoft Windows host. Without the CIM Extension, the management server can determine if Oracle and Microsoft Exchange are on the host, but it cannot obtain further information about the applications.	■ **IBM AIX** - See Chapter 6, “Installing the CIM Extension for IBM AIX” on page 161. ■ **SGI ProPack for Linux** - See Chapter 7, “Installing the CIM Extension for SGI ProPack for Linux” on page 175. ■ **HP-UX** - See Chapter 8, “Installing the CIM Extension for HP-UX” on page 187. ■ **SGI IRIX** - See Chapter 9, “Installing the CIM Extension for SGI IRIX” on page 201. ■ **SUSE and Red Hat Linux** - See Chapter 10, “Installing the CIM Extension for SUSE and Red Hat Linux” on page 213. ■ **HP OpenVMS (Alpha)** - See Chapter 12, “Installing the CIM Extension for OpenVMS” on page 239. ■ **HP Tru64 UNIX** - See Chapter 13, “Installing the CIM Extension for HP Tru64 UNIX” on page 253. ■ **Sun Solaris** - See Chapter 11, “Installing the CIM Extension for Sun Solaris” on page 225. ■ **Microsoft Windows** - See Chapter 14, “Installing the CIM Extension for Microsoft Windows” on page 267.

Table 1-1: Roadmap for Installation and Initial Configurations (Continued)

Step	Description	Where to Find
4	If you installed the management server on Solaris, install and configure the Windows Proxy. Windows Proxy lets the management server on Solaris discover Windows hosts.	See Chapter 15, “Installing and Discovering the Windows Proxy” on page 279.
5	Configure the applications and hosts for monitoring. This step includes discovering applications and hosts.	See Chapter 16, “Discovering Applications and Hosts” on page 285.
6	If your license lets you collect disk drive statistics from Engenio storage systems, set up the management server to collect those statistics. You can determine if you license lets you collect this data, by accessing the feature list, which is accessible from the Documentation Center (**Help** > **Documentation Center**).	See “Obtaining Disk Drive Statistics from Engenio Storage Systems” on page 318.
7	Change the password of the admin account for the management server and system accounts.	See “Changing Your Password” on page 333 and “Changing the Password of System Accounts” on page 349.
8	Add users.	See “Adding Users” on page 330.

About this Product

This product can simplify your complex environment and lower your cost of management with CIM-based integrated storage management. The management software integrates the management of applications, servers, storage networks and storage subsystems in a single, easy to implement and intuitive solution.

The management software integrates the various components in the storage infrastructure into a CIM/WBEM/SMI-S standards based database so you can eliminate any vendor dependencies and view and manage your infrastructure as a whole.

By giving your administrators a single, integrated console to manage tactical activities such as provisioning storage, managing real time events, installing new applications, and migrating servers and storage, as well as strategic activities such as forecasting, planning and cost analysis, the management software's integrated storage management lowers your cost of acquiring and managing a heterogeneous storage environment.

Storage Management Terms

- **CIM** - A common data model of an implementation-neutral schema for describing overall management information in a network/enterprise environment.
- **Web-Based Enterprise Management (WBEM)** - An initiative based on a set of management and Internet standard technologies developed to unify the management of enterprise computing environments.

See the glossary in the management server User Guide or in the management server help system for additional definitions.

Key Benefits

- More efficient use of existing assets
- Increased application availability and performance
- Quicker deployment of storage infrastructure and business applications
- Protection of customer flexibility and investments with a standards-based interface

Key Features

- **End-to-end visibility of business applications** - Provides an interface for you to monitor your business applications, including their associated infrastructure and interdependencies.
- **Integrated storage management** - Lowers cost of acquiring and managing a heterogeneous storage environment using multiple disparate, point solutions.

- **Standards-based architecture** - Protects customer flexibility and investments with a standards-based interface for managing heterogeneous storage environments.
- **Storage server, network and subsystem provisioning** - Reduces manual processes and risk of downtime due to free-space outages with multi-level storage provisioning.
- **Reporting** - Offers flexible, in-depth report generation in both predefined and user defined formats, or export data to other management applications.
- **Integrated asset management and chargeback** - Centralizes all aspects of storage inventory for maximum asset utilization. Improves accountability and budgeting with cost accounting based chargeback on user defined utilization characteristics.
- **Web-based global management console** - Provides management of heterogeneous storage environments through a web-based user interface.

Software Requirements

To find the software requirements for the management server and for the elements you plan to discover, refer to the support matrix (`SupportMatrix.html`), which can be found on the top-level of the management server CD-ROM.

Web Browser Configuration Requirements

Before you can use the management server, verify the following are enabled on your Web browser:

- cookies
- JavaScript
- Java

You can verify these settings by doing the following:

- **Microsoft Internet Explorer** - Go to the Internet Options window by selecting **Tools** > **Internet Options**.
  - **To verify if cookies are enabled** - Click the **Privacy** tab. This setting requires a medium or lower security setting.
  - **To verify if Java is enabled** - Click the **Advanced** tab. Under the Sun setting, verify that the option, **Use JRE <version number>** is selected.
- **Netscape** - Go to the Preferences window by selecting **Edit** > **Preferences** in Netscape.

- **To verify if cookies are enabled** - Expand the **Privacy & Security** category, and then click **Cookies**.
- **To verify if Java is enabled** - Click **Advanced**.
- **To verify if JavaScript is enabled** - Expand the **Advanced** category, and then click **Scripts & Plug-ins**.

For more information about enabling the items listed above, refer to the online help for your Web browser.

CHAPTER 2

Installing the Management Server on Sun Solaris

If you did not receive a computer with the management server installed on it, first complete the steps in this section.

Note: These steps are for installing the management server on Sun Solaris. See “Upgrading the Management Server” on page 36 for information about how to upgrade the management server.

Keep in mind the following:

- **All steps must be completed for the management server to work properly.**
- For optimal performance, install the management server on a dedicated computer. See the Support Matrix for hardware requirements.
- Installation through a terminal server or using Virtual Network Computing (VNC) software is not supported.

This chapter describes the following:

- Step 1 - Install the Oracle Database (Solaris) on page 10
- Step 2 - Install the Management Server on page 26
- Step 3 - Verify that Processes Can Start on page 28

- Step 4 - Verify You Can Connect to the Management Server on page 29
- Configurations Required for Discovering EMC CLARiiON Storage Systems on page 32
- Installing the Java Plug-in on Sun Solaris on page 31
- Removing the Management Server on page 33
- Porting the Management Server Across Operating Systems on page 35
- Upgrading the Management Server on page 36

Step 1 - Install the Oracle Database (Solaris)

The management server uses a database to store the data it collects from the hardware it monitors. The management server ships with a three-CD set for the management server database and an additional CD-ROM for Database Server Patch 9.2.0.6.0. During the installation of the database, you are prompted to change CD-ROMs. After the installation, you must install the database patch from the Database Patch CD-ROM.

There are two sets of instructions for installing the database. Follow the instructions for your configuration after first reading through “Before Installing the Oracle Database” on page 10 and “Prerequisites” on page 11:

- **Secure Shell (SSH) Server with X Forwarding** - See “Installing the Database on a Secure Shell (SSH) Server with X Forwarding” on page 12
- **Other Configurations, including SSH Server without X Forwarding** - See “Installing the Database for Configurations Other Than SSH with X Forwarding” on page 17

Important: Install the database for the management server on a computer that does not already have Oracle installed. In later steps, you will install the management server on the same machine that you installed Oracle.

Before Installing the Oracle Database

Keep in mind the following:

- Refer to the Support Matrix on the management server CD-ROM for system requirements.
- Once you start the installation, do not exit. The Oracle installer creates the orauser file within the first few minutes of the installation. This file remains on the system if the installation is stopped before completion. Future installations of the management server database look for the orauser file to verify that the database is installed. If you exit the Oracle installation before the installation is finished, the Oracle database is not installed and the management server cannot run correctly without a successful database installation.
- Install the database on the computer on which you plan to install the management server.
- Before you can install Oracle on Sun Solaris, the Solaris server must have X Window System installed.
- Install the database on Solaris, then install the Oracle patch. If you are upgrading the management server, see “Upgrading the Management Server” on page 36 for more information.
- When you install the database on Solaris, files with group writeable permissions are installed in the `/opt/oracle` directory.
- For double-byte languages, the Oracle installation provides an extra dialog screen, which is for the Oracle Net Configuration Assistant. This screen requires the user to select the check box and click **Next**. Once you click **Next**, a command window appears. The command window closes itself once the operation running inside the command window completes.

Prerequisites

Before you install the database on a Sun Solaris server, do the following:

- Verify that the server is running Solaris 9 or 10.
- Verify that the server is running sh, ksh or bash shell. C shell is not supported.
- Verify the following directories have write permissions:

  ```
  /
  /tmp/
  /opt/
  /opt/oracle/
  /var/opt/
  ```

- If you have **Sun Solaris 9** installed, add the following lines to the `/etc/system` file and reboot the server if they do not exist in the file already. Use the following as an example of how to set up `/etc/system` to have the kernel tunables set properly for Oracle. See the next bullet if you have Solaris 10.

```
forceload: sys/semsys
forceload: sys/shmsys
set shmsys:shminfo_shmmax = 4294967295
set shmsys:shminfo_shmmin = 1
set shmsys:shminfo_shmmni = 100
set shmsys:shminfo_shmseg = 10
set semsys:seminfo_semmni = 100
set semsys:seminfo_semmsl = 500
set semsys:seminfo_semmns = 5000
set semsys:seminfo_semopm = 100
set semsys:seminfo_semvmx = 32767
```

- If the management server is being installed on Sun Solaris 10, ensure that the following attributes in the user.root project are set to a minimum value of 100:

```
project.max-shm-ids
project.max-sem-ids
```

  For more information on how to set project attributes, see the man pages for project(4) and resource_controls(5).

  To verify the root user project id, enter the following at the command prompt:

```
id -p root

uid=0(root) gid=0(root) projid=1 (user.root)
```

Installing the Database on a Secure Shell (SSH) Server with X Forwarding

Important: Follow the steps in this section carefully, especially if you are installing the database on an SSH server with X Forwarding. If you are installing the database on an SSH server with X Forwarding, you must run the following scripts at the designated time as described in this section:

```
install_as_user_root

install_as_user_oracle
```

To install the database:

1. Make sure there are no existing Oracle user accounts on the computer.
2. Access the Solaris host by doing one of the following:
   - **Windows client/X Term program** - Start up a local X server, connect through xterm to the remote system and set your DISPLAY environment variable appropriately.
   - **Solaris** - Run the following command at the command prompt on the host:
     `# /usr/openwin/bin/xhost +`
     Then, set the display to your client. Refer to the documentation for your shell for more information.
3. Insert the first Oracle Database CD-ROM.
4. Start the installation of the database by entering the following:
   `# /cdrom0/appdb51_disk1/install_as_user_root`

   Note: All commands and files are case-sensitive on Sun Solaris.

5. Open a second terminal window. You will need the second window in a moment. Return to the first terminal window.
6. If you are asked for a location for the Oracle user home directory, select `/export/home/oracle`.

If you are asked where you want to install Oracle, you can select the default, which is `/opt/oracle`

If the installation detects Oracle already on the server, it selects the installation directory of the current program.

```
Checking for required PACKAGES
INFO: Creating dba group
INFO: Creating oracle user
Operating Environment: Solaris 9 9/04
System architecture: Ultra-Enterprise, sparc, sun4u
Installed on: Wed Sept 29 18:33:47 EDT 2004
```

7. Before entering the following command, log in as Oracle and set the display.
   `# /cdrom/appdb51_disk1/install_as_user_oracle`
   where `/cdrom` is the name of the CD-ROM drive and `/appdb51_disk1` is the name of the CD-ROM.
8. When asked for the base directory, click **OK** for the default location:
   `/export/home/oracle/oraInventory`
9. If you are shown the following window, go to the second terminal window and run the following command at the command prompt:
   `# /tmp/orainstRoot.sh`

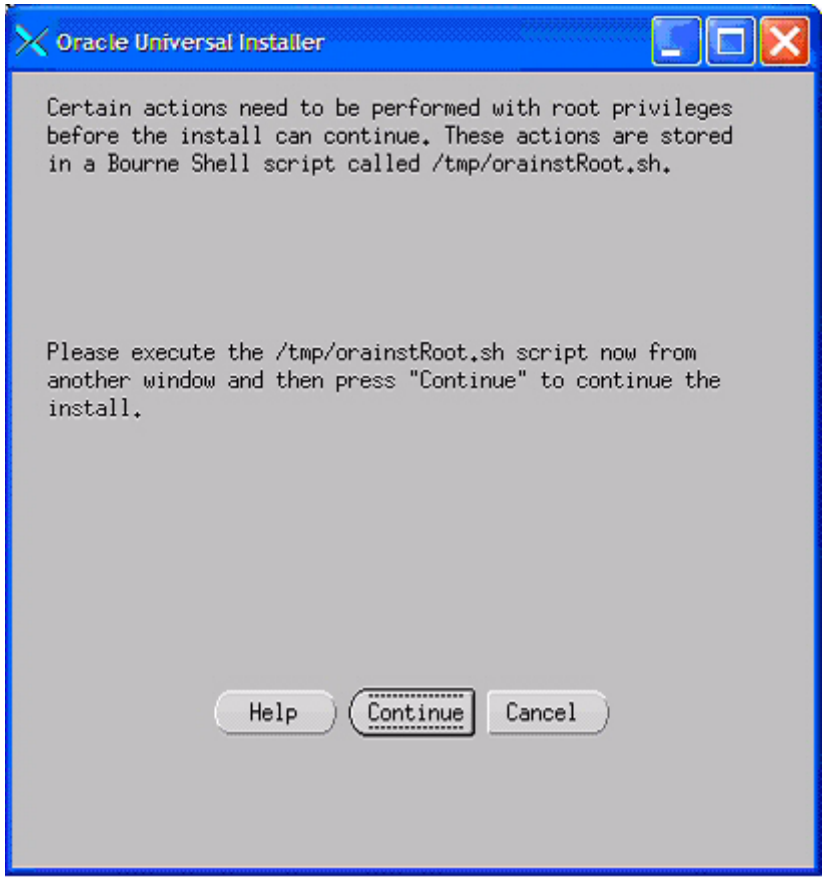


Figure 2-1: /tmp/orainstRoot.sh Script with X Forwarding

10. Once the command you entered has completed and returned you to system prompt, go back to the installer in the first terminal window and click **Continue**.
11. Verify the file locations and click **Next**.
12. Select the **NO** radio button on the **Oracle Universal Installer: Create Database** window and click **Next**. Selecting **No** installs the Oracle database files and not the instance which is created by the management server when you install the management server software.

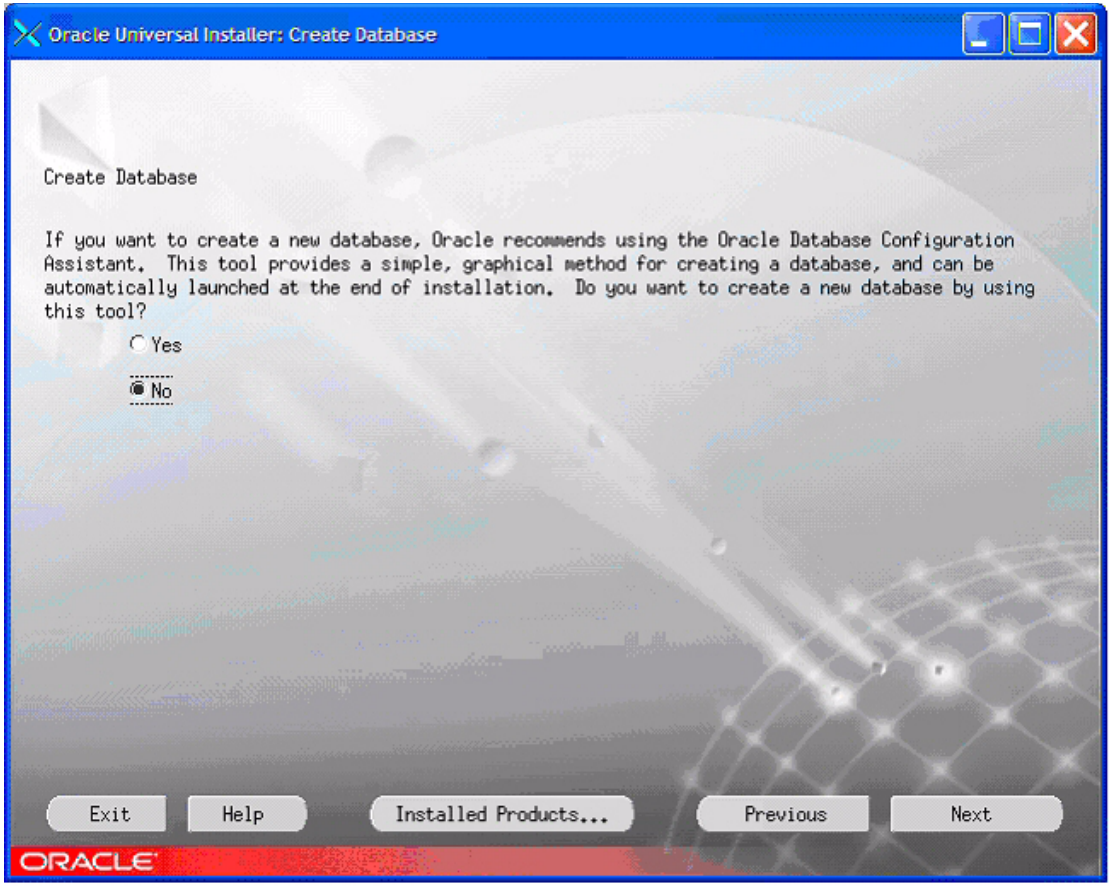


Figure 2-2: Do not Create a New Database with X Forwarding

The Oracle Universal Installer installs the contents of all three CDs. When all of the files on the first CD (Disk 1) are installed, the Oracle Universal Installer prompts you for the second CD (Disk 2).

13. Replace Disk 1 with Disk 2 in the disk drive, change the 1 to 2 so the path is correct in the Disk Location dialog box, and click **OK**.

14. When the Setup Privileges dialog box is displayed, go to the second terminal window and run the `root.sh` script described in the Setup Privileges window:
    `# /opt/oracle/product/9.2.0.1.0/root.sh`
    where `/opt/oracle/product/9.2.0.1.0` is the Oracle home path.

Important: The path displayed in the command and in the Setup Privileges dialog box may be different depending on your Oracle home path.

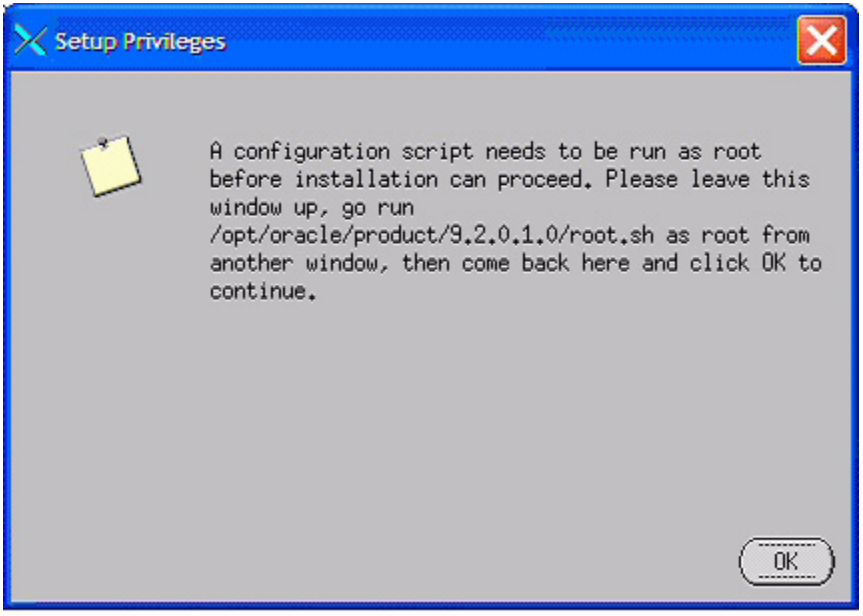


Figure 2-3: Setup Privileges with X Forwarding

The following is the output of the script. Your output may differ slightly based on the file paths you entered.

```
Running Oracle9 root.sh script...
The following environment variables are set as:
    ORACLE_OWNER= oracle
    ORACLE_HOME=  /opt/oracle/product/9.2.0.1.0
Enter the full pathname of the local bin directory: [/usr/local/bin]:
```

```
Creating /usr/local/bin directory...
   Copying dbhome to /usr/local/bin ...
   Copying oraenv to /usr/local/bin ...
   Copying coraenv to /usr/local/bin ...
Creating /var/opt/oracle/oratab file...
Adding entry to /var/opt/oracle/oratab file...
Entries will be added to the /var/opt/oracle/oratab file as needed by
Database Configuration Assistant when a database is created
Finished running generic part of root.sh script.
Now product-specific root actions will be performed.
#
```

15. When the script is done running, click **OK** in the first terminal window and eject the Oracle Database disk 3. The installation is done when you see the script `S98dbora` in the `/etc/rc3.d` directory.

Important: You do not need to reboot at this time.

16. Install the Oracle patch as described in “Installing the Oracle Patch” on page 22.

Installing the Database for Configurations Other Than SSH with X Forwarding

Important: This section is for configurations other than those with SSH with X forwarding. If you are installing the database on an SSH server with X forwarding, follow the steps in “Installing the Database on a Secure Shell (SSH) Server with X Forwarding” on page 12.

To install the database:

1. Make sure there are no existing Oracle user accounts on the computer.
2. Access the Solaris host by doing one of the following:
   - **Windows client/X Term program** - Start up a local X server, connect through xterm to the remote system and set your DISPLAY environment variable appropriately.
   - **Solaris** - Run the following command at the command prompt on the host:

```
# /usr/openwin/bin/xhost +
```

Then, set the display to your client. Refer to the documentation for your shell for more information.

3. Put the first Oracle Database CD-ROM (Disk 1) in the CD-ROM drive.
4. Start the installation of the database by entering the following at the command prompt:
   ```
   # /cdrom/appdb51_disk1/InstallDatabase
   ```
   where `/cdrom` is the name of the CD-ROM drive and `/appdb51_disk1` is the name of the CD-ROM.
5. If you are asked for a location for the Oracle user home directory, select `/export/home/oracle`.
6. If you are asked where you want to install Oracle, you can select the default, which is `/opt/oracle`. If the installation detects Oracle already on the server, it selects the installation directory of the current program.
   ```
   Checking for required PACKAGES
   INFO: Creating dba group
   INFO: Creating oracle user
   Operating Environment: Solaris 9 9/04
   System architecture: Ultra-Enterprise, sparc, sun4u
   Installed on: Wed Sept 29 18:33:47 EDT 2004
   ```
7. When asked for the base directory, click **OK** for the default location, which is `/export/home/oracle/oraInventory`
8. If you are shown the following window, run the following command at the command prompt. You do not have to run the following command in a second terminal window.
   ```
   # /tmp/orainstRoot.sh
   ```

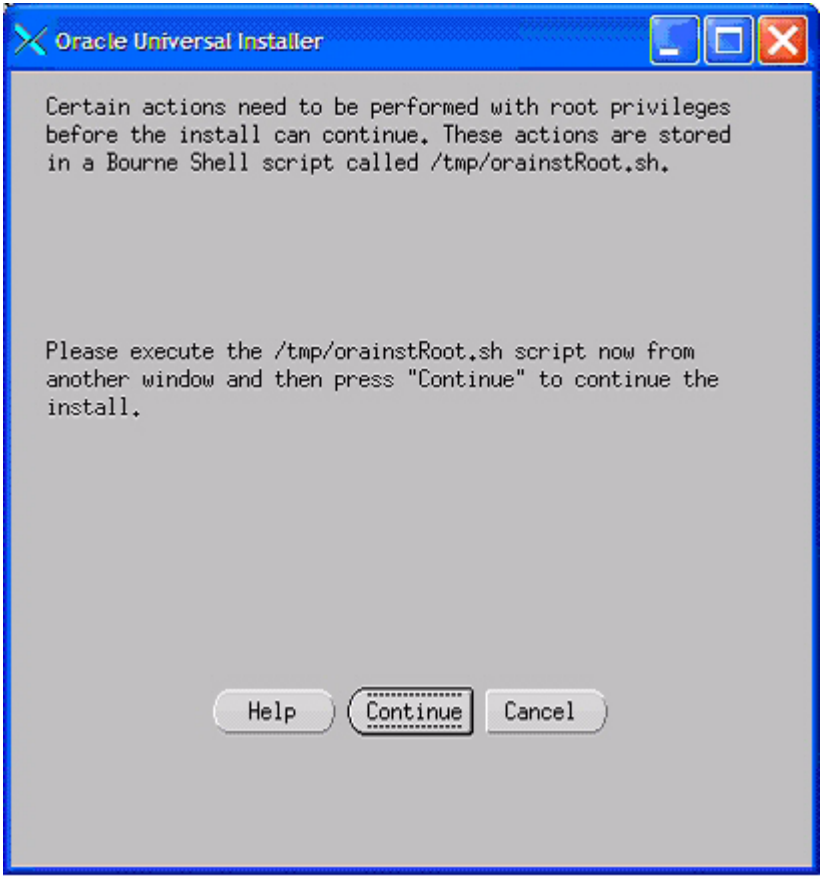


Figure 2-4: /tmp/orainstRoot.sh Script

9. Once the command you entered has completed and returned you to system prompt, go back to the installer in the first terminal window and click **Continue**.
10. Verify the file locations and click **Next**.
11. Select the **NO** radio button on the **Oracle Universal Installer: Create Database** window and click **Next**. Selecting **No** installs the Oracle database files and not the instance which is created by the management server when you install the management server software.

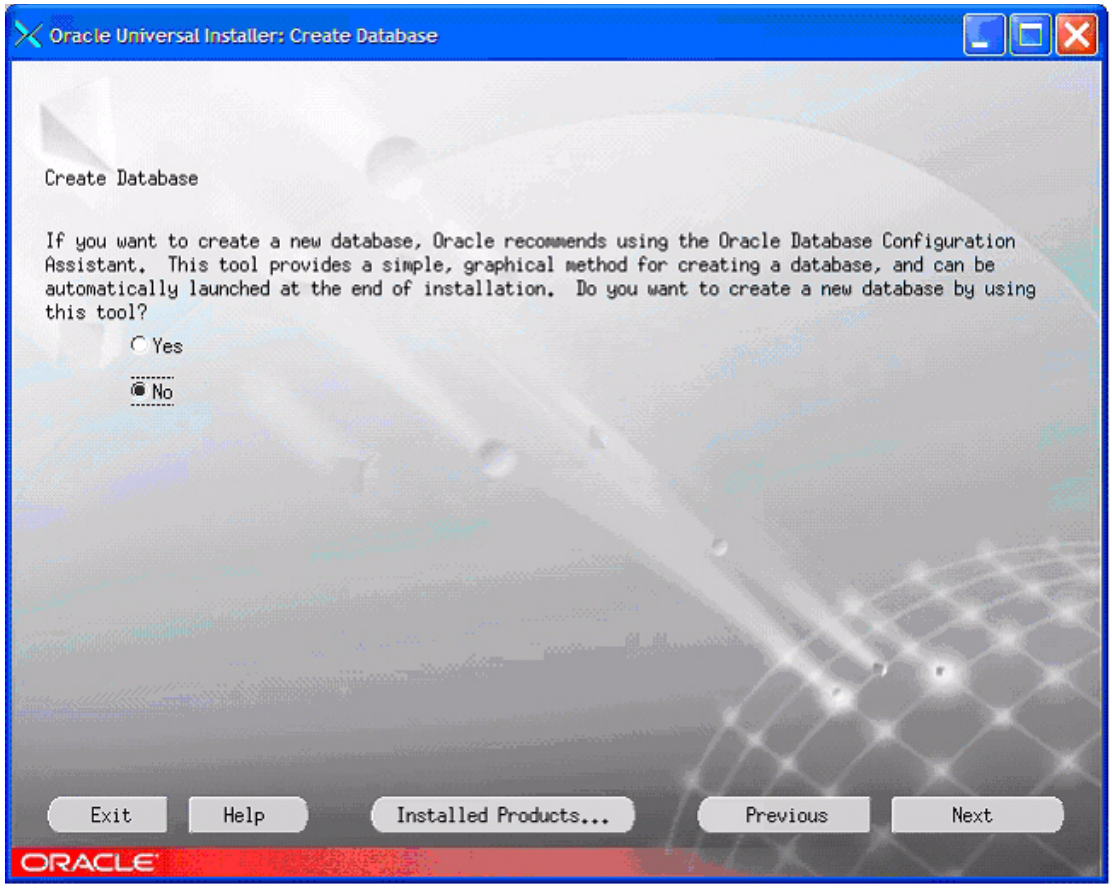


Figure 2-5: Do not Create a New Database

The Oracle Universal Installer installs the contents of all three CDs. When all of the files on the first CD (Disk 1) are installed, the Oracle Universal Installer prompts you for the second CD (Disk 2).

12. Replace Disk 1 with Disk 2 in the CD-ROM drive, change the 1 to 2 so the path is correct in the Disk Location dialog box, and click **OK**.
13. Replace the Oracle Database Disk 2 with Disk 3 when prompted, change the 2 to 3 in the path, and click **OK**.

14. When the Setup Privileges dialog box is displayed, go to the second terminal window and run the `root.sh` script described in the Setup Privileges window:
    `# /opt/oracle/product/9.2.0.1.0/root.sh`
    where `/opt/oracle/product/9.2.0.1.0` is the Oracle home path.

Important: The path displayed in the command and in the following figure may be different depending on your Oracle home path.

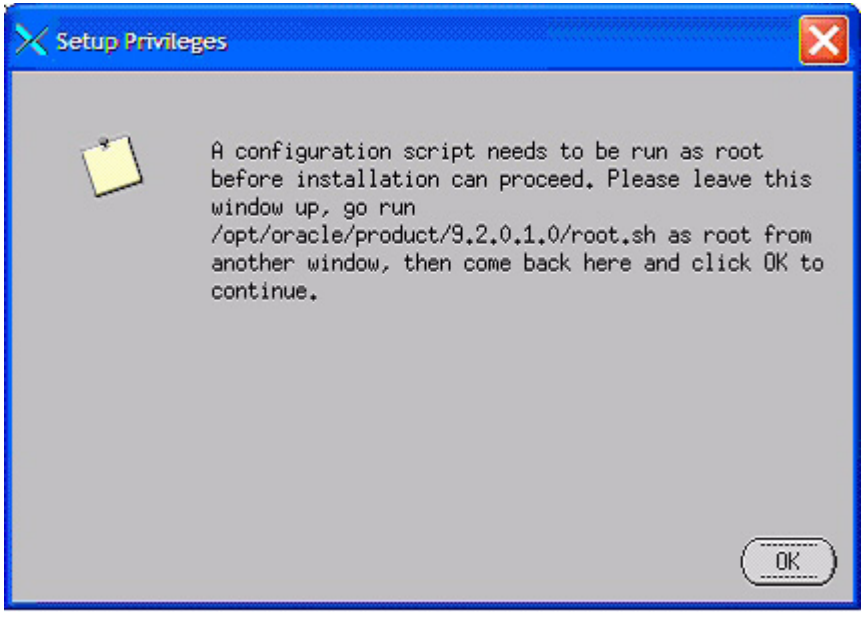


Figure 2-6: Setup Privileges

The following is the output of the script. Your output may differ slightly based on the file paths you entered.

```
Running Oracle9 root.sh script...
The following environment variables are set as:
    ORACLE_OWNER= oracle
    ORACLE_HOME=  /opt/oracle/product/9.2.0.1.0
Enter the full pathname of the local bin directory: [/usr/local/bin]:
```

```
Creating /usr/local/bin directory...
   Copying dbhome to /usr/local/bin ...
   Copying oraenv to /usr/local/bin ...
   Copying coraenv to /usr/local/bin ...
Creating /var/opt/oracle/oratab file...
Adding entry to /var/opt/oracle/oratab file...
Entries will be added to the /var/opt/oracle/oratab file as needed by
Database Configuration Assistant when a database is created
Finished running generic part of root.sh script.
Now product-specific root actions will be performed.
#
```

15. When the script is done running, click **OK** in the first terminal window. The installation is done when you see the script `S98dbora` in the `/etc/rc3.d` directory.

Important: You do not need to reboot at this time.

16. Eject the Oracle Database Disk 3 from the disk drive and install the Oracle patch as described in “Installing the Oracle Patch” on page 22.

Installing the Oracle Patch

To install the Oracle patch on Solaris:

1. Log in as root and then enter the following at the command prompt to change to user oracle:
   ```
   # su - oracle
   ```
2. Verify whether or not you need to install the Oracle patch by entering the following at the command prompt and noting the reported release version. If you are running Oracle version 9.2.0.6.0 or later, you do not need to install the patch.
   ```
   # sqlplus /nolog
   ```
   You are shown the reported release version.
   a. Exit the SQL prompt if you are running Oracle version 9.2.0.6.0 or later by entering the following at the command prompt:
      ```
      SQL> exit
      ```
   b. Return to user root if you need to install the Oracle patch by entering the following at the command prompt:
      ```
      # exit
      ```

3. Stop the appstormanager process and all Oracle processes if they are running.
   a. As user root (the required user level from step 2), enter the following to determine if the appstormanager and the Oracle processes are running:
      ```
      # ps -ef | grep appstorm
      # ps -ef | grep ora
      # ps -ef | grep dbsnmp
      ```
      Additionally, if the Oracle processes are running, the Oracle Universal Installer displays a similar error message, as shown in the following figure.

Figure 2-7: Oracle Processes Error Message

   b. Continue to step 4 if the processes are not running. Or complete the following sub-steps to stop the processes before proceeding.
   c. Stop the appstormanager process if the process is running by entering the following at the command prompt:
      ```
      # /etc/init.d/appstormanager stop
      ```
      The appstormanager process is stopped.
   d. Stop the Oracle processes if any are running by changing to user oracle.
      ```
      # su - oracle
      ```
      Then, enter the following commands at the command prompt:

      ```
      # sqlplus /nolog
      SQL> connect sys/<sys password>@appiq as sysdba
      SQL> shutdown immediate
      SQL> exit
      ```

```
# lsnrctl stop
# exit
```

e. Verify that appstormanager is not running by entering the following at the command prompt:

```
# ps –ef | grep appstorm
```

f. Verify that Oracle processes are not running by entering the following at the command prompt:

```
# ps –ef | grep ora

# ps -ef | grep dbsnmp
```

If the dbsnmp processes are running, kill them by entering the following:

```
# kill -9 <process Ids>
```

g. Verify that tnslsnr is not running by entering the following at the command prompt:

```
# ps –ef | grep tns
```

4. Put the Database Patch CD in the disk drive.
5. Access the Solaris host by doing one of the following:
   - **Windows client/X Term program** - Start up a local X server, connect through xterm to the remote system and set your DISPLAY environment variable appropriately.
   - **Solaris** - Run the following command at the command prompt:
     ```
     # /usr/openwin/bin/xhost +
     ```

   Then, set the display to your client. Refer to the documentation for your shell for more information.
6. As user oracle (`su - oracle`), execute the following command:
   `/mnt/cdrom/runOraInstallPatch.sh`
   where /mnt/cdrom is your CD-ROM disk drive.

   The Oracle Installer launches.

   Note: Text similar to the following may be displayed on some Solaris systems and can safely be disregarded:

```
Checking operating system patches: 108652-66,108921-16,108940-53,108773-
18,111310-01,109147-24,111308-03,111111-03,112396-02,110386-03,111023-
02,108987-13,108528-23,108989-02,108993-18    Failed <<<<
Checking for patch 108652-66; found 108652-79
Checking for patch 108921-16; found 108921-13    Failed <<<<
Checking for patch 108940-53; found 108940-37    Failed <<<<
```

```
Checking for patch 108773-18; found 108773-12    Failed <<<<
Checking for patch 111310-01; found 111310-01
Checking for patch 109147-24; found 109147-28
Checking for patch 111308-03; found 111308-01    Failed <<<<
>>> Ignoring optional pre-requisite failures. Continuing...
```

7. To begin the installation of the patch, click **Next**.
   The installer dismisses itself when done.
8. If you have patched an existing management server database, the processes that were stopped at Step 3 need to be restarted. You must also run the `migrateDB.sh` script, as described in the following steps.

Important: You must perform the following steps as user oracle. You should already be user ‘oracle’ if you have been following the steps in this section.

---

   a. Start the Oracle listener by entering the following at the command prompt:
      `# lsnrctl start`
   b. Start the database for the management server by entering the following commands at the command prompt:
      ```
      # sqlplus /nolog
      SQL> connect sys/<sys password>@appiq as sysdba
      SQL> startup
      SQL> exit
      ```
   c. Run migrateDB.sh and enter the sys password when prompted:
      `./migrateDB.sh`

Note: The migrateDB.sh script may take an excess of 15 minutes to run. When it completes, a message similar to the following is displayed:

```
Disconnected from Oracle9i Enterprise Edition Release 9.2.0.6.0
- 64bit Production
With the OLAP option
JServer Release 9.2.0.6.0 - Production
```

   d. As user root, start appstormanager by entering the following at the command prompt:
      `/etc/init.d/appstormanager start`
9. Go to the root directory before you attempt to eject the CD-ROM from the CD-ROM drive.
10. If this is a new installation, see “Step 2 - Install the Management Server” on page 26.

11. If you plan to upgrade the management server, see “Upgrading the Management Server” on page 36.

Step 2 - Install the Management Server

Install the management server on the same computer you installed Oracle as described in “Step 1 - Install the Oracle Database (Solaris)” on page 10.

Keep in mind the following:

- Refer to the release notes for late breaking information.
- Make sure no other programs are running when you install the management server.
- When you install the management server on Sun Solaris, you must install the software using a POSIX (Portable Operating System Interface) shell, such as sh. C Shell is not supported.
- If you receive a message saying there is not enough room in the temp directory to perform the installation, set the IATEMPDIR variable to another directory. The installation uses this directory to extract the installation files. Refer to the documentation for your operating system for information on how to set this variable.
- You must install the management server on a machine with a static IP address.
- When you install the management server on Solaris, the following files from InstallAnywhere are left with writable permissions, but they should not be modified. Modifying them may impact other installations that use InstallAnywhere:
  - `$mgr_dist/Uninstall_AppIQ_StorageAuthority/.com.zerog.registry.xml`
  - `/var/.com.zerog.registry.xml`

To install the management server:

1. Access a Solaris host by doing one of the following:
   - **Windows client/X Term program** - Start up a local X server, connect through xterm to the remote system and set your DISPLAY environment variable appropriately.
   - **Solaris** - Run the following command at the command prompt:
     ```
     # /usr/openwin/bin/xhost +
     ```
     Then, set the display to your client. Refer to the documentation for your shell for more information.

2. (Double-byte operating systems only) Remove the `sqlnet.ora` file, which can be found in the `/opt/oracle/product/9.2.0.1.0/network/admin` directory for a default Oracle installation.
3. Mount the Solaris Manager CD-ROM and go to the top directory on the management server CD-ROM. Enter the following at the command prompt:
   `# ./InstallManager.bin`
4. When you see the introduction screen, click **Next**.
5. When you are asked for an installation directory, you can select the default or choose your own. To choose your own directory, click the Choose button. You can always display the default directory by clicking the **Restore Default Folder** button. When you are done, click **Next**.
6. Read the important notes, such as disabling IIS before running the software. Click **Next**.
7. Check the pre-installation summary. You are shown the following:
   - Product Name
   - Installation Folder
   - Disk Space Required
   - Disk Space Available

   Note: Refer to the Support Matrix for information about supported hardware.

8. Do one of the following:
   - Click **Install** if you agree with the pre-installation summary.
   - Click **Previous** if you want to modify your selections.

   The management server is installed.

   Caution: Do not click the **Cancel** button during the installation. You can always remove an unsatisfactory installation.

9. When the installation is complete, you are shown the directory containing the management server and the machine ID, which is used by technical support for licenses.
   You do not need to write down the machine ID. You can obtain it easily from the management server (**Security** > **Licenses**).
10. Do one of the following:
    - **Solaris 9** - Enter the following at the command prompt:

```
# /etc/init.d/appstormanager start
```

- ☐ **Solaris 10** - Do the following:

a. Enter the following at the command prompt:
```
# /etc/init.d/dbora stop
```
b. Enter the following at the command prompt:
```
# /etc/init.d/dbora start
```
c. Enter the following at the command prompt:
```
# /etc/init.d/appstormanager start
```

Important: If you have any questions about the installation, you can look at the install logs, which are located in the `[installation_directory]\logs` directory.

Step 3 - Verify that Processes Can Start

After you install the management server, verify the process for the management server has started. It may take some time for the process to start depending on the server's hardware. The process must be running to monitor and manage your elements. Refer to the appropriate section for your operating system.

Verify that the processes for the management server and Oracle have started.

1. To verify that the required processes for the management server have started, enter the following at the command prompt:
   ```
   # ps -ef | grep java
   ```
   The following is displayed if the CIMOM and for the Java processes have started. This output may differ for your server:

   ```
   /opt/productname/jre/bin/sparcv9/java -Dappiq.mgr.dist=/opt/AppIQ_St
   /opt/productname/jre/bin/sparcv9/java -Xms256m -Xmx1024m -XX:MaxNewS
   ```
   where `/opt/productname` is the directory where you installed the management server
2. To verify the Oracle process has started, enter the following at the command prompt:
   ```
   # ps -ef | grep ora
   ```
   Output resembling the following is displayed:

   ```
   /opt/oracle/product/9.2.0.1.0/bin/tnslsnr LISTENER -inherit
   ```

```
./appstormservice /opt/productname/ManagerData/conf/solaris-wrapper.
 oracle   356     1  0   Jul 30 ?        0:01 ora_pmon_APPIQ
 oracle   358     1  0   Jul 30 ?        0:26 ora_dbw0_APPIQ
 oracle   360     1  0   Jul 30 ?        1:13 ora_lgwr_APPIQ
 oracle   362     1  0   Jul 30 ?        0:39 ora_ckpt_APPIQ
 oracle   364     1  0   Jul 30 ?        0:10 ora_smon_APPIQ
 oracle   366     1  0   Jul 30 ?        0:00 ora_reco_APPIQ
 oracle   368     1  0   Jul 30 ?        0:00 ora_cjq0_APPIQ
 oracle   370     1  0   Jul 30 ?        0:07 ora_arc0_APPIQ
 oracle   372     1  0   Jul 30 ?        0:06 ora_arc1_APPIQ
 oracle  3424     1  0 13:04:48 ?        0:04 oracleAPPIQ (LOCAL=NO)
```

where `/opt/productname` is the directory where you installed the management server

3. If you find your processes for Oracle has not started, you can start the process by entering the following at the command prompt:

   ```
   # /etc/init.d/dbora start
   ```

   If you need to stop the process for Oracle, enter the following at the command prompt:

   ```
   # /etc/init.d/dbora stop
   ```

   Important: If you are starting the processes manually, start the Oracle process before the process for the management server.

4. If you find your process for the management server has not started, you can start the process by entering the following at the command prompt:

   ```
   # /etc/init.d/appstormanager start
   ```

   If you need to stop the process, enter the following at the command prompt:

   ```
   # /etc/init.d/appstormanager stop
   ```

Step 4 - Verify You Can Connect to the Management Server

The appstormanager process must be running for you to connect to the management server.

Keep in mind the following:

- If you do not have a license installed, you are asked to install the license. If you do not have a valid license, contact customer support, as mentioned in the Documentation Center (**Help** > **Documentation Center**). To install the license, click the **Import License File** button on the Licenses tab (**Configuration** > **Licenses**).
- Make sure you do not have pop-up blocking software enabled. If your Web browser has an option for blocking pop-ups, disable it. The management server uses pop-ups for dialog boxes.
- You must manually install the Java Plug-in to access several components on the management server. See the topic, “Installing the Java Plug-in on Sun Solaris” on page 31 for more information.

To access the management server:

1. Type one of the following in a Web browser:
   - For secure connections:
     `https://machinename`
     where `machinename` is the name of the management server.

     To stop receiving a Security Alert message each time you use the HTTPS logon, install the security certificate as described in “Installing the Software Security Certificate” on page 377. Install the security certificate after you have completed the steps in this chapter.

     Important: Enter the DNS name of the computer in the URL instead of localhost, even if you are running a Web browser directly on the management server. If you use `https://localhost` to access the management server, you will receive a “Hostname Mismatch” error when you attempt to use System Explorer or Performance Explorer in the management server.

   - For nonsecure connections:
     `http://machinename`
     where `machinename` is the name of the management server.
2. If you receive an error message when you attempt to connect to the management server, the appstromanger process might be still starting. Wait for it to complete its start script.

Note: If you see a message resembling the following, see the topic, “Receiving “HTTP ERROR: 503" When Accessing the Management Server” on page 365: `Receiving HTTP ERROR: 503 javax.ejb.EJBException: null; CausedByException is: Unexpected Error; nested exception is: java.lang.NoClassDefFoundError`

3. In the management server login page, type `admin` in the **Name** field and `password` in the **Password** field. Then, click **Login**.
4. If you are shown the software license agreement and you agree with its terms, click the **Accept** button.

Note: To prevent the license agreement from being displayed each time you log on to the management server, select **Do not show me this again**.

5. If the management server does not detect a license, you are asked to import the license. Click the **Import License File** button to install the license.
The license file can be obtained from customer support.

Installing the Java Plug-in on Sun Solaris

Java 2 Runtime Environment is required to access several features in the management server, such as System Explorer. If your Web browser is running on Sun Solaris, you must manually install the Java plug-in as described in this section.

To install the Java plug-in:

1. Go to the following URL and download the installation file for the Sun JRE when asked:
`http://<management_server>/appiq/j2re-1_4_2_08- solaris-sparc.sh`

where <management_server> is the hostname of the management server.

2. In a terminal window, execute the downloaded file in a directory where you want the JRE installed.
   This executable installs the Sun JRE on your computer.

   The Java plug-in for your Web browser is available in the following file: $JRE_HOME/plugin/sparc/ns610/libjava_oji.so

   where $JRE_HOME is the directory containing the JRE installation.
3. In a terminal window, go to the $HOME/.mozilla/plugins directory. Create a plugins directory if it does not exist.
4. Remove any existing links to the Java plug-in in this directory.
5. Create a symbolic link to the Java plug-in by using the following command:
   ln -s $JRE_HOME/plugin/sparc/ns610/libjava_oji.so .

   Note: Remember the dot at the end of the command.

6. If you are a root user on the server and you want to make the plug-in available to all users, create a symbolic link in the plugins directory under the browser's installation directory, typically /opt/SUNWns/plugins.

   Note: Any existing plug-ins in a user's home directory take precedence over this system-wide plug-in.

7. Restart your Web browser.

Configurations Required for Discovering EMC CLARiiON Storage Systems

The EMC Navisphere CLI is required for the management server to communicate with the CLARiiON storage system. At the time this documentation was created, EMC distributed the Navisphere CLI as part of the EMC Navisphere Software Suite. Contact your EMC representative

for more information about obtaining the Navisphere CLI. Distribution rights for the Navisphere CLI belong to EMC. For Solaris, you must install the Navisphere Disk Array Management Tool CLI (NAVICLI).

Contact your EMC representative for more information about obtaining the Navisphere CLI. Distribution rights for the Navisphere CLI belong to EMC.

In Navisphere add the following to the privilege user section:

```
SYSTEM@name_of_my_management_server
SYSTEM@IP_of_my_management_server
```

where

- `name_of_my_management_server` is the DNS name of the computer running the management server software
- `IP_of_my_management_server` is the IP address of the computer running the management server software

Removing the Management Server

To remove the management server from Sun Solaris:

1. Access the Solaris host by doing one of the following:
   - **Windows client/X Term program** - Start up a local X server, connect through xterm to the remote system and set your DISPLAY environment variable appropriately.
   - **Solaris** - Run the following command at the command prompt:
     `# /usr/openwin/bin/xhost +`
     Then, set the display to your client. Refer to the documentation for your shell for more information.
2. Stop processes for the management server by entering the following at the command prompt. Leave the Oracle process running
   `# /etc/init.d/appstormanager stop`
3. Verify that the Oracle process is running by entering the following at the command prompt:
   `ps -ef | grep ora`
   Output resembling the following is displayed:

   ```
   /opt/oracle/product/9.2.0.1.0/bin/tnslsnr LISTENER -inherit
   ```

```
./appstormservice /opt/productname/ManagerData/conf/solaris-wrapper.
 oracle   356     1  0   Jul 30 ?        0:01 ora_pmon_APPIQ
 oracle   358     1  0   Jul 30 ?        0:26 ora_dbw0_APPIQ
 oracle   360     1  0   Jul 30 ?        1:13 ora_lgwr_APPIQ
 oracle   362     1  0   Jul 30 ?        0:39 ora_ckpt_APPIQ
 oracle   364     1  0   Jul 30 ?        0:10 ora_smon_APPIQ
 oracle   366     1  0   Jul 30 ?        0:00 ora_reco_APPIQ
 oracle   368     1  0   Jul 30 ?        0:00 ora_cjq0_APPIQ
 oracle   370     1  0   Jul 30 ?        0:07 ora_arc0_APPIQ
 oracle   372     1  0   Jul 30 ?        0:06 ora_arc1_APPIQ
 oracle  3424     1  0 13:04:48 ?        0:04 oracleAPPIQ (LOCAL=NO)
```

where `/opt/productname` is the directory where you installed the management server

4. To uninstall the management server, enter the following at the command prompt:
   `/opt/productname/Uninstall_productname/Uninstall_productname`
   where
   - `/opt/productname` is the directory where you installed the management server
   - `productname` - is the name of the product.
5. If you want to remove license files, remove the directory containing the license files by entering the following at the command prompt:
   `# rm -rf /var/sadm/appiq/app*`
6. To remove leftover files from the management server, remove the directory for the management server by entering the following at the command prompt:
   `# rm -rf /opt/productname`
   where `/opt/productname` is the directory where you installed the management server
7. If you want to remove the EMC WideSky API that installed with the management server, enter the following command to remove the directory containing the API:
   `# rm -rf /var/symapi/`
8. To remove the Oracle instance containing the data for the management server, enter the following at the command prompt:
   `# /opt/oracle/product/9.2.0.1.0/bin/dbca`
9. Select the option for deleting a database. Then, click **Next**.
10. Delete the database using the username SYS. The default password is `change_on_install`. If this password has changed, contact your network administrator.
11. Click **Finish**.
12. (Optional) Verify that the product has been deleted by running the Oracle Database Configuration Assistant (DBCA) again. APPIQ should not be listed as a database.

13. Open the `/var/opt/oracle/oratab` file in a text editor, and remove entries beginning with `APPIQ`, as shown in the following example:
    `APPIQ:/opt/oracle/product/9.2.0.1.0:Y`
14. If you are going to reinstall a new version of the management server, make sure you keep the file `/var/sadm/appiq/orahome`. This file lets you install a new version of the management server by assuming you kept the same Oracle installation.
15. To remove the Oracle software:
    a. Go to `$ORACLE_HOME/oui/bin/`.
    b. Run the `runInstaller.sh` script by entering the following at the command prompt:
    `runInstaller.sh`
    c. If you are asked if you want to continue, click **Y**.
    d. Click **Deinstall Products**.
    e. Select all components.
    f. Click **Remove**.
    The Oracle software is removed.
16. Reboot the server.

Porting the Management Server Across Operating Systems

Use the dbAdmin tool to move data from the management server on Microsoft Windows to Sun Solaris or vice versa. Earlier versions of the management server can be moved to Solaris; however, the earliest build supported for porting is 3.0.

Keep in mind the following:

- The following steps assume you want to move the management server from Windows to Solaris. You can also use the following steps for moving the management server from Solaris to Windows.
- When you move the management server from Windows to Solaris the Windows hosts must be rediscovered for the Windows proxy to become aware of the hosts.
- When the Windows proxy is installed on a new server, the Windows hosts must be re-discovered.

To move the management server from Windows to Solaris:

1. Use the dbAdmin tool to export the database. See the topic, "Exporting the Database" in the User Guide for more information.
   The exported *.zip file contains the following:
   - **Database Schema** - Contains information about the elements your management server monitors.
   - **Oracle Network Configuration Files** - `tnsnames.ora` and `listener.ora`
   - **CIM Repository**
   - **File SRM**
2. Install the management server on Solaris.
3. Move the *.zip file you exported in the first step to the computer running Solaris, such as through FTP.
4. Use the dbAdmin tool to import the *.zip file. See the topic, "Importing the Database" in the User Guide for more information.
5. The dbAdmin tool does the following when the file is imported:
   a. Removes the APPIQ_SYSTEM account.
   b. Creates an APPIQ_SYSTEM account.
   c. Imports data into the APPIQ_SYSTEM account.
   d. Determines the version of the management server the data is from.
   e. Applies the upgrade script according for the version detected. The upgrade script does not run if the detected version is the same as the latest version. The upgrade script updates sequentially.
   f. Upgrades and restores the CIM repository that was exported.
   g. Restores File SRM from the exported files.
6. Sybase is not listed in the topology after you port the management server. Click **Get Topology** (**Discovery** > **Topology**) or **Get Details** (**Discovery** > **Details**) to make the management server aware of Sybase.

Upgrading the Management Server

Keep in mind the following:

- Refer to the release notes for late breaking information about upgrading the management server.
- Complete the upgrade and its subsequent steps in one session, which may take several hours depending on your network configuration. Completing the steps over several sessions will result in incomplete data until all steps have been completed.
- It is necessary to perform Get Details after you upgrade to repopulate the database.
- Upgrade and start the Windows proxy first and then the management server, as described in this section.
- CLI clients earlier than the current revision are not supported.
- Additional steps are required after an upgrade, see the steps in this section for more information.
- The upgrade lets you know about any customizations to configuration files that were made in previous releases. You can view the differences that have been detected in an HTML file in the `[Install_DIR]/logs` directory.

Files backed-up and restored to their original location:

- All files in `$MGR_DIST/JBossandJetty/server/appiq/remoteScripts`
- All files and subdirectories in `$MGR_DIST/JBossandJetty/server/appiq/fsrm`
- *All files and subdirectories in `$MGR_DIST/JBossandJetty/server/appiq/reports/customTreeNodes`
- *All files and subdirectories in `$MGR_DIST/JBossandJetty/server/appiq/reports/custom`
- *All files and subdirectories in `$MGR_DIST/JBossandJetty/server/appiq/reports/definitions/custom`

*This directory may not exist if you have not used Report Designer to create custom reports.

Files backed up to $MGR_DIST/SavedData:

- All files and subdirectories in `$MGR_DIST/JBossandJetty/server/appiq/remoteScripts/advisors` - Used in Business Tools.
- All files and subdirectories in `$MGR_DIST/JBossandJetty/server/appiq/remoteScripts/automators` – Used in Business Tools.

- All files in `$MGR_DIST/JBossandJetty/server/appiq/remoteScripts` – Used in System Explorer.
- All files and subdirectories in `$MGR_DIST/JBossandJetty/server/appiq/policies` - Used in Policy Manager.
- All files and subdirectories in `$MGR_DIST/JBossandJetty/server/appiq/fsrm` – Used in File Server SRM.
- All files and subdirectories in `$MGR_DIST/JBossandJetty/server/appiq/reports` - Used in Reporter.
- `$MGR_DIST/Cimom/bin/runcim.sh`
- `$MGR_DIST/Cimom/config/cimomlog4j.properties`
- `$MGR_DIST/JBossandJetty/server/appiq/conf/log4j.xml`
- `$MGR_DIST/JBossandJetty/server/appiq/conf/jboss.properties`
- `$MGR_DIST/JBossandJetty/bin/run.sh`
- `$MGR_DIST/ManagerData/conf/wrapper.conf`

Step 1 - Stop AppStorManager

Before you begin upgrading the management server, stop AppStorManager, which is the process that runs the management server.

To stop AppStomanager, enter the following at the command prompt as user ‘root’:

```
$ /etc/init.d/appstormanager stop
```

You can make sure AppStorManager has stopped by entering the following at the command prompt:

```
ps -ef | grep java
```

Step 2 - Export Your Existing Database

Export your existing database by using the Database Admin Utility. Refer to the User Guide or online help for more information.

Step 3 - Upgrade and Start the Windows Proxy

You can install the latest version of the Windows Proxy over the previous version. See “Installing the Windows Proxy” on page 280. After you upgrade the Windows proxy, start its service AppStorWinProxy from the Services window on the Windows host.

Step 4 - Upgrade the Management Server

The following steps are required for all users:

1. Make sure OracleOraHome92TNSListener and OracleServiceAPPIQ are running before you begin the upgrade of the management server.
   a. Verify that Oracle processes are running by entering the following at the command prompt:
      ```
      # ps –ef | grep ora
      ```
   b. Verify that ‘tnslsnr’ is running by entering the following at the command prompt:
      ```
      # ps –ef | grep tns
      ```
2. Make sure AppStorManager is stopped before you begin the upgrade.
   You can make sure AppStorManager has stopped by entering the following at the command prompt:

   ```
   ps -ef | grep java
   ```
3. Install the management server, as described in the topic, “Step 2 - Install the Management Server” on page 26.
   The management server automatically installs to its previous location.
4. Start AppStorManager by entering the following at the command prompt:
   ```
   $ /etc/init.d/appstormanager start
   ```
5. Check for the following:
   - The AppStorManager process has started.
   - The OracleOraHome92TNSListener and OracleServiceAPPIQ processes have started.
   - You can access the management server by a Web browser.

Step 5 - Required Changes for Discovered McDATA and Connectrix Switches

If you have previously discovered McDATA and Connectrix switches through SNMP, you must modify the cimom.properties file as described in the following steps:

1. Click **Configuration** > **Product Health**.
2. Click **Advanced** in the Disk Space tree.
3. Click **Show Default Properties** at the bottom of the page.
4. Copy the following property. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.
   `#cimom.useSnmpMcDataProvider=true`
5. Return to the Advanced page (**Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree).
6. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
7. Uncomment the `cimom.useSnmpMcDataProvider=true` property by removing the number sign (#) in front of `cimom.useSnmpMcDataProvider=true`.
8. When you are done, click **Save**.
9. Restart the process for the management server for your changes to take effect.
   While appstormanager is restarting, users are not able to access the management server. The appstormanager process must be running for the management server to monitor elements. See the help for your operating system platform for details on how to verify that the process is running.

Step 6 - Remove and Rediscover Certain Elements

If you previously discovered the following elements, you must remove and rediscover them as described in this section:

- File servers - You must remove its access points.
- Cisco, QLogic, or CNT switches supported through SMI-S
- Elements discovered in builds earlier than 4.0:
  - CNT switches
  - HP XP storage systems

- HP EVA storage systems
- Sun 6920 storage systems

1. To remove elements and their access points:
   a. Go to the Get Topology Information page for the Topology (**Discovery** > **Topology** in the upper-right corner).
   b. Click the  button corresponding to the elements you need to remove.

Note: An element may be listed more than once in the table if it was discovered through multiple access points. You must delete all of its access points by removing all the entries of the element in the topology table.You may end up removing other elements from the table as well. For example, if a CNT switch was used to discover host_A and host_B, you will end up removing host_A and host_B from the topology table. You will obtain information about your elements again, once you perform Get Details in the next step.

---

2. Rediscover the elements you removed. Select **Discovery** > **Setup** in the upper-right corner. Authentication information is already be stored with the elements.
3. Click the **Start Discovery** button to rediscover the deleted access points.

Step 7 - Perform Get Details

Perform Get Details for all elements to repopulate the database. Get Details is also required to repopulate information for Brocade switches. Click **Discovery** > **Details**. Then, click **Get Details**.

Step 8 - Re-add Remote Sites in Global Reporter

All sites that provide global reports must be upgraded to this version of the management server. Install this version of the management server on all remote sites, then complete the following steps for each management server that is using Global Reporter.

1. You must modify the listener.ora file at each remote site, as described in the following steps. For example, assume you have three remote sites. You must log onto each of these remote sites and modify the listener.ora file at each remote site, as described in the following steps:

a. Log onto the remote site.
b. Stop the process for the management server.
c. As user 'Oracle' (`su - oracle`), stop the Oracle listener by entering the following at the command prompt:
   `# lsnrctl stop`
d. Open the following file in a text editor on the computer:
   `$ORACLE_HOME/network/admin/listener.ora`
e. After `(ADDRESS = (PROTOCOL = TCP)(HOST = localhost)(PORT = 1521))`, add the following line:
   `(ADDRESS = (PROTOCOL = TCP)(HOST =` 192.168.10.1`)(PORT = 1521))`
   where 192.168.10.1 is the IP address of the local host server. Replace 192.168.10.1 with the IP address of your local host.

   The text should now appear as follows:

```
LISTENER =
 (DESCRIPTION_LIST =
   (DESCRIPTION =
     (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = localhost)(PORT = 1521))
      (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.10.1)(PORT = 1521))
     )
   )
 )
```

f. Save the file and exit.
g. Start the listener process for Oracle (OracleOraHome92TNSListener).
h. Start AppStorManager.

2. Open the page for Global Reporter (**Configuration** > **Reports** > **Data Collection** > **Global Reporter**) on the Global Reporter server and remove all remote sites listed by clicking the  button.
3. Click the **Refresh Now** button at the bottom of the page. This action clears the management server database.
4. Add desired remote sites, by clicking the **New Site** button and providing the appropriate information. Refer to the User Guide and online help for more information.
5. To update the database with data from the added sites, click the **Refresh Now** button at the bottom of the page.

Step 9 - Rescan for File Servers

File SRM data will be incomplete after upgrading the management server. You must run a File SRM scan. Refer to the User Guide for more information on how to schedule a File SRM scan.

CHAPTER 3

Installing the Management Server on Microsoft Windows

If you did not receive a computer with the management server installed on it, first complete the steps in this section.

Note: The steps in this section are for installing the management server on Microsoft Windows. See “Upgrading the Management Server” on page 56 for information about how to upgrade the management server.

Keep in mind the following:

- **All steps must be completed for the management server to work properly.**
- Before beginning any installation or upgrade steps, refer to the Support Matrix to determine the minimum software and hardware requirements.
- For optimal performance, install the management server on a dedicated computer.
- Installation through a terminal server or using Virtual Network Computing (VNC) software is not supported.
- The directory in which you install the management server must have write access for the local Administrators group. Be aware that installing the management server in a directory created by another program (for example: the Proliant Support Pack) is not recommended.

This chapter describes the following:

- Step 1 - Install the Oracle Database (Windows) on page 46
- Step 2 - Install the Management Server on page 49
- Step 3 - Verify that Services Can Start on page 51
- Step 4 - Verify You Can Connect to the Management Server on page 51
- Configurations Required for Discovering EMC CLARiiON Storage Systems on page 53
- Removing the Management Server on page 54
- Porting the Management Server Across Operating Systems on page 55
- Upgrading the Management Server on page 56

Step 1 - Install the Oracle Database (Windows)

Important: Install Oracle on a computer that does not already have Oracle installed, but with the latest service pack and security patches.

The management server uses Oracle to store the data it collects from the hardware it monitors. The management server ships with a three-CD set for the management server database and an additional CD-ROM for Database Patch 9.2.0.6.0. During the installation of the database, you are prompted to change CD-ROMs. After the installation, you must install the database patch from the Database Patch CD-ROM.

Keep in mind the following:

- Refer to the Support Matrix on the management server CD-ROM for system requirements.
- Once you have started the installation, do not exit out of it. Future installations of the management server database may think you have already installed the software if you exit several minutes into the installation and orauser has already been created.
- Install the database on the computer on which you plan to install the management server.
- For double-byte languages, the Oracle installation provides an extra dialog screen, which is for the Oracle Net Configuration Assistant. This screen requires the user to select the check box and click **Next**. Once you clicked **Next**, a command window appears. The

command window will close itself once the operation running inside the command window completes.

The installation of Oracle is comprised of two steps:

- Installing the database - See “Installing the Oracle Database” on page 47.
- Installing the Oracle patch - See “Installing the Oracle Patch (Windows)” on page 47.

Installing the Oracle Database

To install the database:

1. Insert CD 1 of the database set that ships with the management server.
2. Allow the CD to autorun. If you must run the installation manually, double-click **inst.cmd** found in the `/AppIQ` directory.
   The installation spans several CD-ROMs. During the installation, you are asked to switch CD-ROMs.
3. When you are asked if you want to set the `ORA_HOME` environment variable, click **Yes** if it has not been set or you want to change the location. The default is `c:\oracle\ora92`.
4. Enter the directory and its path that will contain the database, for example: `D:\database` where `D:\database` is the directory that will contain the database.

   Important: Do not specify a directory with spaces, such as the Program Files directory or any directories under Program Files.

5. Select **No Database Creation** when you are asked if you want to create a database. Select the defaults for all three CDs (Disks).

Installing the Oracle Patch (Windows)

The steps provided in this section describe how to install Oracle Server Patch 9.2.0.6.0 and a supplemental patch (`runDictionaryUpgrade.bat`). After you install Oracle Server Patch 9.2.0.6.0, you must install a supplemental patch (`runDictionaryUpgrade.bat`) if you have an existing management server database.

Note: If you are not sure if you have already installed the patch, access the Oracle Universal Installer (**Start** > **Programs** > **Oracle Installation Products** > **Universal Installer**). In the Oracle Universal Installer, click **Installed Products**. Then, expand the OraHome tree. The installed products are displayed. Look for the highest patch level. To exit the Oracle Universal Installer, click **Close**, and then click **Exit**. When asked if you want to exit, click **Yes**.

To install the Oracle patch:

1. Change the service startup type of all Oracle services, AppStorManager and the Distributed Transaction Coordinator service to manual. The AppStorManager service is not available if you are installing the management server for the first time. Oracle services usually start with Oracle, for example:
   - OracleOraHome92Agent
   - OracleOraHome92ClientCache
   - OracleOraHome92SNMPPeerEncapsulator
   - OracleOraHome92SNMPPeerMasterAgent
   - OracleOraHome92TNSListener
   - OracleServiceAPPIQ

   Note: Before you change the service startup types, make note of the services that are set to automatic, as you will need to restore the service startup settings when you are done with installing the patch.

2. Reboot the server.
3. Insert the Database Patch CD into the CD-ROM drive.
4. Open a command prompt window and go to the CD-ROM directory by entering the following:
   `d:`
   where d is the drive letter for the CD-ROM drive
5. Enter the following at the command prompt:
   `d:\> installPatch.cmd`
   If you are asked for the path to the Oracle home, provide the path. The path for the default Oracle installation is `c:\oracle\ora92`.
6. To accept the default settings in the File Locations dialog, click **Next**.

The patch is installed.

7. If you are patching an existing management server database, start the OracleServiceAPPIQ service, OracleOraHome92TNSListener (listener) service and run the `runDictionaryUpgrade.bat` script. The `runDictionaryUpgrade.bat` script can be found on the top level of the Database Patch CD-ROM.
8. You receive an error if a database does not exist. Ignore the error.
9. Restore the Oracle services, AppStorManager and the Distributed Transaction Coordinator service to automatic so they automatically start the next time the server is rebooted.
10. Reboot the server.

Step 2 - Install the Management Server

Keep in mind the following:

- Refer to the Support Matrix for operating system requirements on the management server CD-ROM.
- Refer to the release notes for late breaking information.
- Make sure no other programs are running when you install the management server.
- If you are installing the management server in a production environment, you must install the management server on a machine with a static IP address.
- The management server uses the following ports. Make sure these ports are available:
  - 4444 - JBoss JRMPInvoker
  - 4445 - JBoss PooledInvoker
  - 8009 - JBoss EmbeddedTomcatService
  - 8083 - JBoss WebService
  - 8093 - JBoss UILServerILService
  - 5986 - RMI port for JwsMain (see JwsMain.java)
  - 5988 - WBEM HTTP

To install the management server:

1. (Operating systems running double-byte languages only) Remove the `sqlnet.ora` file, which can be found in the `\oracle\ora92\network\admin` directory for a default Oracle installation.
2. Insert the Windows Manager CD-ROM and double-click **InstallManager.exe**.

3. When you see the introduction screen, click **Next**.
4. When you are asked for an installation directory, you can select the default or choose your own. To choose your own directory, click the Choose button. You can always display the default directory by clicking the **Restore Default Folder** button. When you are done, click **Next**.
5. Read the important notes, such as disabling IIS before running the software. Click **Next**.
6. Check the pre-installation summary. You are shown the following:
   - Product Name
   - Installation Folder
   - Disk Space Required
   - Disk Space Available

   Note: Refer to the Support Matrix for information about supported hardware.

7. Do one of the following:
   - Click **Install** if you agree with the pre-installation summary.
   - Click **Previous** if you want to modify your selections.

   The management server is installed.

   Caution: Do not click the **Cancel** button during the installation. You can always remove an unsatisfactory installation.

8. When the installation is complete, you are shown the directory containing the management server and the machine ID, which is used by technical support for licenses.
   You do not need to write down the machine ID. You can obtain it easily from the management server (**Security** > **Licenses**).
9. You must reboot the server.
   The AppStorManager service starts automatically after a reboot.

Important: If you have any questions about the installation, you can look at the install logs, which are located in the `%MGR_DIST%\logs` directory.

Step 3 - Verify that Services Can Start

After you install the management server, verify the service for the management server has started. It may take some time for the service to start depending on the server's hardware. The service must be running to monitor and manage your elements. Refer to the appropriate section for your operating system.

After you restart the management server, you can verify that the required services have started.

To verify services have started:

1. Access the Services window by doing the following:
   a. Right-click **My Computer**.
   b. Select **Manage** from the drop-down menu.
   c. In the left pane of the Computer Management window, select **Services and Applications**.
   d. In the right pane, double-click **Services**.
2. Verify that the following services have been started by looking under the Status column in the Services window.
   - AppStorManager (must be set to automatic)
   - OracleOraHome92TNSListener (must be set to automatic)
   - OracleServiceAPPIQ (must be set to automatic)
3. Verify that the following services are disabled or not installed by looking under the Status column in the Services window
   - OracleOraHome92HttpServer
   - IIS (Internet Information Server)

Step 4 - Verify You Can Connect to the Management Server

The AppStorManager service must be running for you to connect to the management server. You can tell the service has started by looking under the Status column in the Services window. Refer to the documentation accompanying the operating system for more information.

Keep in mind the following:

- If you do not have a license installed, you are asked to install the license. If you do not have a valid license, contact customer support, as mentioned in the Documentation Center (**Help** > **Documentation Center**). To install the license, click the **Import License File** button on the Licenses tab (**Configuration** > **Licenses**).
- Make sure you do not have pop-up blocking software enabled. If your Web browser has an option for blocking pop-ups, disable it. The management server uses pop-ups for dialog boxes.

To access the management server:

1. Type one of the following in a Web browser:
   - For secure connections:
     `https://machinename`
     where `machinename` is the name of the management server.

     To stop receiving a Security Alert message each time you use the HTTPS logon, install the security certificate as described in “Installing the Software Security Certificate” on page 377. Install the security certificate after you have completed the steps in this chapter.
   - For nonsecure connections:

     Important: Enter the DNS name of the computer in the URL instead of localhost, even if you are running a Web browser directly on the management server. If you use `https://localhost` to access the management server, you will receive a “Hostname Mismatch” error when you attempt to use System Explorer or Performance Explorer in the management server.

     `http://machinename`
     where `machinename` is the name of the management server.
2. If you receive an error message when you attempt to connect to the management server, the AppStorManager service might be still starting. Wait for it to complete its start script.

Note: If you see a message resembling the following, see the topic, “Receiving “HTTP ERROR: 503" When Accessing the Management Server” on page 365: `Receiving HTTP ERROR: 503 javax.ejb.EJBException: null; CausedByException is: Unexpected Error; nested exception is: java.lang.NoClassDefFoundError`

3. In the management server login page, type `admin` in the **Name** field and `password` in the **Password** field. Then, click **Login**.
4. If you are shown the software license agreement and you agree with its terms, click the **Accept** button.

Note: To prevent the license agreement from being displayed each time you log on to the management server, select **Do not show me this again**.

5. If the management server does not detect a license, you are asked to import the license. Click the **Import License File** button to install the license.
The license file can be obtained from customer support.

Configurations Required for Discovering EMC CLARiiON Storage Systems

The EMC Navisphere CLI is required for the management server to communicate with the CLARiiON storage system. At the time this documentation was created, EMC distributed the Navisphere CLI as part of the EMC Navisphere Software Suite. Contact your EMC representative for more information about obtaining the Navisphere CLI. Distribution rights for the Navisphere CLI belong to EMC. For Solaris, you must install the Navisphere Disk Array Management Tool CLI (NAVICLI).

Contact your EMC representative for more information about obtaining the Navisphere CLI. Distribution rights for the Navisphere CLI belong to EMC.

In Navisphere add the following to the privilege user section:

```
SYSTEM@name_of_my_management_server
SYSTEM@IP_of_my_management_server
```

where

- `name_of_my_management_server` is the DNS name of the computer running the management server software
- `IP_of_my_management_server` is the IP address of the computer running the management server software

Removing the Management Server

This section describes how to remove the management server. Refer to the appropriate section for your operating system.

To remove the management server:

1. Stop the service for the management server by doing the following:
   a. Go to the Services window (**Control Panel** > **Administrative Tools** > **Services**).
   b. Right-click the **AppStorManager** service in the Services window.
   c. Select **Stop** from the drop-down menu.
2. Open the Add/Remove Programs window, which is accessible from the Control Panel.
3. In the Add/Remove Programs window, select **the product name** and then click the Change/Remove button.
4. In the InstallShield Wizard window, select the **Remove** option. Then, click **Next**.
5. When you are asked if you want to completely remove the selected application and all of its features, click **OK**.
6. If files were added or modified after the original installation, the `%MGR_DIST%` directory may still exist. You may need to reboot the management server before you can delete this directory.

7. Remove the OracleServiceAPPIQ database instance from Oracle, as described in the following steps:

   Note: You can also use the Oracle DBCA (Database Configuration Assistant) tool to remove OracleServiceAPPIQ. Click **Start** > **Oracle-OraHome92** > **Configuration and Management Tools** > **Database Configuration Assistant**.

   a. Enter the following at a command prompt on the management server:
      `oradim -delete -SID APPIQ`
   b. Delete the following directories and their contents on the management server:
      - `c:\oracle\oradata\APPIQ`
      - `c:\oracle\admin\APPIQ`
      - `%ORA_HOME%\rman if applicable`

      The above deletes the APPIQ database instance.

Porting the Management Server Across Operating Systems

Use the dbAdmin tool to move data from the management server on Microsoft Windows to Sun Solaris or vice versa. Earlier versions of the management server can be moved to Solaris; however, the earliest build supported for porting is 3.0.

Keep in mind the following:

- The following steps assume you want to move the management server from Windows to Solaris. You can also use the following steps for moving the management server from Solaris to Windows.
- When you move the management server from Windows to Solaris the Windows hosts must be rediscovered for the Windows proxy to become aware of the hosts.
- When the Windows proxy is installed on a new server, the Windows hosts must be re-discovered.

To move the management server from Windows to Solaris:

1. Use the dbAdmin tool to export the database. See the topic, "Exporting the Database" in the User Guide for more information.
   The exported *.zip file contains the following:
   - **Database Schema** - Contains information about the elements your management server monitors.
   - **Oracle Network Configuration Files** - `tnsnames.ora` and `listener.ora`
   - **CIM Repository**
   - **File SRM**
2. Install the management server on Solaris.
3. Move the *.zip file you exported in the first step to the computer running Solaris, such as through FTP.
4. Use the dbAdmin tool to import the *.zip file. See the topic, "Importing the Database" in the User Guide for more information.
5. The dbAdmin tool does the following when the file is imported:
   a. Removes the APPIQ_SYSTEM account.
   b. Creates an APPIQ_SYSTEM account.
   c. Imports data into the APPIQ_SYSTEM account.
   d. Determines the version of the management server the data is from.
   e. Applies the upgrade script according for the version detected. The upgrade script does not run if the detected version is the same as the latest version. The upgrade script updates sequentially.
   f. Upgrades and restores the CIM repository that was exported.
   g. Restores File SRM from the exported files.
6. Sybase is not listed in the topology after you port the management server. Click **Get Topology** (**Discovery** > **Topology**) or **Get Details** (**Discovery** > **Details**) to make the management server aware of Sybase.

Upgrading the Management Server

Keep in mind the following:

- Refer to the release notes for upgrade path and late breaking information about upgrading the management server.
- Complete the upgrade and its subsequent steps in one session, which may take several hours depending on your network configuration. Completing the steps over several sessions will result in incomplete data until all steps have been completed.
- It is necessary to perform Get Details after you upgrade to repopulate the database.
- By default, the Brocade switch provider is set to Fabric Access API after upgrading. See “Important Information About Upgrading and Brocade Switches” on page 60 if your SAN includes Brocade switches and you are upgrading to build 5.1.
- It is important to clear the client java cache after upgrading the management server.
- Additional steps are required after an upgrade, see the steps in this section for more information.
- CLI clients earlier than the current revision are not supported.
- The upgrade lets you know about any customizations to configuration files that were made in previous releases. You can view the differences that have been detected in an HTML file in the `%MGR_DIST%\logs` directory.

Files backed-up and restored to their original location:

- All files in `%MGR_DIST%\JBossandJetty\server\appiq\remoteScripts`
- All files and subdirectories in `%MGR_DIST%\JBossandJetty\server\appiq\fsrm`
- *All files and subdirectories in `%MGR_DIST%\JBossandJetty\server\appiq\reports\customTreeNodes`
- *All files and subdirectories in `%MGR_DIST%\JBossandJetty\server\appiq\reports\custom`
- *All files and subdirectories in `%MGR_DIST%\JBossandJetty\server\appiq\reports\definitions\custom`

*This directory may not exist if you have not used Report Designer to create custom reports.

Files backed up to %MGR_DIST%\SavedData:

- All files and subdirectories in `%MGR_DIST%\JBossandJetty\server\appiq\remoteScripts\advisors` - Used in Business Tools.

- All files and subdirectories in `%MGR_DIST%\JBossandJetty\server\appiq\remoteScripts\automators` - Used in Business Tools.
- All files in `%MGR_DIST%\JBossandJetty\server\appiq\remoteScripts` - Used in System Explorer.
- All files and subdirectories in `%MGR_DIST%\JBossandJetty\server\appiq\policies` - Used in Policy Manager.
- All files and subdirectories in `%MGR_DIST%\JBossandJetty\server\appiq\fsrm` - Used in File Server SRM.
- All files and subdirectories in `%MGR_DIST%\JBossandJetty\server\appiq\reports` - Used in Reporter.
- `%MGR_DIST%\Cimom\bin\runcim.sh`
- `%MGR_DIST%\Cimom\config\cimomlog4j.properties`
- `%MGR_DIST%\JBossandJetty\server\appiq\conf\log4j.xml`
- `%MGR_DIST%\JBossandJetty\server\appiq\conf\jboss.properties`
- `%MGR_DIST%\JBossandJetty\bin\run.sh`
- `%MGR_DIST%\ManagerData\conf\wrapper.conf`

Step 1 - Stop AppStorManager

Before you begin upgrading the management server, stop AppStorManager, which is the service that runs the management server.

Step 2 - Export Your Existing Database

Export your existing database by using the Database Admin Utility. Refer to the User Guide or online help for more information.

Step 3 - Upgrade the Management Server

This step is required for all users. To upgrade the Management Server:

1. Make sure OracleOraHome92TNSListener and OracleServiceAPPIQ are running before you begin the upgrade of the management server.

2. Make sure AppStorManager is stopped.
3. Set AppStorManager service startup type to Manual.
4. Be sure that the installation directory has write access for the local Administrators group.
5. Install the management server. See “Step 2 - Install the Management Server” on page 49.
6. Reboot the system when you are asked.
   This step is important as the AppStorManager service may not start correctly otherwise.
7. Check for the following:
   - ☐ The AppStorManager service has started.
   - ☐ The OracleOraHome92TNSListener and OracleServiceAPPIQ services have started.
   - ☐ You can access the management server by a Web browser.

Step 4 - Required Changes for Discovered McDATA and Connectrix Switches

If you have previously discovered McDATA and Connectrix switches through SNMP, you must modify the cimom.properties file as described in the following steps:

1. Click **Configuration** > **Product Health**.
2. Click **Advanced** in the Disk Space tree.
3. Click **Show Default Properties** at the bottom of the page.
4. Copy the following property. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.
   `#cimom.useSnmpMcDataProvider=true`
5. Return to the Advanced page (**Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree).
6. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
7. Uncomment the `cimom.useSnmpMcDataProvider=true` property by removing the number sign (**#**) in front of `cimom.useSnmpMcDataProvider=true`.
8. When you are done, click **Save**.
9. Restart the service for the management server for your changes to take effect.
   While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor

elements. See the help for your operating system platform for details on how to verify that the service is running.

Step 5 - Remove and Rediscover Certain Elements

If you previously discovered the following elements, you must remove and rediscover them as described in this section:

- File servers - You must remove its access points.
- Brocade (see “Important Information About Upgrading and Brocade Switches” on page 60), CNT, Cisco, QLogic, and specific models of McDATA switches supported through SMI-S (see the Support Matrix for details on SMI-S compliant McDATA switches. Click **Help** > **Documentation Center** > **Support Matrix** from the management server).
- Elements discovered in builds earlier than 4.0:
  - CNT switches
  - HP XP storage systems
  - HP EVA storage systems
  - Sun 6920 storage systems

1. To remove elements and their access points:
   a. Go to the Get Topology Information page for the Topology (**Discovery** > **Topology** in the upper-right corner).
   b. Click the  button corresponding to the elements you need to remove.

Note: An element may be listed more than once in the table if it was discovered through multiple access points. You must delete all of its access points by removing all the entries of the element in the topology table.You may end up removing other elements from the table as well. For example, if a CNT switch was used to discover host_A and host_B, you will end up removing host_A and host_B from the topology table. You will obtain information about your elements again, once you perform Get Details in the next step.

---

2. Rediscover the elements you removed. Select **Discovery** > **Setup** in the upper-right corner. Provide the authentication information for your elements, as described in “Discovery Steps” on page 66.

Step 6 - Perform Get Details

Perform Get Details for all elements to repopulate the database. Get Details is also required to repopulate information for Brocade switches. Click **Discovery** > **Details**. Then, click **Get Details**.

Important Information About Upgrading and Brocade Switches

As mentioned earlier, with new installations of build 5.1 of the management server, the default Brocade provider is SMI-S. If you upgrade to build 5.1 from any build prior to 4.2 of the management server your Brocade switches are discovered using the Brocade Fabric Access API.

To change the default discovery provider from Brocade Fabric Access API to Brocade SMI-S after an upgrade follow the steps below:

1. Delete any previously discovered Brocade switches. See “Step 5 - Remove and Rediscover Certain Elements” on page 59 for details.
2. Change the Brocade provider setting. See “About Brocade Discovery (Specifying Brocade Discovery Using Fabric Access API or SMI-S)” on page 83 and specify the Brocade SMI-S setting).
3. Restart the AppStorManager service.

Important: Before performing any provisioning operations that involve a Brocade switch you must perform Discovery Data Collection/Get Details for any subset of elements that includes the Brocade switch. See “Get Details” on page 138.

See “Discovering Brocade Switches” on page 81 and “About Brocade Discovery (Specifying Brocade Discovery Using Fabric Access API or SMI-S)” on page 83 for important information.

Step 7 - Re-add Remote Sites in Global Reporter

All sites that provide global reports must be upgraded to this version of the management server. Install this version of the management server on all remote sites, then complete the following steps for each management server that is using Global Reporter.

1. You must modify the listener.ora file at each remote site, as described in the following steps. For example, assume you have three remote sites. You must log onto each of these remote sites and modify the listener.ora file at each remote site, as described in the following steps:
   a. Log onto the remote site.
   b. Stop the service for the management server running.
   c. Stop the listener service for Oracle (OracleOraHome92TNSListener).
   d. Open the following file in a text editor on the computer:
      `%ORA_HOME%\network\admin\listener.ora`
   e. After `(ADDRESS = (PROTOCOL = TCP)(HOST = localhost)(PORT = 1521))`, add the following line:
      `(ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.10.1)(PORT = 1521))`
      where 192.168.10.1 is the IP address of the local host server. Replace 192.168.10.1 with the IP address of your local host.

      The text should now appear as follows:

```
LISTENER =
 (DESCRIPTION_LIST =
   (DESCRIPTION =
     (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = localhost)(PORT = 1521))
      (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.10.1)(PORT = 1521))
     )
   )
 )
```

   f. Save the file and exit.
   g. Start the listener service for Oracle (OracleOraHome92TNSListener).
   h. Start AppStorManager.
2. Open the page for Global Reporter (**Configuration** > **Reports** > **Data Collection** > **Global Reporter**) on the Global Reporter server and remove all remote sites listed by clicking the  button.

3. Click the **Refresh Now** button at the bottom of the page. This action clears the management server database.
4. Add desired remote sites, by clicking the **New Site** button and providing the appropriate information. Refer to the User Guide and online help for more information.
5. To update the database with data from the added sites, click the **Refresh Now** button at the bottom of the page.

Step 8 - Rescan for File Servers

File SRM data will be incomplete after upgrading the management server. You must run a File SRM scan. Refer to the User Guide for more information on how to schedule a File SRM scan.

CHAPTER 4

Discovering NAS Devices, Tape Libraries, Switches and Storage Systems

Before you can use the management server, you must make the software aware of the elements on your network. An element is anything on the network that can be detected by the management server, such as a switch. This is done through the discovery process. Discovery obtains a list of discovered elements and information about their management interface and dependencies. The management server can discover only elements with a suitable management interface. Refer to the support matrix for supported hardware.

This chapter describes the following:

- Discovery Steps on page 66
- Overview of Discovery Features on page 69
- Step 1 - Discover Switches on page 78
- Step 2 - Discover Storage Systems, NAS Devices and Tape Libraries on page 106
- Step 3 - Build the Topology on page 132
- Step 4 - Get Details on page 137
- Troubleshooting Mode on page 142
- Managing McDATA and EMC Connectrix Switches on page 143
- Assigning a File Extension in Netscape 7 on page 146
- Filtering Discovery Groups on page 147
- Moving Elements to Another Discovery Group on page 147
- Placing an Element in Quarantine on page 148

- Removing an Element from Quarantine on page 149
- Updating the Database with Element Changes on page 149
- Notifying the Software of a New Element on page 150

Discovery Steps

Discovery for switches, storage systems, tape libraries and NAS devices consists of several steps:

1. Discover your switches. See “Step 1 - Discover Switches” on page 78.
2. Discover your storage systems, tape libraries, and NAS devices. See “Step 2 - Discover Storage Systems, NAS Devices and Tape Libraries” on page 106.
3. (Optional) If you want to view the topology quickly in System Explorer, obtain the topology as described in “Step 3 - Build the Topology” on page 132. Keep in mind this step only gathers the information necessary for displaying the topology.
4. Perform Get Details. Get Details is required to obtained detailed information from the elements you discovered. You must run Get Details to obtain provisioning information. This step takes some time to complete. Run Get Details when the network is not busy. See “Step 4 - Get Details” on page 137 for more information.

Important: Before performing any provisioning operations that involve a Brocade switch you must perform Discovery Step 3 for any subset of elements that includes this Brocade switch.

Overall Discovery Tasks

Make sure you have reviewed Table 1-1, “Roadmap for Installation and Initial Configurations,” on page 2 to ensure you are at the correct step.

Keep in mind the following:

- To save time, make sure the user names and passwords are correct. When credentials are not supplied, the default user names and passwords are tried for the element.
- After you discover an EMC Connectrix or McDATA switch, the IP address displayed next to the name of the switch is actually the IP address of the service processor for the switch in

the Get Details screens. To find the IP address of the switch, click the link for the switch in one of the following screens:

- Topology screen (**Discovery** > **Topology**).
- Get Details screen (**Discovery** > **Details**).

Then, click the **Properties** tab. The Properties tab can also be accessed by double clicking the switch in System Explorer. Complete the steps in this chapter before you try to find the IP address of the switch.

- If you are having a problem with discovering an element, try enabling Troubleshooting Mode. See “Troubleshooting Mode” on page 142 for more information. If you are still having a problem, see Chapter 18, “Troubleshooting” on page 363.
- The management server does not display additional information about excluded elements in the user interface; however, the IP addresses of excluded elements appear in the following locations:
  - Discovery screen (**Discovery** > **Setup**).
  - Topology screen (**Discovery** > **Topology**).
  - Get Details screen (**Discovery** > **Details**).

  The management server, however, does mention in the logs (**Discovery** > **View Logs**) that a provider instance has been created for an excluded element. You can ignore this message that appears in the logs.
- To obtain information about the storage area network (SAN), include in the discovery the IP addresses for the following:
  - **Fibre channel switch** The fibre channel switch contains a list of all elements within the fabric. The management server obtains a detailed listing of all elements connected to the switch fabric.
  - **A host containing a Host Bus Adapter (HBA)** All fibre channel host adapters look for available elements attached to the HBA. This information is gathered by CIM Extensions and sent to the management server. Since you have not installed CIM Extensions yet, the management server obtains limited information on the hosts when you perform discovery this time around.
  - **A proxy connected to the SAN** - Include a proxy that has a direct connection or a SAN connection to the management server. An example of a proxy is the EMC Solutions Enabler or Hitachi HiCommand Device Manager. Engenio storage systems do not require a proxy, as they can be accessed directly. Make sure the proxy service has started. On a computer running Windows, this can be determined by looking in the Services window. EMC Solutions Enabler version 5.1 requires additional steps for discovery. See “Discovering EMC Solutions Enabler 5.1” on page 110 for more information.

Note: Before performing any provisioning operations that involve a Brocade switch you must perform Discovery Step 3 for any subset of elements that includes this Brocade switch.

To make the management server aware of elements on your network follow the steps in the following table.

Table 4-1: Discovery Steps for Switches, NAS Devices, and Storage Systems

Step	Description
1	If you have several switches and storage systems that use the same password and user name, set that password and user name as the default. See “Setting Default User Names and Passwords” on page 70 for more information.
2	Discover your switches. See Table 4-2, “Discovery Requirements for Switches,” on page 79 for information on how to discover the types of switches in your network. One way to detect multiple IP addresses at once is to add an IP range for scanning. The management server scans the IP range for elements and populates the discovery list with element it could contact. You can then discover those elements. See “Adding an IP Range for Scanning” on page 72 for more information.

Table 4-1: Discovery Steps for Switches, NAS Devices, and Storage Systems (Continued)

Step	Description
3	Discover your NAS devices and storage systems. See Table 4-7, “Discovery Requirements for Storage Systems, Tape Libraries & NAS Devices,” on page 107.
4	Get Details (**Discovery** > **Details**) is required to obtain information from your discovered elements. Obtaining details takes some time. You might want to perform this process when the network and the managed elements are not busy. You can obtain a picture of device connectivity quickly, by clicking the **Get Topology** button on the **Topology** tab. See the following topics for more information: ■ “Step 3 - Build the Topology” on page 132 ■ “Step 4 - Get Details” on page 137

Overview of Discovery Features

With discovery, you can:

- Provide up to three default user name and passwords for discovery.
- Import pre-existing discovery lists, so you do not need to re-enter discovery information.
- Save your existing discovery list.
- Modify a discovery entry.
- Remove elements from a discovery list.

This section describes the following:

- Setting Default User Names and Passwords on page 70
- Adding an IP Range for Scanning on page 72
- Adding a Single IP Address or DNS Name for Discovery on page 73
- Modifying a Single IP Address Entry for Discovery on page 75
- Removing Elements from the Addresses to Discover List on page 76

Setting Default User Names and Passwords

You can specify up to three default user names and passwords. If several of the elements in the same domain use the same user name and password, assign the user name and password as the default. The management server uses the default user names and passwords if a user name and password are not assigned to an element in the **Setup** screen.

For example, if you have several hosts using the same user name and password, you could enter the default user name and password. If one of the hosts is connected to a storage system with another user name and password, you would also enter this user name and password. Do not specify the user name and password for the storage system in the individual range because that overrides the default user name and password.

To access a Windows-based device, prefix the user name with `domain_name\`, as shown in the following example. This is required by the Windows login mechanism.

```
domain_name\user_name
```

where

- `domain_name` is the domain name of the element
- `user_name` is the name of the account used to access that element

To save time, make sure the user names and passwords are correct. The software tries each of the default user names and passwords whenever it finds an element.

To add the default user name and passwords:

1. Click **Discovery**, then click **Setup** in the upper-right pane of the window.
2. Under Discovery Setup, select **Step 1** at the top of the screen.
3. Click the link, **Set Default User Name and Password**.
4. In the **User Name** field, type the user name for one or more elements.
5. In the **Password** field, type the corresponding password for the user name typed in the previous step.
6. In the **Verify Password** field, retype the password.
7. Repeat steps 4 through 6 for other default user names and passwords you want to add.
8. Click **Add System**.

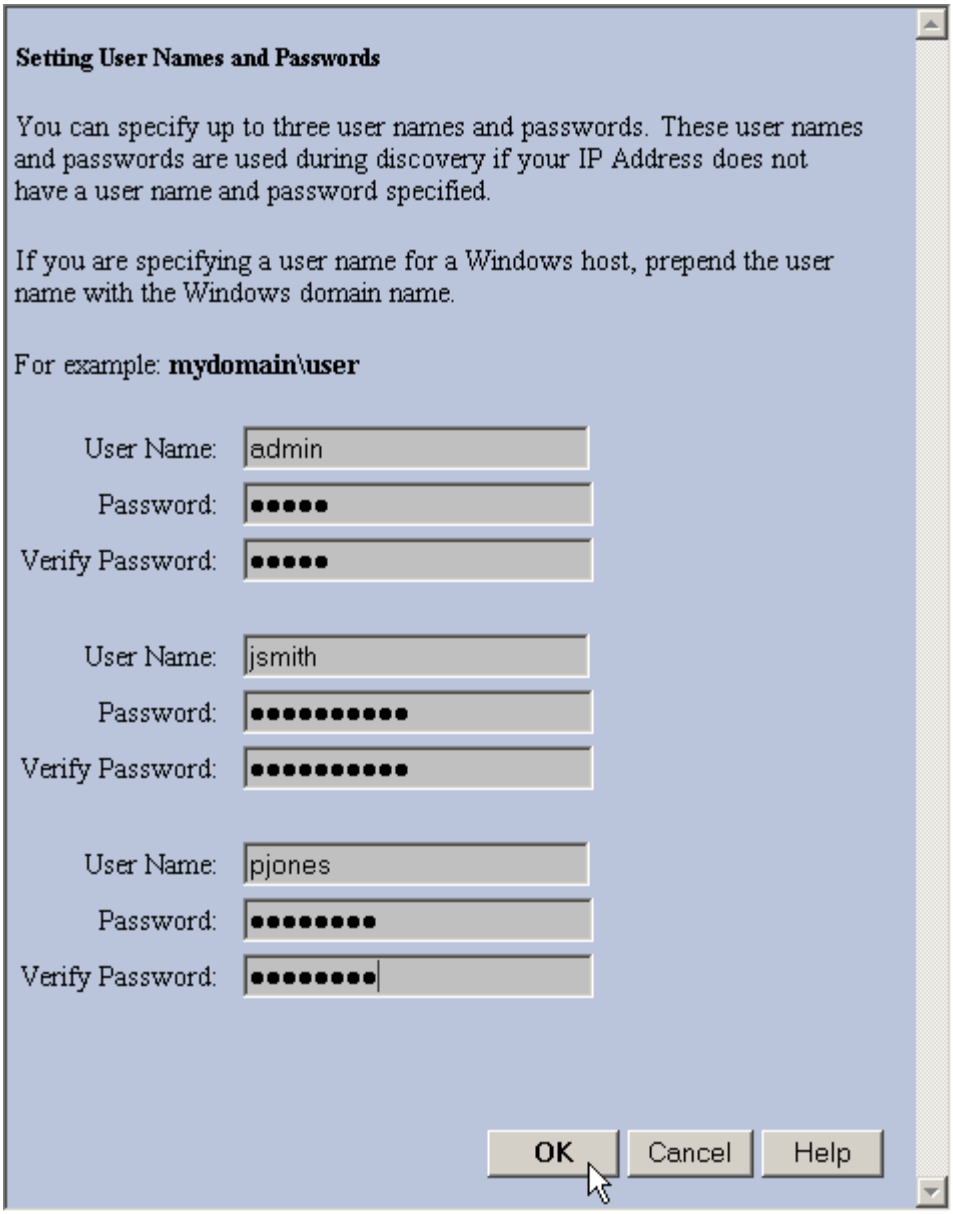


Figure 4-1: Setting Default User Names and Passwords

Adding an IP Range for Scanning

Instead of adding each IP address individually for scanning, the management server can detect a range of IP addresses, automatically populating the list of elements to be discovered.

Keep in mind the following:

- Include in the scanning, the proxy server that has a direct connection or a SAN connection to the management server, such as the EMC Solutions Enabler. Make sure the proxy service has started. On a computer running Microsoft Windows, this can be determined by looking in the **Services** window.
- You cannot scan an IP range to discover an instance of HiCommand Device Manager that listens on a port other than 2001. The management server does not allow port numbers in the scanning of IP ranges, and thus, you are not able to specify the port. See “Discovering HDS Storage Systems” on page 115 for more information.
- Enter a range within the same subnet. The management server cannot scan IP ranges across subnets.

To add an IP address range to scan:

1. Click **Discovery**, then click **Setup** in the upper-right pane of the window.
2. Click the **IP Ranges** tab.
   The IP ranges already added are listed.
3. Click the **Add Range** button.
4. In the **From IP Address** field, type a lowest IP address in the range to be scanned.
5. In the **To IP Address** field, type the highest IP address in the range to be scanned.
6. In the **User Name (Optional)** field, type a common user name for elements in the IP range.
7. In the **Password (Optional)** field, type a common password for elements in the IP range.
8. In the **Verify Password** field, retype the password.
9. In the **Comment** field, type a brief description of the servers. For example, “Servers in Marketing.”
10. Click **OK**.

Figure 4-2: Adding an IP Range for Scanning

11. Click the **Start Scanning** button on the **IP Ranges** tab.
    The management server scans the IP range and populates the **Addresses to Discover** table on the **IP Addresses** tab.

Adding a Single IP Address or DNS Name for Discovery

Keep in mind the following for discovering Engenio storage systems:

- Discover both controllers for the Engenio storage system. Each controller has its own IP address. In Step 1 of discovery, specify all the IP addresses for all the controllers (usually two). The management server discovers these controllers as one single storage system.

- The following steps provide general information on how to discover an element. See Table 4-2, “Discovery Requirements for Switches,” on page 79, Table 4-7, “Discovery Requirements for Storage Systems, Tape Libraries & NAS Devices,” on page 107, and Table 16-1, “Making the Management Server Aware of Hosts,” on page 287.
- To obtain drive-related statistics, install a proxy host. Ensure the proxy host has at least one LUN rendered by each controller of the array. See “Obtaining Disk Drive Statistics from Engenio Storage Systems” on page 318 for more information.
- The **Do Not Authenticate** option is for Engenio storage systems. The Engenio storage systems do not require a password for Get Details. If you want do not want to use the management server for provisioning on Engenio storage systems, you can leave the password field blank and select the **Do Not Authenticate** option. The management server will still monitor the Engenio storage system; however, you will not be able to do provisioning tasks.

To add a single IP address or DNS name to discover:

1. Click **Discovery**, then click **Setup** in the upper-right pane of the window.
2. Under Discovery Setup, select **Step 1** at the top of the screen.
3. On the **IP Addresses** tab, click the **Add Address** button.
4. In the **IP Address/DNS Name** field, type the IP address or DNS name of the device you want to discover.
5. In the **User Name (Optional)** field, type the user name. If you are discovering an Engenio storage system, leave this field blank.
   This field can also be left blank if the element's user name and password are one of the default user names and passwords.
6. Do one of the following for the password:
   - If you do not want to do provisioning on a storage system, leave the **Password** field blank. For Engenio storage systems, you must also select the **Do Not Authenticate** option.
   - If you want to do provisioning on a storage system, type the corresponding password for controller or proxy and make sure the **Do Not Authenticate** option is not selected.
   - For all other elements other than storage systems, provide the password if it is necessary for authentication. If the element does not require a password, leave the **Password** field blank.
7. If you typed a password in the previous step, retype the password in the **Verify Password** field.
8. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).

9. Click **OK**.
10. To start discovering elements on the network, click the **Start Discovery** button on the **IP Addresses** tab.

Modifying a Single IP Address Entry for Discovery

You can change the user name and password the software uses to access an element. Whenever a user name and/or password has changed on an element the management server monitors, the management server must be made aware of the change. For example, assume the password for a host was changed. You would need to updated the management server database with the new password.

Important: These steps only change the user name and password stored in the database. It does not change the device's user name and password.

To modify a user name or password for discovery:

1. Click **Discovery**, then click **Setup** in the upper-right pane of the window.
2. Click the  button for the element you want to modify the user name and/or password.
3. To change the user name, type the new user name in the **User Name** field.
4. To add or change a comment, type a comment in the **Comment** field.
5. To change the password:
   a. Click the **Change password** button.
   b. Type the new password in the **New Password** field.
   c. Type the password again in the **Verify Password** field.
   d. Click **OK** in the Change Password page.
6. Click **OK** in the Edit Address for Discovery page.
7. Select the option, **Step 2 - Topology: Select the discovered elements and build the topology view**.
8. Select the element for which you changed the user name and/or password.
9. Click the **Get Topology** button.
   The software updates its database with the new user name and/or password.

Removing Elements from the Addresses to Discover List

When you remove IP addresses and/or ranges from the Addresses to Discover list, the elements associated with those IP addresses are not removed from the management server. Only the information that was used to discover them is removed.

To remove items from the Discovery list:

1. Click the **Discovery** icon in the upper-right pane of the home page.
2. Click **Setup**.
3. Select **Step 1** at the top of the page.
4. Do one of the following:
   - Select the IP addresses and/or IP ranges you want to remove from the list. Then, click the **Delete** button.
   - Click the  button corresponding to the elements you want to remove from the Addresses to Discover list.

Important: The elements associated with these addresses are not removed from the management server. See “Deleting Elements from the Product” on page 135 for information about how to remove an element from the management server.

Importing Discovery Settings from a File

If you have a previous discovery list you can import it, rather than re-entering the information.

The import discovery settings feature lets you import the following information to the **Discovery** list:

- IP addresses to discover
- Default user names and passwords, which are encrypted
- Discovery information for applications

To prevent re-entering the information for each management server instance, you can import the same file for multiple management server instances.

Important: When you import a file, your previous settings are overwritten.

If you are shown an error message when you try to import the discovery settings, verify you are using the right password. If you are using the correct password, there could be a possibility that the file is corrupt.

To import discovery settings from a file:

1. Click **Discovery**, then click **Setup** in the upper-right pane of the window.
2. Click the **Import Settings from File** link.
3. In the **Import Settings from File** window, do one of the following:
   - Click the **Browse** button to find the file.
   - In the **Filename** field, type a complete path to the file.
4. In the **Password** field, type the password for the management server.
5. Click **OK**. The information on the following tabs is updated:
   - IP Addresses
   - IP Ranges
   - Applications
   - Windows Proxy tab

Saving Discovery Settings to a File

After you have discovered your elements, save the discovery settings of the elements in your discovery list.

The **Save Settings to File** link on the **Discovery Targets** tab lets you save the following:

- IP addresses to discover
- Default user names and passwords, which are encrypted
- Oracle TNS Listener ports
- Microsoft Exchange configuration

To prevent re-entering the information for each instance of the management server, you can import the file for multiple instances.

To save the discovery settings to a file:

1. Click**Discovery**, then click **Setup** in the upper-right pane of the window.
2. Click **Setup** in the upper-right corner.
3. Click the **Save Settings to File** link.
4. In the **Password** field, type the password for the management server.
5. In the **Verify Password** field, type the password from the previous step. Then, click **OK**.
6. When you are asked if you want to open or save the file, do one of the following:
   - **Microsoft Internet Explorer** - Click the **Save** button.
   - **Netscape 7** - Select the **Save this file to disk** option.

   The Downloading window appears.
7. Type a name for the *.xml file and select the directory to which you want to save the file. The name of the file is `DiscoverySettings.xml` by default.

   Important: Netscape 7 assumes the file is an HTML file. If you are running Netscape, make sure the file type is selected to **All Files** and the file extension is xml. You can make Netscape 7 recognize the xml file next time, by clicking the **Advanced** button See the topic, “Assigning a File Extension in Netscape 7” on page 146 for more information.
8. Leave the **Password** field blank, a password is not required. If you enter a password, that password is required later when you import the file. Leaving the password field blank allows the file to be imported without a password.
9. Click the **Save** button in the Save As window. The file is saved.

Step 1 - Discover Switches

This section describes the following:

- “SMI-S Switches Must Be Removed and Rediscovered After Upgrading” on page 81
- “Discovering Brocade Switches” on page 81
- “Discovering CNT Switches” on page 86
- “Discovering Cisco Switches” on page 87

- "Discovering Sun StorEdge and QLogic Switches" on page 89
- "Changing the SNMP Trap Listener Port for Sun StorEdge Switches" on page 90
- "Discovering McDATA and EMC Connectrix Switches" on page 91
- "Excluding McDATA and EMC Connectrix Switches from Discovery" on page 102

The following table provides an overview of the discovery requirements for switches.

Table 4-2: Discovery Requirements for Switches

Element	Discovery Requirements	Additional Information
Brocade switches (Fabric Access API)	Enter the IP address/DNS name, user name and password of the Brocade switch to discover it. The user name (default admin) and password must be for the Admin Account.	See "Discovering Brocade Switches" on page 81.
Brocade switches (SMI-S*)	Enter the IP address/DNS name, user name and password of the Brocade SMI-S proxy server to discover it. The user name (default admin) and password must be for the Admin Account. Note that some SMI-S providers require you to specify the server using its IP address: `http://IPADDRESS`.	See "Discovering Brocade Switches" on page 81.
CNT switches	Enter the IP address and the port number for the InVsn Software that manages the switch as well as the user name and password.	See "Discovering CNT Switches" on page 86.
Cisco switches (SMI-S)*	Enter the IP address/DNS name of the Cisco switch as well as the user name and password of the switch. All SMI-S switches require a user name and password.	See "Discovering Cisco Switches" on page 87.

Table 4-2: Discovery Requirements for Switches (Continued)

Element	Discovery Requirements	Additional Information
Cisco switches (SNMP)	Enter the IP address/DNS name of the Cisco switch. Enter the SNMP read-only community string as the user name. You do not need to enter a password.	See "Discovering Cisco Switches" on page 87.
QLogic switches (SMI-S)*	Enter the IP address/DNS name of the QLogic SMI-S switch as well as the user name and password of the switch. All SMI-S switches require a user name and password.	See "Discovering Sun StorEdge and QLogic Switches" on page 89.
Sun StorEdge and QLogic switches (SNMP)	Enter the IP address/DNS name of the Sun StorEdge or QLogic switch. Enter the SNMP read-only community string as the user name. You do not need to enter a password.	See "Discovering Sun StorEdge and QLogic Switches" on page 89.
McDATA and EMC Connectrix switches	Additional steps are required for discovering these switches, and the steps vary according to your network configuration.	See "Discovering McDATA and EMC Connectrix Switches" on page 91.

* SMI-S switches must be removed and rediscovered after upgrading from builds earlier than 4.2. See "SMI-S Switches Must Be Removed and Rediscovered After Upgrading" on page 81 for important information. See "Important Information About Upgrading and Brocade Switches" on page 61 for specific details related to Brocade switches.

Important: Make sure pop-up blocking software is disabled. If your Web browser has an option for blocking pop-ups, disable it. The management server uses pop-ups for dialog boxes.

SMI-S Switches Must Be Removed and Rediscovered After Upgrading

You must remove and rediscover Brocade, Cisco, QLogic, or CNT switches supported through SMI-S after you upgrade the management server.

1. Remove the Brocade, Cisco, QLogic, or CNT switches supported through SMI-S . See “Deleting Elements from the Product” on page 135.
2. Rediscover the Brocade, Cisco, QLogic, or CNT switches. See “Step 1 - Discover Switches” on page 78.
3. Perform Get Details. See “Step 4 - Get Details” on page 137.

Discovering Brocade Switches

If you are upgrading to build 5.1 from any build prior to 4.2 of the management server your Brocade switches are discovered using the Brocade Fabric Access API after the upgrade. See “Important Information About Upgrading and Brocade Switches” on page 61 for upgrade details. If this is a new installation of the management server software, your Brocade switches are discovered using the Brocade SMI-S (Storage Management Initiative Specification) provider and you must download and install the Brocade SMI-S provider software from the following FTP site: ftp://ftp.compaq.com/pub/products/storageworks/smisproviders/brocade_provider.pdf.

Table 4-3: Brocade Discovery Methods

Management Server Installation Status:	Default Brocade Discovery Method:
New installation of Build 5.1	SMI-S (You must download the Brocade SMI-S provider from the following site: ftp://ftp.compaq.com/pub/products/storageworks/smisproviders/brocade_provider.pdf.)
Upgrade from Build 4.2	Fabric Access API (The Brocade Fabric Access API provider installed with build 4.2 of the management server is used.)

Important: When using the Brocade Fabric Access API, Brocade recommends that the switch with the most recent version of Brocade API firmware (newer than v.2.6.x) is configured as the proxy switch.

When discovering Brocade SMI-S hosts the IP address of the Brocade SMI-S proxy server must be entered for Discovery Step 1. Be sure to see the Support Matrix for the latest details on firmware requirements.

Brocade SMI-S Provider Installation Requirements (New Installations of the Management Server)

If this is a new installation of the management server, the management server is configured to discover Brocade switches through SMI-S, by default, as noted earlier. You must first download and install the Brocade SMI-S provider software from the following site:

```
ftp://ftp.compaq.com/pub/products/storageworks/smisproviders/
brocade_provider.pdf
```

Be sure to check this FTP site periodically to be sure you are running a current version of the Brocade SMI-S provider. See the Support Matrix for details.

Keep in mind the following for Brocade SMI-S switches:

- You must verify that the Rapid program on the switch is set to 1. Rapid must be set to 1 so that the management server or any Brocade SMI-S agent can communicate with the switch. Be sure to see “Verifying Brocade Rapid Program Is Set to 1” on page 83 for more information. Note that this requirement also applies to Brocade switches that are configured to use the Fabric Access API provider.
- Before performing any provisioning operations that involve a Brocade switch after an upgrade to build 4.2 or 5.1 from any build prior to 4.2, you must perform Discovery Data Collection/Get Details for any subset of elements that includes this Brocade switch. See “Step 4 - Get Details” on page 137 for details on running Discovery Data Collection/Get Details.

Verifying Brocade Rapid Program Is Set to 1

If you are discovering Brocade switches or Brocade SMI-S agents, verify that the Rapid program on the switch is set to 1.

1. (Optional) Set the command prompt window so that it displays many rows.
   While completing the following steps, the command prompt window displays a large amount of data. You might want to expand the size and buffer of the command prompt window. To do this in Microsoft Windows 2000, click the upper-right corner of the command prompt window, click the **Layout** tab, and then modify the options under Screen Buffer Size and Window Size.
2. Access the Brocade switch or SMI-S agent by using the telnet option. For example,
   `telnet`
   `open 10.1.213.228`
   where `10.1.213.228` is the IP address of the switch.
3. When prompted for the user name and password, supply them.
4. Type the following to see what is supported on the switch or Brocade SMI-S agent:
   `configshow`
   The output is displayed in a page-by-page format.
5. Select all of the output.
6. Paste the output in a text editor, for example Notepad. Use the Find command to search for `rpc.rapid`.
7. Verify Rapid is set to one, as displayed below:
   `rpc.rapid:  1`

About Brocade Discovery (Specifying Brocade Discovery Using Fabric Access API or SMI-S)

For new installations, SMI-S is the default Brocade discovery protocol with this release of the management server as noted earlier. For existing installations, Fabric Access API is the default Brocade discovery protocol with this release of the management server. You can change from SMI-S to Fabric Access API by following the steps below:

To change the Brocade discovery settings to Fabric Access API on the management server:

1. Click **Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree.

2. In the **Custom Properties** field type `cimom.brocade.useApi=true` to use Fabric Access API (or you can type: `cimom.brocade.useApi=false` to use SMI-S). If the cimom.brocade.useApi value is not specified the management server uses SMI-S.
3. When you are done, click **Save**.
4. Restart the service for the management server for your changes to take effect. While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements. See the help for your operating system platform for details on how to verify that the service is running.

Important: When using the Brocade API, Brocade recommends that the switch with the most recent version of Brocade API firmware (newer than v.2.6.x) is configured as the proxy switch.

When discovering Brocade SMI-S hosts the IP address of the Brocade SMI-S proxy server must be entered for Discovery Step 1. Be sure to see the Support Matrix for the latest details on firmware requirements.

To discover Brocade switches:

1. Click **Discovery**, then click **Setup** in the upper-right pane of the window.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click the **Add Address** button.
5. In the **IP Address/DNS Name** field, do one of the following depending on the provider:
   - **SMI-S**

     Type the IP address of the proxy server that is running the SMI-S agent. (Some proxy servers require the following format: `http://IPADDRESS`.)
   - **Fabric Access API**

     Type the IP address or DNS name of the Brocade switch you want to discover.
6. In the **User Name** field, do one of the following depending on the provider:
   - **SMI-S**

     Type the user name for the SMI-S proxy server.

     This field can be left blank if one or more of the following conditions are fulfilled:

- The element's user name and password are one of the default user names and passwords.
- The element does not require authentication.

□ **Fabric Access API**

This field can be left blank if one or more of the following conditions are fulfilled:

- The element's user name and password are one of the default user names and passwords.
- The element does not require authentication.

7. In the **Password** field, do one of the following:

□ **SMI-S**

Type the password for the SMI-S proxy server.

This field can be left blank if one or more of the following conditions exists:

- The proxy server's user name and password are one of the default user names and passwords.
- The proxy server does not require authentication.

□ **Fabric Access API**

Type the corresponding password for the switch.

This field can be left blank if one or more of the following conditions are fulfilled:

- The element's user name and password are one of the default user names and passwords.
- The element does not require authentication.

8. If you typed a password in the previous step, retype the password in the **Verify Password** field.
9. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. To start discovering elements on the network, click the **Start Discovery** button on the **IP Addresses** tab.

Discovering CNT Switches

The management server uses the CNT SMI-S provider to discover CNT switches. A provider is a small software program that is used by the management server to communicate with a device, such as a switch.

This provider communicates with CNT InVsn Enterprise Manager to obtain information about the switch. The provider requires a certain version of InVsn depending on the switch model. See the following table for more information.

Table 4-4: Required Switch Models and InVsn Versions for Discovery

Switch Model	InVsn Software Version
FC/9000	9.0 or later
UMD	9.5 or later

Important: The InVsn credentials are used by the SMI-S provider. Make sure the SMI-S provider is enabled as described in the steps in this section.

Keep in mind the following for CNT switches:

- SNMP is not supported for CNT switches. If you discovered CNT switches in builds earlier than 4.0, you will need to rediscover the CNT switches by using the steps in this section.
- CNT InVsn Enterprise Manager must be running for the management server to discover it.
- The management server does not support provisioning for CNT switches. Only the active zone set and its zone members are reported.
- No ports are reported for uninstalled blades or GBICs.

To discover CNT switches

1. Before you can discover a CNT switch, you must do the following in the CNT InVsn Enterprise Manager software:
   a. Open the file `ProductInfo.ini` in a text editor, such as Notepad. If the software was installed in the default directory, this file should be in the following directory: `\Program Files\CNT\inVSN_EM`
   b. Change the following entry in the file:

```
cimomenabled=TRUE
```

c. Save the file, then restart the InVsn software.

2. In the **IP Address/DNS Name** field, type the primary IP address of the host running the InVsn software you want to discover followed by its namespace and port number, as shown in the following example:
`192.168.10.76//root/cntfabric:5989`
where
   - `192.168.10.76` is the IP address of the host running the InVsn software
   - `//root/cntfabric` is the namespace
   - `5989` is the port number
3. In the **User Name** field, type the user name for the login to the InVsn software.
4. In the **Password** field type the password for the login to the InVsn software.
5. In the **Verify Password** field type the password you provided previously.
6. Click **Start Discovery**.

Discovering Cisco Switches

The management server discovers Cisco switches through SNMP (Simple Network Management Protocol) and SMI-S (Storage Management Initiative Specification) connections—depending on the model of the Cisco switch. See the Support Matrix for details on supported switch models and firmware revisions.

Note: The Cisco MDS 9020 Multilayer Fabric Switch does not support VSANs.

Keep in mind the following for Cisco SNMP switches:

- When you discover a Cisco SNMP switch, you do not need to provide a password. .
- You can view zones, zone sets and zone aliases on a Cisco switch; however, you cannot use the management server to create, modify or remove them from a Cisco switch.
- The management server gathers information about the Cisco inactive database during Get Details . .
- The management server groups active zone sets in all Virtual SANs (VSANs) in a fabric into a zone set called “ACTIVE”, and the “ACTIVE” zone set is shown associated with the physical fabric. The members of the “ACTIVE” zone set (zones, zone sets, zone aliases)

have the name of the VSAN prefixed to their name. For example, an active zone named “ZONE1” from a VSAN named “VSAN1” is displayed as a zone on the physical fabric with name “VSAN1:CISCO1:ZONE1”.

Keep in mind the following for Cisco SMI-S switches:

- When you discover a Cisco SMI-S switch you need to provide a user name and password. All SMI-S switches require a user name and password.
- Cisco switches on the fabric are displayed without their names — each Cisco SMI-S switch name on the fabric is replaced with a generic name such as: Switch_1401 after running Get Details.

  To view the correct names for the Cisco SMI-S switches after running Get Details, manually enter the correct name for the Cisco SMI-S switches.

To discover a Cisco switch:

1. Click**Discovery**, then click **Setup** in the upper-right pane of the window.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click the **Add Address** button.
5. In the **IP Address/DNS Name** field, type the DNS name or primary IP address of the Cisco switch you want to discover.
6. Do one of the following:
   - For **Cisco** switches with **SNMP** connections:
     In the **User Name** field, type the user name for the switch. This is the public community SNMP string for the switch. This field can be left blank if the element's user name and password are one of the default user names and passwords.
   - For **Cisco** switches with **SMI-S** connections:
     In the **User Name** field, type the user name for this SMI-S switch.
7. Do one of the following:
   - For **Cisco** switches with **SNMP** connections:
     Leave the **Password** field blank.
   - For **Cisco** switches with **SMI-S** connections:
     In the **Password** field, type the password for this SMI-S switch.
8. Do one of the following:
   - For **Cisco** switches with **SNMP** connections:
     Leave the **Verify Password** field blank.
   - For **Cisco** switches with **SMI-S** connections:
     In the **Verify Password** field, type the password of the SMI-S switch again.

Discovering Sun StorEdge and QLogic Switches

The management server discovers Sun StorEdge switches through an SNMP connection and QLogic switches—depending on the model—are discovered through SNMP or SMI-S. See the Support Matrix for details on supported switch models and firmware revisions.

Keep in mind the following for Sun StorEdge and QLogic SNMP switches:

- When you discover a Sun StorEdge or QLogic SNMP switch, you do not need to provide a password.
- The management server does not support provisioning for Sun StorEdge and QLogic switches. Only the active zone set and its zone members are reported.
- To manage a fabric of Sun StorEdge and/or QLogic switches, every switch in the fabric must be included in the discovery list. If a switch is not included in the discovery list, it may show up as a generic host system.
- No ports are reported for uninstalled blades or GBICs.
- The default SNMP trap listener port for all Sun StorEdge switches is 162. To change this port, see “Changing the SNMP Trap Listener Port for Sun StorEdge Switches” on page 90.
- To receive events from Sun StorEdge switches, verify the SNMP trap community string is set to public in SANbox Manager or via telnet. Also, make sure the SNMP traps are configured to be sent to the management server.

Keep in mind the following for QLogic SMI-S switches:

- A user name and password are required to discover any SMI-S switch.
- You must perform Get Details to obtain all available information from QLogic SMI-S switches—otherwise, attributes such as vendor, fabric, and port information will be missing for the QLogic SMI-S switches.

To discover Sun StorEdge or QLogic switches:

1. Click **Discovery** > **Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click the **Add Address** button.
5. In the **IP Address/DNS Name** field, type the DNS name or primary IP address of the Sun StorEdge or QLogic switch you want to discover.
6. Do one of the following:
   - For **Sun StorEdge** and **QLogic** switches with **SNMP** connections:
     In the **User Name** field, type the user name for the switch. This is the public

community SNMP string for the switch. This field can be left blank if the element's user name and password are one of the default user names and passwords.

- For **QLogic** switches with **SMI-S** connections:
  In the **User Name** field, type the user name for this switch. All SMI-S switches require a user name and password.

7. Do one of the following:
   - For **Sun StorEdge and QLogic** switches with **SNMP** connections:
     Leave the **Password** field blank.
   - For **QLogic** switches with **SMI-S** connections:
     In the **Password** field, type the password for this switch.
8. Do one of the following:
   - For **Sun StorEdge and QLogic** switches with **SNMP** connections:
     Leave the **Verify Password** field blank.
   - For **QLogic** switches with **SMI-S** connections:
     In the **Verify Password** field, type the password of the switch again.

Changing the SNMP Trap Listener Port for Sun StorEdge Switches

The default SNMP trap listener port for all Sun StorEdge switches is 162. To change this port for all switches that are discovered through SNMP, modify the `cimom.snmpTrapListenerPort` property as described in the following steps:

1. Select **Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the `cimom.snmpTrapListenerPort` property. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.
4. Return to the Advanced page (**Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree).
5. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
6. Make your changes in the **Custom Properties** field. Make sure the property is not commented out by removing the hash (#) symbol in front of the property.
7. Set the `cimom.snmpTrapListenerPort` property to the port you want, as shown in the following example:

```
cimom.snmpTrapListenerPort=162
```

8. When you are done, click **Save**.
9. Restart the service for the management server for your changes to take effect.
   While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

Discovering McDATA and EMC Connectrix Switches

McDATA and EMC Connectrix switches use the Fibre Channel Switch Application Programming Interface (SWAPI) to communicate with devices on the network. The management server can discover multiple instances of Enterprise Fabric Connectivity Manager.

Use one of the following techniques to discover McDATA and Connectrix switches:

Table 4-5: Discovery Settings for McDATA and Connectrix Switches

Discovery	SWAPI setting through a Proxy	SNMP setting Through a Proxy	Contacting the switch directly
Description	Use this option if you have Enterprise Fabric Connectivity (EFC) Manager. You will need to connect through the proxy instead of the switch. See "SWAPI Setting Through a Proxy" on page 93 for more information.	Contact the switch through a proxy. You can use this option with EMC Connectrix™ Manager and Enterprise Fabric Connectivity (EFC) Manager to contact the switch. See "SNMP Setting Through a Proxy" on page 97 for more information.	Contact the switch by its IP address or DNS name. This connection uses SNMP or SMI-S depending on the McDATA switch model. See the Support Matrix for details on McDATA switch models (**Help** > **Documentation Center** > **Support Matrix**). See "Contacting a McDATA or Connectrix Switch Directly" on page 99.
Provisioning Limitations	The SWAPI setting lets you activate a zone set, in addition to creating, editing, and deleting zones and zone sets. You cannot manage or view information about zone aliases.	This SNMP setting through a proxy does not let you manage or access information about zones, zone sets or zone aliases.	This SNMP setting provides view only access to the active zone set and its members. You cannot create, modify, and/or delete zone sets or its members. SMI-S provides active management of zones.

Keep in mind the following:

- If you change a discovery configuration from SNMP to SWAPI or vice versa, the user ID and password will no longer work. For this reason, it is recommended that you set this property before discovering any McDATA switches. If you must change the configuration, see "Changing the Discovery Settings" on page 101.
- After you discover a McDATA or Connectrix switch through a proxy, the IP address displayed next to the name of the switch is actually the IP address of the proxy for the switch in the Discovery, Topology, and Get Details screens. To find the IP address of the switch, click the link for the switch in theTopology screen (**Discovery** > **Topology**) or Get

Details screen (**Discovery** > **Details**) and then click the **Properties** tab. The **Properties** tab can also be accessed by double clicking the switch in System Explorer.

- If you want to add, remove, or replace McDATA or Connectrix switches after you have discovered the service processor, you must perform additional steps, see “About Managing McDATA and EMC Connectrix Switches” on page 144.
- If you have problems obtaining information from McDATA or Connectrix switches during discovery and/or Get Details, see “Step 2 - Discover Storage Systems, NAS Devices and Tape Libraries” on page 106.
- All McDATA switches in a fabric must be managed by the same EFC Manager. Do not have more than one EFC Manager to a fabric for McDATA switches. If you do use more than one EFC Manager in a fabric, you must use the same EFC Manager for your zoning. Do not use the other EFC Managers for zoning, as this will create zoning database problems.
- All Connectrix switches in a fabric must be managed by the same Connectrix Manager. Do not have more than one Connectrix Manager to a fabric for Connectrix switches. If you do use more than one Connectrix Manager in a fabric, you must use the same Connectrix Manager for your zoning. Do not use the other Connectrix Managers for zoning, as this will create zoning database problems.
- If you want the management server to receive SNMP events from Connectrix or McDATA switches, do one of the following:
  - If you discovered Connectrix Manager or EFC Manager, only enable SNMP trap forwarding to the management server on the Connectrix Manager or EFC Manager, not on the individual switches.Connectrix Manager or EFC Manager should be configured to forward SNMP traps to the IP address of the management server, and the community string should match the user ID you used to discover Connectrix Manager or EFC Manager.
  - If you discovered Connectrix or McDATA switches directly, enable SNMP trap forwarding on the switches, not on any other management software. The switches should be configured to forward SNMP traps to the IP address of the management server, and the community string should match the user ID you used to discover the Connectrix or McDATA switches.

SWAPI Setting Through a Proxy

With the SWAPI setting, the management server contacts a proxy to obtain information about the switches connected to it. Use Enterprise Fabric Connectivity (EFC) Manager for this option. If you do not have EFC Manager, see “SNMP Setting Through a Proxy” on page 97. EFC Manager versions 7.0, 1.3 and later can communicate with the management server and the switch. EFC Manager accesses the switch through a SWAPI connection. This configuration lets multiple

instances of the management server or other clients contact EFC Manager, which in turn provides information about the switch.

Important: EMC customers using the EMC Connectrix Manager (EMC's rebranded EFCM) cannot use the EMC Fibre Zone Bridge (EMC's rebranded Bridge Agent) to discover EMC switches using SWAPI. The McDATA SWAPI library is incompatible with EMC's Fibre Zone Bridge Agent.

If the Fibre Zone Bridge Agent is not installed or not needed, you can uninstall the Fibre Zone Bridge Agent and install McDATA's Bridge Agent. The McDATA Bridge Agent will work with EMC's Connectrix Manager, but it cannot co-exist with EMC's Fibre Zone Bridge Agent.

If you are running Connectrix Manager and you need to have the EMC Fibre Zone Bridge Agent running, you will not be able to discover EMC switches using SWAPI. You must discover them through the SNMP provider, either directly or through a proxy. See "SNMP Setting Through a Proxy" on page 97 for more information about using the SNMP provider to discover switches through a proxy. See "Contacting a McDATA or Connectrix Switch Directly" on page 99 for more information about discovering switches by their IP address.

Note: Neither McDATA nor EMC officially support running the EMC Connectrix Manager with the McDATA Bridge Agent. Although this configuration has been tested for discovering EMC switches using SWAPI, you should check with your EMC or McDATA representative to determine the implications of this configuration.

Step 1 - (McDATA Switches Only) Install the Bridge Agent

To communicate with EFC Manager, the management server requires the Bridge Agent. Refer to your McDATA representative for more information about the Bridge Agent.

Step 2 - Verify the Discovery Setting for McDATA and Connectrix Switches is Set to SWAPI

By default the discovery settings for McDATA and Connectrix switches is set to SWAPI. If you believe it has been changed to SNMP, you can perform the following steps to change it back to SWAPI.

1. Click **Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the following property. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.
   `cimom.useSnmpMcDataProvider=TRUE`
4. Return to the Advanced page (**Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree).
5. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
6. Uncomment the `cimom.useSnmpMcDataProvider` property by removing the number sign (#) in front of `cimom.useSnmpMcDataProvider`.
7. Change the cimom.useSnmpMcDataProvider property to false.
   `cimom.useSnmpMcDataProvider=FALSE`
8. When you are done, click **Save**.
9. Restart the service for the management server for your changes to take effect. While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

Step 3 - Discover the Proxy

To discover the proxy:

1. Click **Discovery**, then click **Setup** in the upper-right pane of the window.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click the **Add Address** button.
5. In the **IP Address/DNS Name** field, type the IP address or DNS name of the EFC Manager/Connectrix Manager you want to discover.

6. In the **User Name** field, type the user name for EFC Manager/Connectrix Manager.
   This field can be left blank if one or more of the following conditions are fulfilled:
   - The element's user name and password are one of the default user names and passwords.
   - The element does not require authentication.

   To access a Windows-based device, prepend the user name with the Windows domain name, as shown in the following example.

   ```
   domain_name\user_name
   ```

   where
   - `domain_name` is the domain name of the machine
   - `user_name` is the name of your network account
7. In the **Password** field, type the corresponding password for EFC Manager/Connectrix Manager.
   This field can be left blank if one or more of the following conditions are fulfilled:
   - The element's user name and password are one of the default user names and passwords.
   - The element does not require authentication.
8. If you typed a password in the previous step, retype the password in the **Verify Password** field.
9. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
10. Click **OK**.
11. To start discovering elements on the network, click the **Start Discovery** button on the **IP Addresses** tab.
    Discovery is complete when the software displays the DISCOVERY COMPLETED message in the Log Messages field.

CIM_ERR_FAILED When Trying to Activate a Zone Set Using McDATA SWAPI

When the user tries to activate a zone set using McDATA SWAPI, the operation may return CIM_ERR_FAILED with one of the following detailed messages:

```
Cannot activate zone set. SWAPI Handle is not valid for fabric
Cannot activate zone set. Active zone set information is out of date for
fabric
```

```
There is no active SWAPI connection for fabric
Fabric is not in the cache
```

These error messages indicate that the SWAPI connection to the EFCM managing the fabric is no longer valid, or the active zone information was changed on the fabric without using the management server. The management server does not activate a zone set under these conditions.

(Discovery from HP SE only) To fix this problem, use the **Test** button on the discovery screen to check the status of the SWAPI connection. If necessary, re-discover the EFCM to re-establish the SWAPI connection.

Once the connection is working, the provisioning operation should succeed. If it continues to fail because the active zone set information is out of date, do a Get Details for this element to update the zoning information.

SNMP Setting Through a Proxy

This SNMP setting through a proxy does not let you manage or access information about zones, zone sets or zone aliases.

This option is required if you want to discover McDATA or Connectrix switches through a proxy using the SNMP provider. You can use this option with EMC Connectrix™ Manager and Enterprise Fabric Connectivity (EFC) Manager to contact the switch.

Step 1 - Change the Discovery Setting for Switches to SNMP

To change the discovery settings to SNMP:

1. Click **Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the following command:
   `#cimom.useSnmpMcDataProvider=true`
4. Return to the Advanced page.
5. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
6. Uncomment the property by removing the hash (#) symbol in front of the property if needed:
   `cimom.useSnmpMcDataProvider=true`

7. When you are done, click **Save**.
8. Restart the service for the management server.
9. Verify the following on the proxy and the switches accessible from the proxy:
   - ☐ The SNMP agent is enabled.
   - ☐ The read-only community string is configured.

Step 2 - Discover the Proxy

To discover the proxy:

1. Click **Discovery**, then click **Setup** in the upper-right pane of the window.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click the **Add Address** button.
5. In the **IP Address/DNS Name** field, type the IP address or DNS name of the proxy you want to discover.
6. In the **User Name** field, type the user name, which is the read-only community string of the EFC Manager or Connectrix Manager. The default community-string is "public" but this can be changed on the EFC Manager or Connectrix Manager.
7. Leave the **Password (Optional)** field blank. The password does not matter since the management server is not doing any configurations through SNMP.
8. You can leave the **Verify Password** field blank.
9. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. To start discovering elements on the network, click the **Start Discovery** button on the **IP Addresses** tab.
    Discovery is complete when the software displays the DISCOVERY COMPLETED message in the Log Messages field.

Important: To obtain more information about the switch, you need to map the topology and obtain element details. See the topics, “Building the Topology View” on page 132 and “Get Details” on page 137.

Step 3 - Make Sure There Are No Port Conflicts for Receiving SNMP Traps

When the management server is configured to contact the proxy by SNMP, the management server receives events from the proxy in the form of SNMP traps. By default, the management server uses port 162 to receive SNMP traps. If another software package is using that port, the management server is unable to receive the traps. To change the port the management server uses:

1. Select **Product Health**. Then, click **Advanced** in the **Disk Space** tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the following command:
   `cimom.snmpTrapListenerPort`
4. Return to the Advanced page.
5. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
6. Set the `cimom.snmpTrapListenerPort` to another port, as shown in the following example:
   `cimom.snmpTrapListenerPort=1234`
   where 1234 is the new port
7. When you are done making your changes, click **Save**.
8. Restart the service for the management server for your changes to take effect.
   While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

Step 4 - Set Up the Proxy to Send Traps to the Correct Port

When you are using the SNMP setting to discover a proxy, you must configure the SNMP agent on the proxy manager to send traps to the management server using the port you selected. This configuration sends traps from all switches managed by that proxy. Refer to your documentation for your proxy for more information.

Contacting a McDATA or Connectrix Switch Directly

The management server uses SWAPI to discover a McDATA or Connectrix switch by its IP address or DNS name. SWAPI is the default setting. If you want to discover McDATA or Connectrix switches by SNMP, you must change to SNMP before you begin the following steps. See “Changing the Discovery Settings” on page 101. If you are using a McDATA SMI-S compliant switch model, a direct connection to the switch is required and the switch must be contacted via its IP address. See the Support Matrix for McDATA switch details (**Help** > **Documentation Center** > **Support Matrix**).

To discover a McDATA or Connectrix switch directly:

1. Click **Discovery**, then click **Setup** in the upper-right pane of the window.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click the **Add Address** button.
5. In the **IP Address/DNS Name** field, type the IP address or DNS name of the switch you want to discover.
6. In the **User Name** field, type the user name for accessing the switch. If you are using SNMP the user name is the read-only community string of the switch. The default community-string is "public" but this can be changed on the switch. If you are using SMI-S the user name is the user name of the admin login of the switch.
7. If you are using SNMP leave the **Password (Optional)** field blank. The password does not matter since the management server is not doing any configurations through SNMP. If you are using SMI-S type the password of the admin account on the switch.
8. In the **Verify Password** field type the same thing you typed in the password field.
9. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. To start discovering elements on the network, click the **Start Discovery** button on the **IP Addresses** tab.
    Discovery is complete when the software displays the DISCOVERY COMPLETED message in the Log Messages field.

Important: To obtain more information about the switch, you need to map the topology and obtain element details. See the topics “Building the Topology View” on page 132 and “Get Details” on page 137.

Make Sure There Are No Port Conflicts for Receiving SNMP Traps

When the management server is configured to contact a switch by SNMP, the management server receives events from the switch in the form of SNMP traps. By default, the management server uses port 162 to receive SNMP traps. If another software package is using that port, the management server is unable to receive the traps. To change the port the management server uses:

1. Select **Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the following command:
   `cimom.snmpTrapListenerPort`
4. Return to the Advanced page.
5. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
6. Set the `cimom.snmpTrapListenerPort` to another port, as shown in the following example:
   `cimom.snmpTrapListenerPort=1234`
   where 1234 is the new port
7. When you are done making your changes, click **Save**.
8. Restart the service for the management server for your changes to take effect. While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

Step 4 - Set Up the Proxy to Send Traps to the Correct Port

When you are using the SNMP setting to discover a proxy, you must configure the SNMP agent on the proxy manager to send traps to the management server using the port you selected. This configuration sends traps from all switches managed by that proxy. Refer to your documentation for your proxy for more information.

Changing the Discovery Settings

To change the discovery settings from SWAPI to SNMP or vice versa:

1. Delete all McDATA and Connectrix switches in the application by going to the Get Topology for Discovered Elements table (**Discovery** > **Topology**) and selecting the switches you want to delete. Then, click the **Delete** button.
2. Delete all McDATA and Connectrix switches listed in the Addresses To Discover table (**Discovery** > **Setup**) by selecting the switches you want to delete and clicking the Delete button.
3. Click **Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree.
4. Click **Show Default Properties** at the bottom of the page.
5. Change the `cimom.useSnmpMcDataProvider` property as follows:
   - **SNMP setting** - Uncomment `cimom.useSnmpMcDataProvider` property by removing the number sign (#) in front of the `cimom.useSnmpMcDataProvider` property as follows: `cimom.useSnmpMcDataProvider=true`
   - **SWAPI setting** - Comment out the cimom.useSnmpMcDataProvider property by placing a number sign (#) in front of the cimom.useSnmpMcDataProvider property.
6. Click **Save**.
7. Restart the service for the management server.
8. Add new elements in the Discovery screen (**Discovery** > **Setup** > **Add Address**) by using the appropriate IP address and user name
   - **SWAPI connection** - Enter the IP address, user name and password for the proxy.
   - **SNMP connection** - Enter the IP address of the proxy. The default user name is “public” (the read-only community string). The password does not matter since the management server is not doing any configurations through SNMP.
9. Verify the following on the proxy and the switches accessible from the proxy:
   - The SNMP agent is enabled.
   - The read-only community string is configured.
10. Run Discovery.
11. Run Get Details.

Excluding McDATA and EMC Connectrix Switches from Discovery

Specific McDATA and Connectrix switches can be excluded from discovery by using system properties.

To exclude one or more switches from discovery, you must modify the `cimom.mcdata.exclude` property. Set the property `cimom.mcdata.exclude` to a comma separated list of Worldwide Names of the McDATA and Connectrix switches you want excluded, as shown in the following example:

```
cimom.mcdata.exclude=1000080088A07024,1000080088A0D0B6
```

The management server excludes the switches with one of the following Worldwide Names: 1000080088A07024 and 1000080088A0D0B6

If the `cimom.mcdata.exclude` property is not modified, the management server discovers and obtains details from all McDATA and Connectrix switches.

Important: The IP addresses of excluded elements appear in the discovery lists (**Discovery** > **Setup**), topology (**Discovery** > **Topology**),or Get Details lists (**Discovery** > **Details**). The management server does not display additional information about excluded elements in the user interface. The management server, however, does mention in the logs (**Discovery** > **View Logs**) that a provider instance has been created for an excluded element. You can ignore this message that appears in the logs.

To modify the `cimom.mcdata.exclude` property:

1. Select **Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the `cimom.mcdata.exclude` property. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.
4. Return to the Advanced page (**Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree).

5. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
6. Make your changes in the **Custom Properties** field. Make sure the property is not commented out by removing the hash (#) symbol in front of the property.
7. Add the Worldwide Names corresponding to the switches you want to exclude from discovery. Separate additional Worldwide Names with a comma, as shown by the following example:
   `cimom.mcdata.exclude=1000080088A07024,1000080088A0D0B6`
   where 1000080088A07024 and 1000080088A0D0B6 are the Worldwide Names for McDATA and Connectrix switches.
8. When you are done, click **Save**.
   While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

Viewing Log Messages

Use the **View Logs** page to obtain the status of the following:

- Discovery
- Building the Topology

During these operations, the management server displays its status at regular intervals.

To view logs for these operations:

1. Click **Discovery** > **View Logs**.
2. To obtain the latest status, click the **Get Latest Messages** button.

If the software is unable to discover or obtain information about a device, the log messages might provide some information as to where the problem occurred.

For example, if a host was not discovered, the log messages might indicate the provider configuration for that device was never created. This could mean the software was given the wrong user name and/or password for that host. As a result, the software logged onto the host with a guest account, which does not have enough permissions to start WMI.

Important: Look at Event Manager for additional information. See “About Event Manager” on page 536 for more information.

Viewing the Status of System Tasks

The Task Dashboard allows you to view the status of the tasks running on the management server. The dashboard provides the name of each task, its latest status, and the time the status was last reported.

To view the status of system tasks:

1. Click **Discovery** > **System Tasks**.
2. To obtain the latest status, click the **Get the Latest Status** button.

The following task statuses are provided by the Task Dashboard:

Table 4-6: Task Status Descriptions

Status	Description
Not Found	This task can not be found on this server.
Completed	This task has been completed successfully.
Failed	This task failed with an error.
Aborted	This task has been aborted by the user or other automated actions.
In Progress	This task is in progress. CPU and disk activities are active on this server.
Queued	This task is scheduled to be executed in the future.
Rejected	This task has been rejected by this server.

Duplicate Logs for Brocade Switches in Same Fabric

If you discover more than one Brocade switch in the same fabric, the discovery log displays duplicate listings for the Brocade switches. Each Brocade switch is listed multiple times with the IP address of the other switches and its own.

For example, assume you are discovering Brocade switches QBrocade2 and QBrocade5 in the same fabric, two duplicate entries are displayed in the log. QBrocade2 is listed twice, once with its own IP address, the other time with the IP address of QBrocade5, as shown below.

```
[Nov 27, 2002 8:45:05 AM] Discovered Switch: QBrocade2 at 192.168.10.22

[Nov 27, 2002 8:45:09 AM] Discovered Switch: QBrocade5 at 192.168.10.22

[Nov 27, 2002 8:45:09 AM] Enabling provider configuration:
APPIQ_BrocadeElementManagerConfig

[...]

[Nov 27, 2002 8:45:37 AM] Discovered Switch: QBrocade2 at 192.168.10.25

[Nov 27, 2002 8:45:42 AM] Discovered Switch: QBrocade5 at 192.168.10.25

[Nov 27, 2002 8:45:42 AM] Enabling provider configuration:
APPIQ_BrocadeElementManagerConfig
```

Note: On the **Topology** page, the software displays each Brocade switch (`192.168.10.22` and `192.168.10.25`) as elements:

```
192.168.10.22 Switch QBrocade2, QBrocade5 admin

192.168.10.25 Switch QBrocade2, QBrocade5 admin
```

Step 2 - Discover Storage Systems, NAS Devices and Tape Libraries

- “Discovering 3PAR Storage Systems” on page 109
- “Discovering EMC Solutions Enabler 5.1” on page 110
- “Excluding EMC Symmetrix Storage Systems from Discovery” on page 111
- “Discovering EMC CLARiiON Storage Systems” on page 113
- “Discovering Engenio Storage Systems” on page 113

- “Discovering HDS Storage Systems” on page 115
- “Excluding HDS Storage Systems from Discovery” on page 116
- “Discovering HP StorageWorks XP Arrays” on page 118
- “Discovering IBM Storage Systems” on page 121
- “Discovering Sun StorEdge 3510 Storage Systems” on page 123
- “Discovering Sun StorEdge 6920 and 6940 Storage Systems” on page 125
- “Discovering Sun StorEdge 6130 Storage Systems” on page 125
- “Discovering Xiotech Storage Systems” on page 126
- “Discovering HP NAS Devices on Windows” on page 127
- “Discovering HP NAS Devices on Linux” on page 128
- “Discovering NetApp NAS Devices” on page 129
- “Discovering Sun NAS Devices” on page 130
- “Discovering HP and IBM Tape Libraries” on page 131

Table 4-7: Discovery Requirements for Storage Systems, Tape Libraries & NAS Devices

Element	Discovery Requirements	Additional Information
3PAR storage systems	Discover the 3PAR storage system directly.	See “Discovering 3PAR Storage Systems” on page 109.
EMC CLARiiON storage systems	The EMC Navisphere CLI is required for the management server to communicate with the CLARiiON storage system.	See “Discovering EMC CLARiiON Storage Systems” on page 113 for more information.
EMC Symmetrix storage system (Including EMC Symmetrix DMX storage systems)	Discover the server running the EMC Solutions Enabler.	See “Discovering EMC Solutions Enabler 5.1” on page 110 for more information.

Table 4-7: Discovery Requirements for Storage Systems, Tape Libraries & NAS Devices

Element	Discovery Requirements	Additional Information
Engenio storage systems	Can be discovered two ways: ■ Entering the IP address/ DNS name, user name and password of a controller for an Engenio storage system. Discovers only the corresponding IP address of the controller. ■ Entering the IP address/ DNS name, user name and password of a proxy that is used to manage an Engenio storage system. Discovers all controllers known to the proxy.	See “Discovering Engenio Storage Systems” on page 113.
HDS storage systems	Discover the server running HiCommand Device Manager.	See “Discovering HDS Storage Systems” on page 115 for more information.
HP storage systems	Discover the server running the HP CIMOM.	See “Discovering HP StorageWorks XP Arrays” on page 118.
IBM Storage Systems	Discover the CIMOM that talks to the IBM storage systems you want to monitor.	See “Discovering IBM Storage Systems” on page 121.
Sun StorEdge 3510	Discovered through proxy software called Sun StorEdge™ Configuration Service. On the discovery page the user should enter the hostname or IP address of the computer running the Sun StorEdge 3510 SMI-S provider.	See “Discovering Sun StorEdge 3510 Storage Systems” on page 123.
Sun StorEdge 6920 and 6940	Discover the storage system directly.	See “Discovering Sun StorEdge 6920 and 6940 Storage Systems” on page 125.

Table 4-7: Discovery Requirements for Storage Systems, Tape Libraries & NAS Devices

Element	Discovery Requirements	Additional Information
Sun StorEdge 6130	Discover the storage system directly. The username does not matter. The password matters only for provisioning.	See “Discovering Sun StorEdge 6130 Storage Systems” on page 125.
Xiotech Storage Systems	Discover the storage system directly.	See “Discovering Xiotech Storage Systems” on page 126.
HP NAS Devices	Discover the device directly.	See “Discovering HP NAS Devices on Windows” on page 127 and “Discovering HP NAS Devices on Linux” on page 128.
NetApp Devices	Discover the device directly.	See “Discovering NetApp NAS Devices” on page 129.
Sun NAS Devices	Discover the server running the SMI-S provider for the Sun NAS Devices.	See “Discovering Sun NAS Devices” on page 130.
HP and IBM Tape Libraries	Provide the IP address, namespace, user name and password for the tape library.	See “Discovering HP and IBM Tape Libraries” on page 131

Discovering 3PAR Storage Systems

Note: You do not need to provide the interop namespace because the management server includes the interop namespace for 3PAR storage systems in its default list.

Important: To be able to discover a 3PAR storage system, the SMI-S server for the 3PAR storage system must be running. By default, the 3PAR SMI-S server is not started on the array. To start the SMI-S server, bring up the InForm CLI and run the following command:
startcim
This command starts the SMI-S server within a minute or so.

To discover a 3PAR storage system:

1. Click **Discovery** > **Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click the **Add Address** button.
5. In the **IP Address/DNS Name** field, the following for the 3PAR storage system you want to discover.
   `<host>`
   where `<host>` is the IP address or DNS name of the 3PAR storage system you want to discover.
6. Enter the **User Name** of the storage system.
7. Enter the **Password** of the storage system.
8. Retype the password in the **Verify Password** field.
9. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. To start discovering elements on the network, click the **Start Discovery** button on the IP Addresses tab.

Discovering EMC Solutions Enabler 5.1

EMC Solutions Enabler restricts access to itself through the nethost file. If present, the nethost file is located in the same directory as the netcnfg file. If you are using a nethost file, edit it to allow the management server to discover the Solutions Enabler and the Symmetrix storage systems that it manages.

Important: Use a nethost file unless you are running a version of the Solutions Enabler earlier than the 5.1 version. You must have the license installed for the Solutions Enabler. The nethost file provides access to the Solutions Enabler API.

Sometimes you can access an EMC Symmetrix storage system through several Solutions Enabler servers. In this case if you do not have access to a particular Solutions Enabler, you may still be able to access the Symmetrix storage system through another Solutions Enabler.

If you do not have a nethost file, you may need to create one. For example, assume you are running Solutions Enabler on a Solaris server, you would create a nethost file as described in the following steps. Refer to the documentation for Solutions Enabler for other operating systems.

1. Create a file called “nethost” in the `/opt/emc/API/symapi/config` directory.
2. Add the following lines to the nethost file:
   Management Server Running on Microsoft Windows

   ```
   [management server name] SYSTEM
   [management server IP] SYSTEM
   ```

   Management Server Running on Sun Solaris

   ```
   [management server name] root
   [management server IP] root
   ```

   where

   - `[management server name]` is the DNS name of the management server
   - `[management server name]` is the IP address of the management server
3. Add the following line to the /opt/emc/API/symapi/config/netcnfg file:
   `SYMAPI_SERVER - TCPIP <IP of SymAPI server> 2707`
4. Use the following command to start the daemon:
   `/opt/emc/SYMCLI/V5.5.0/bin/symapisrv -service SYMAPI_SERVER start -background`
5. Use the following command to stop the daemon:
   `/opt/emc/SYMCLI/V5.5.0/bin/symapisrv stop`
6. You may need to discover the Symmetrix arrays the SymAPI server can see by running the following command:
   `/opt/emc/SYMCLI/V5.5.0/bin/symcfg discover`

Important: If error 214 is present in the discovery log and/or cimom.log during discovery, this means the SymAPI server is not licensed for remote connections. The end-user will have to acquire and install the license before discovery can occur.

Required Licenses

If you want to use all of the features of the management server, such as provisioning, with an EMC Symmetrix storage system, you must have licenses for the following products:

- BASE
- DeltaMark
- SERVER
- DevMasking
- Config Manager
- Mapping (SOLUTION_4)

Excluding EMC Symmetrix Storage Systems from Discovery

When multiple EMC Symmetrix storage systems are managed through a single Solutions Enabler, specific storage systems may be excluded from discovery by using system properties.

To exclude one or more Symmetrix storage systems from discovery, you must modify the `cimom.symmetrix.exclude` property. Set the property `cimom.symmetrix.exclude` to a comma separated list of serial numbers of the storage systems you want excluded, as shown in the following example:

```
cimom.symmetrix.exclude=000183500570,000183610580
```

The management server excludes the storage systems with one of the following serial numbers: 000183500570 and 000183610580.

If the `cimom.symmetrix.exclude` property, the management server discovers and obtains details from all EMC Symmetrix Storage Systems managed by discovered Solutions Enablers.

Important: The IP addresses of excluded elements appear in the discovery (**Discovery** > **Setup**), topology (**Discovery** > **Topology**), Discovery Data Collection (**Discovery** > **Run Discovery Data Collection**), or Get Details lists (**Discovery** > **Details**). The management server does not display additional information about excluded elements in the user interface. The management server, however, does mention in the logs that a provider instance has been created for an excluded element. You can ignore this message that appears in the logs.

To modify the `cimom.symmetrix.exclude` property:

1. Select **Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the following command. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.
   `#cimom.symmetrix.exclude=000183500570,000183500575`
4. Return to the Advanced page.
5. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
6. Make sure the property is not commented out by removing the hash (#) symbol in front of the property. Add the serial numbers corresponding to the Symmetrix storage systems you want to exclude from discovery. Separate additional serial numbers with a comma, as shown by the following example:
   `cimom.symmetrix.exclude=000183500570,000183500575`
   where 000183500570 and 000183500575 are serial numbers for Symmetrix storage systems.
7. When you are done, click **Save**.
8. Restart the service for the management server for your changes to take effect. While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

Discovering EMC CLARiiON Storage Systems

The EMC Navisphere® CLI must be installed on the management server for the management server to communicate with the CLARiiON® storage system. At the time this documentation was created, EMC distributed the Navisphere CLI as part of the EMC Navisphere Software Suite. Contact your EMC representative for more information about obtaining the Navisphere CLI. Distribution rights for the Navisphere CLI belong to EMC. For Solaris, you must install the Navisphere Disk Array Management Tool CLI (NAVICLI).

Contact your EMC representative for more information about obtaining the Navisphere CLI. Distribution rights for the Navisphere CLI belong to EMC.

Important: Before you discover your CLARiiON storage systems, you must have already installed all required software components for your CLARiiON storage system, such as the Navisphere Host Agent. Refer to the documentation for your storage system for more information.

In Navisphere Manager add one of the following to the privilege user section:

```
SYSTEM@name_of_my_management_server
SYSTEM@IP_of_my_management_server
```

where

- `name_of_my_management_server` is the DNS name of the computer running the management server software
- `IP_of_my_management_server` is the IP address of the computer running the management server software

When you use the management server to discover the CLARiiON storage system, provide the IP address for the CLARiiON storage system and the user name and password used to log into Navisphere.

Discovering Engenio Storage Systems

Keep in mind the following when discovering an Engenio storage system:

- Discover all controllers on an Engenio storage system by entering the IP address of each controller.
- The management server must have the User Name field populated to discover the Engenio storage system. If your Engenio storage system does not have a user name set, you must enter something in the **User Name** field, even though the storage system has no user name.
- Discover both controllers for the Engenio storage system. Each controller has its own IP address. When you discover, specify all the IP addresses for all the controllers (usually two). The management server discovers these controllers as one single storage system.
- To obtain drive-related statistics, install a proxy host. Ensure the proxy host has at least one LUN rendered by each controller of the array. See the topic, “Obtaining Disk Drive Statistics from Engenio Storage Systems” on page 318 for more information.
- A license key is required for each storage system and that the key is obtained from the Web site specified on the Activation Card that shipped with your storage system.
- Engenio storage systems do not require a password for Get Details. If you want do not want to use the management server for provisioning on Engenio storage systems, select the **Do Not Authenticate** option. The management server will still monitor the Engenio storage system; however, you will not be able to do provisioning tasks.

Do the following to discover Engenio storage systems:

1. Click **Discovery** > **Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click the **Add Address** button.
5. In the **IP Address/DNS Name** field, type the IP address or DNS name of the controller or proxy you want to discover.
6. Enter the user name in the **User Name** field. If your Engenio storage system does not have a user name, you must enter something in the **User Name** field, even though the storage system has no user name.
7. Leave the **Password** field blank if you do not want to do provisioning on the Engenio storage system. If you want to do provisioning, type the corresponding password for controller or proxy.
8. If you typed a password in the previous step, retype the password in the **Verify Password** field.
9. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).

10. If you do not plan to use provisioning in the product, select the **Do Not Authenticate** option.
11. Click **OK**.
12. To start discovering elements on the network, click the **Start Discovery** button on the **IP Addresses** tab.

Discovering HDS Storage Systems

HiCommand Device Manager is required for the management server to communicate with an HDS storage system. To discover an HDS storage system, enter the IP address, user name and password for the server running HiCommand Device Manager. Do not point to the disk array for the storage system.

To obtain information about HDS storage systems, the management server must be able to access the port HiCommand Device Manager uses to listen. By default, HiCommand Device Manager listens on port 2001, and the management server assumes this configuration at discovery time. If HiCommand Device Manager uses a different port, specify this other port when you discover HiCommand Device Manager.

Keep in mind the following:

- You cannot scan an IP range to discover an instance of HiCommand Device Manager that listens on a port other than 2001. The management server does not allow port numbers in the scanning of IP ranges, and thus, you are not able to specify the port.
- The management server communicates with HiCommand Device Manager through a nonsecure connection. If you want the management server to communicate with HiCommand Device Manager through a secure sockets layer (SSL) connection, you must modify an internal property or use HTTPS when you discover HiCommand Device Manager. See “Communicating with HiCommand Device Manager Over SSL” on page 403.

To discover an HDS storage system that listens on a port other than 2001:

1. Access the Discovery Setup page (**Discovery** > **Setup**).
2. Click the **Add Address** button.
3. In the **IP Address/DNS Name** field, type the name of the server and the port HiCommand Device Manager uses to listen separated by a colon, as shown in the following example:
   `proxy2:1234`
   where

- `proxy2` is the name of the server running HiCommand Device Manager
- `1234` is the port HiCommand Device Manager uses to listen

4. In the **User Name** field, type the user name for accessing HiCommand Device Manager.
5. In the **Password** field, type the password for accessing HiCommand Device Manager.
6. In the **Verify Password** field, retype the password for accessing HiCommand Device Manager.
7. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
8. Do not select the **Do Not Authenticate** option.
9. Click **OK**.

Excluding HDS Storage Systems from Discovery

When multiple HDS storage systems are managed through a single HiCommand Device Manager, specific storage systems may be excluded from discovery by using system properties.

To exclude one or more HDS storage systems from discovery, you must modify the `cimom.hds.exclude` property. Set the property `cimom.hds.exclude` to a comma separated list of serial numbers of the storage systems you want excluded, as shown in the following example:

```
cimom.hds.exclude=61038,61037
```

The management server excludes the storage systems with one of the following serial numbers: 61038 and 61037.

If the `cimom.hds.exclude` property is not specified, the management server discovers and obtains details from all HDS storage systems managed by the discovered HiCommand Device Manager.

The IP addresses of excluded elements appear in the discovery (**Discovery** > **Setup**), topology (**Discovery** > **Topology**) or Get Details list (**Discovery** > **Details**). The management server does not display additional information about excluded elements in the user interface. The management server, however, does mention in the logs (**Discovery** > **View Logs**) that a provider instance has been created for an excluded element. You can ignore this message that appears in the logs.

To modify the `cimom.hds.exclude` property:

1. Select **Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree.

2. Click **Show Default Properties** at the bottom of the page.
3. Copy the following command. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.
   ```
   #cimom.hds.exclude=61038,61037
   ```
4. Return to the Advanced page.
5. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
6. Make sure the property is not commented out by removing the hash (#) symbol in front of the property. Add the serial numbers corresponding to the HDS storage systems you want to exclude form discovery. Separate additional serial numbers with a comma, as shown by the following example:
   ```
   cimom.hds.exclude=61038,61037
   ```
   where 61038 and 61037 are serial numbers for HDS storage systems.
7. When you are done, click **Save**.
8. Restart the service for the management server for your changes to take effect.
   While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

Discovering HP StorageWorks EVA or MSA Arrays

To discover HP StorageWorks EVA or MSA arrays, you must enter the following information for the instance of the HP CIMOM used to manage the storage system:

- user name and password used for accessing the HP CIMOM
- IP address of the server containing the HP CIMOM

The following should be installed on a server before you discover an HP EVA or MSA storage system:

- HP Storage Management Appliance software
- HP OpenView Storage Operations Manager
- HP StorageWorks Command View EVA or MSA
- HP StorageWorks SMI-S EVA or MSA.

To determine provisioning support for HP StorageWorks Arrays, see Table 5-3, “Provisioning and Pool Support,” on page 177 and Table 5-4, “Volume and HSG Support,” on page 178.

To discover HP EVA or MSA storage systems:

1. Click **Discovery** > **Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click the **Add Address** button.
5. In the **IP Address/DNS Name** field, type the IP address or DNS name of the HP CIMOM you want to discover.
6. Enter the **User Name** used to access the HP CIMOM.
7. Enter the **Password** used to access the HP CIMOM.
8. If you typed a password in the previous step, retype the password in the **Verify Password** field.
9. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. To start discovering elements on the network, click the **Start Discovery** button on the **IP Addresses** tab.

Discovering HP StorageWorks XP Arrays

You can discover HP StorageWorks XP Arrays by using the following:

- Command View XP
- Command View XP Advanced Edition
- XP Provider

To determine provisioning support for HP StorageWorks Arrays, see Table 5-3, “Provisioning and Pool Support,” on page 177 and Table 5-4, “Volume and HSG Support,” on page 178.

Discovering HP XP Arrays by Using Command View XP

To discover HP StorageWorks XP arraysby using Command View XP, you must enter the following information for the instance of the HP CIMOM used to manage the storage system:

- user name and password used for accessing the HP CIMOM
- IP address of the server containing the HP CIMOM

The following should be installed on a server before you discover an HP XP storage system if you are discovering the storage system by using Command View XP:

- HP Storage Management Appliance software
- HP OpenView Storage Operations Manager
- HP StorageWorks Command View XP

To discover HP storage systemsby using Command View XP:

1. Click **Discovery** > **Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click the **Add Address** button.
5. In the **IP Address/DNS Name** field, type the IP address or DNS name of the HP CIMOM you want to discover.
6. Enter the **User Name** used to access the HP CIMOM.
7. Enter the **Password** used to access the HP CIMOM.
   If you have Command View version 2.0 or later, the default password is administrator. If you have Command View earlier than version 2.0, refer to the documentation that shipped with Command View for the default password.
8. If you typed a password in the previous step, retype the password in the **Verify Password** field.
9. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. To start discovering elements on the network, click the **Start Discovery** button on the **IP Addresses** tab.

Discovering HP XP Arrays by Using Command View XP Advanced Edition

To discover HP StorageWorks XP arraysby using Command View XP Advanced Edition, you must enter the following information:

- user name and password used for accessing Command View XP Advanced Edition
- IP address of the server running Command View XP Advanced Edition

The following should be installed on a server before you discover an HP XP storage system if you are discovering the storage system by using Command View XP Advanced Edition:

- HP Storage Management Appliance software
- HP OpenView Storage Operations Manager
- HP StorageWorks Command View XP Advanced Edition

To discover HP storage systemsby using Command View XP Advanced Edition:

1. Click **Discovery** > **Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click the **Add Address** button.
5. In the **IP Address/DNS Name** field, type the IP address or DNS name of the server running Command View XP Advanced Edition.
6. Enter the **User Name** used to access Command View XP Advanced Edition.
7. Enter the **Password** used to access Command View XP Advanced Edition.
8. If you typed a password in the previous step, retype the password in the **Verify Password** field.
9. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. To start discovering elements on the network, click the **Start Discovery** button on the **IP Addresses** tab.

Discovering HP XP Arrays by using the XP Provider

To discover HP StorageWorks XP arrays by using XP provider, you must enter the following information for the XP array:

- user name and password used for accessing the XP array
- IP address of the XP array

To discover HP storage systems by using XP provider:

1. Click**Discovery** > **Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click the **Add Address** button.
5. In the **IP Address/DNS Name** field, type the IP address or DNS name of the XP storage system you want to discover.
6. Enter the **User Name** used to access the XP storage system.
7. Enter the **Password** used to access the XP storage system.
8. If you typed a password in the previous step, retype the password in the **Verify Password** field.
9. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. To start discovering elements on the network, click the **Start Discovery** button on the **IP Addresses** tab.

Discovering IBM Storage Systems

Before you can discover an IBM storage system, you must install the IBM CIM Agent. For Enterprise Storage Server (ESS) devices, the CIM Agent is called “CIM Agent for ESS”; for DS devices and mixed DS and ESS environments, use the “CIM Agent for DS Open (API)”. It is recommended not to install the IBM CIM Agent on the management server. Refer to the “CIM Agent for DS Open (API) - Installation and Configuration Guide” for details on configuring the CIM Agent. In short, this procedure entails:

a. **Installing the software.** The installation checks for the existence of the ESSCLI. If the ESSCLI is not installed, installation of the CIM Agent cannot proceed. The ESSCLI is typically preinstalled on the ESS management server that was configured by the IBM field technician.

b. **Configuring the protocol and ports used to communicate with the CIM Agent.** You can change the CIM Agent port value, protocol (HTTP/HTTPS), and enable or disable the debug option. Unless a secure connection is required between the management server and the CIM Agent, it is recommended to use port 5988 and protocol HTTP. You must change the default authentication method in order to discover the CIM Agent. Stop the IBM CIM Agent service. Then, edit the cimom.properties file in `C:\Program Files\IBM\cimagent` by default. Open the `cimom.properties` file and change the following property to false: `DigestAuthentication=False`

c. **Using the setuser command to configure a user to access the CIM Agent.** The user credentials specified here are used to access the CIM Agent and are specified in the Discovery Step 1. The credentials are not necessarily the same as those used to login to the ESS Specialist management utility or the DS Storage Manager.

d. **Using the setdevice command to configure the ESS and DS devices that are managed through the CIM Agent.** The setdevice command requires a valid user that has the necessary privileges to access and configure the ESS or DS storage systems.

e. **Restarting the IBM CIM Agent service**. Restart the IBM CIM Agent service for your changes to take effect.

f. **Verifying that the CIM Agent is able to communicate with the ESS devices.**

Note: You do not need to provide the interop namespace because the management server includes the interop namespace for IBM storage systems in its default list.

To discover an IBM storage system, you must discover its CIMOM, as described in the following steps:

1. Click **Discovery** > **Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click the **Add Address** button.
5. In the **IP Address/DNS Name** field, type the IP address or DNS name of the system running the IBM CIMOM you want to discover.
6. Enter the **User Name** of the system running the IBM CIMOM.

7. Enter the **Password** of the system running the IBM CIMOM.
8. Retype the password in the **Verify Password** field.
9. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. To start discovering elements on the network, click the **Start Discovery** button on the IP Addresses tab.

Discovering Sun StorEdge 3510 Storage Systems

Before you can discover a Sun StorEdge 3510 storage system, you must set up a Sun StorEdge 3510 SMI-S provider and a Sun StorEdge™ Configuration Service. The provider cannot be installed on the same computer as the management server due to a port conflict.

The Sun StorEdge™ Configuration Service can be installed in one of the following locations:

- on the same computer as the Sun StorEdge 3510 SMI-S provider
- on the management server
- on a separate computer

To install the Sun StorEdge™ Configuration Service you must install the following packages:

- Sun StorEdge™ Configuration Service Console (SUNWscsu)
- Sun StorEdge™ Configuration Service Agent (SUNWscsd)
- Sun StorEdge™ Diagnostic Reporter Agent (SUNWscsa)

You must also install the following packages. Contact Sun technical support for information on how to obtain and configure these packages.

- WBEM Solutions J WBEM Server 1.0
- Sun StorEdge™ CIM/WBEM Provider SDK (SUNWagsdk package) - A readme file is installed as part of SUNWagsdk package. Follow the instructions in that readme file.
- Sun StorEdge™ 3510 SMI-S Provider (SUNW3x10a package) - A readme file is installed as part of SUNW3x10a package. Follow the instructions in that readme file.

To discover Sun StorEdge 3510 storage systems, you must discover the Sun StorEdge 3510 SMI-S provider. To discover a Sun StorEdge 3510 storage system, you must enter the following information for the instance of the Sun StorEdge 3510 SMI-S provider.

- user name and password used for the system running Sun StorEdge 3510 SMI-S provider
- IP address of the system running Sun StorEdge 3510 SMI-S provider

---

Important: The management server is unable to display logical volumes configured on Sun StorEdge 3510 storage systems. Any logical volumes as well as the logical drives that comprise them will not appear in the UI. There will be no indication that this happened.

To discover Sun StorEdge 3510 storage systems:

1. Click **Discovery** > **Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click the **Add Address** button.
5. In the **IP Address/DNS Name** field, type the IP address or DNS name of the system running the Sun StorEdge 3510 SMI-S provider you want to discover.
6. Enter the **User Name** of the system running the Sun StorEdge 3510 SMI-S provider.
7. Enter the **Password** of the system running the Sun StorEdge 3510 SMI-S provider.
8. Retype the password in the **Verify Password** field.
9. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. To start discovering elements on the network, click the **Start Discovery** button on the IP Addresses tab.

Discovering Sun StorEdge 6920 and 6940 Storage Systems

To discover Sun StorEdge 6920 and 6940 storage systems:

1. Click **Discovery** > **Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click the **Add Address** button.
5. In the **IP Address/DNS Name** field, type the IP address or DNS name of the storage system you want to discover.
6. Enter the **User Name** of the storage system.
7. Enter the **Password** used to access the storage system.
8. Retype the password in the **Verify Password** field.
9. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. To start discovering elements on the network, click the **Start Discovery** button on the **IP Addresses** tab.

Discovering Sun StorEdge 6130 Storage Systems

To discover Sun StorEdge 6130 storage systems:

1. Click **Discovery** > **Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click the **Add Address** button.
5. In the **IP Address/DNS Name** field, type the IP address or DNS name of the controller or proxy you want to discover.
6. Leave the **User Name** field blank.

7. Leave the **Password** field blank if you do not want to do provisioning on the storage systems. If you want to do provisioning, type the corresponding password for controller or proxy.
8. If you typed a password in the previous step, retype the password in the **Verify Password** field.
9. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
10. If you do not plan to use provisioning in the product, select the **Do Not Authenticate** option.
11. Click **OK**.
12. To start discovering elements on the network, click the **Start Discovery** button on the **IP Addresses** tab.

Discovering Xiotech Storage Systems

Important: You must have Xiotech's Intelligent Control (ICON) software installed. If you do not have the software, contact your Xiotech representative.

To discover an Xiotech storage system:

1. Click **Discovery** > **Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click the **Add Address** button.
5. In the **IP Address/DNS Name** field, enter the IP address or DNS name for the storage system and its namespace. For example:
   `<IP address/DNS name>/root/cimv2`
   where
   - `<IP address/DNS name>` is the IP address or DNS name of the storage system.
   - `/root/cimv2` is its namespace.
6. You can leave the user name and password for the Xiotech storage system blank.

7. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
8. Do not select the **Do Not Authenticate** option.
9. Click **OK**.
10. To start discovering elements on the network, click the **Start Discovery** button on the IP Addresses tab.

Discovering HP NAS Devices on Windows

In order to discover an HP NAS device on Windows, you must first install a CIM extension on the device. Refer to the *Installation Guide* for information on how to install the CIM extension.

In order to enable NAS support, you must modify a property file on the NAS device. To enable NAS support:

1. Connect to the NAS device on which you have installed the CIM extension.
2. Browse to the installation directory and open the CIMextension/conf directory.
3. Copy the nas.properties-sample file and paste a copy into the same directory.
4. Rename the copied file to nas.properties.
5. Open the file and locate the following line:
   ```
   # Set to true to enable NAS data collection; "false" is the default
   nas=false
   ```
6. Change the value to `true` to enable NAS support, as shown in the following example:
   ```
   nas=true
   ```
7. Save your changes and close the file.
8. Restart the CIM extension. Refer to the *Installation Guide* for information about starting CIM extensions.

To discover an HP NAS device on Windows:

1. Click **Discovery** > **Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click the **Add Address** button.
5. In the **IP Address/DNS Name** field, type the IP address or DNS name of the HP NAS device you want to discover.

6. Enter the **User Name** of the HP NAS device. You must provide a privileged login.
7. Enter the **Password** used to access the HP NAS device.
8. Retype the password in the **Verify Password** field.
9. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. To start discovering elements on the network, click the **Start Discovery** button on the **IP Addresses** tab.

Discovering HP NAS Devices on Linux

In order to discover an HP NAS device on Windows, you must first install a CIM extension on the device. Refer to the *Installation Guide* for information on how to install the CIM extension.

In order to enable NAS support, you must modify a property file on the NAS device. To enable NAS support:

1. Connect to the NAS device on which you have installed the CIM extension.
2. Browse to the installation directory and open the CIMextension/conf directory.
3. Copy the nas.properties-sample file and paste a copy into the same directory.
4. Rename the copied file to nas.properties.
5. Open the file and locate the following line:
   ```
   # Set to true to enable NAS data collection; "false" is the default
   nas=false
   ```
6. Change the value to `true` to enable NAS support, as shown in the following example:
   ```
   nas=true
   ```
7. Save your changes and close the file.
8. Restart the CIM extension. Refer to the *Installation Guide* for information about starting CIM extensions.

To discover an HP NAS device on Linux:

1. Click **Discovery** > **Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.

4. Click the **Add Address** button.
5. In the **IP Address/DNS Name** field, type the IP address or DNS name of the HP NAS device you want to discover.
6. Enter the **User Name** of the HP NAS device. You must provide a privileged login.
7. Enter the **Password** used to access the HP NAS device.
8. Retype the password in the **Verify Password** field.
9. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. To start discovering elements on the network, click the **Start Discovery** button on the **IP Addresses** tab.

Discovering NetApp NAS Devices

Keep in mind the following:

- SMNP must be enabled on the NetApp NAS device before it can be discovered.
- If you want to communicate with the NetApp NAS device via SSL you must set the `cimom.providers.netapp.useSSL` property to “true.” This property is located in the `jboss.properties` file located in the %JBOSS4_DIST%`\server\appiq\conf` directory on the management server. This is a global setting and will cause all NetApp NAS devices to communicate using SSL.
- If you want the management server to be able to receive events from a NetApp NAS device, you must add the IP address of the management server to the NetApp configuration. The management server runs on the same computer running the management server by default.
- You must provide a privileged login, which is one of the following:
  - the root user
  - a user belonging to the “Administrators” group. This is a predefined group by NetApp.
  - a user belonging to a group that has the following roles: api-*, cli-*, login-http-admin, and at least one of the following: login-console, login-telnet, login-rsh, or login-ssh
- Administrative HTTP access to the device can be restricted through the httpd.access and httpd.admin.access options. If that is the case, then the management server needs to be registered with the device. This is done by adding the IP addresses of the management

server to the httpd.admin.access option. More information related to this option is available in the NetApp documentation.

To discover a NetApp NAS device:

1. Click **Discovery** > **Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click the **Add Address** button.
5. In the **IP Address/DNS Name** field, type the IP address or DNS name of the NetApp NAS device you want to discover.
6. Enter the **User Name** of the NetApp NAS device. You must provide a privileged login.
7. Enter the **Password** used to access the NetApp NAS device.
8. Retype the password in the **Verify Password** field.
9. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. To start discovering elements on the network, click the **Start Discovery** button on the **IP Addresses** tab.

Discovering Sun NAS Devices

Note: You do not need to provide the interop namespace because it is included in the management servers list of default namespaces.

To discover a Sun NAS Device:

1. Click **Discovery** > **Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click the **Add Address** button.

5. In the **IP Address/DNS Name** field, type the IP address or DNS name of the server running the SMI-S provider for the Sun NAS Devices you want to discover.
6. Enter the **User Name** of the CIMOM/provider for the Sun NAS Devices you want to discover. You must provide a privileged login.
7. Enter the **Password** used to access the CIMOM/provider for the Sun NAS Devices you want to discover.
8. Retype the password in the **Verify Password** field.
9. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. To start discovering elements on the network, click the **Start Discovery** button on the **IP Addresses** tab.

Discovering HP and IBM Tape Libraries

To discover an HP or IBM tape library:

1. Click **Discovery** > **Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click the **Add Address** button.
5. In the **IP Address/DNS Name** field, enter the IP address or DNS name for the tape library. Provide the namespace for the tape library after the IP address or DNS name of the tape library. For example: 192.168.1.1:root/ibm, where 192.168.1.1 is the IP address of the tape library and root/ibm is its namespace.
6. Enter the **User Name** of the system running the tape library.
7. Enter the **Password** of the system running the tape library.
8. Retype the password in the **Verify Password** field.
9. In the **Comment** field (optional), type a comment for additional information. The information typed into this field is displayed under the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.

12. To start discovering elements on the network, click the **Start Discovery** button on the IP Addresses tab.

Step 3 - Build the Topology

This section describes the following:

- “Building the Topology View” on page 132
- “Modifying the Properties of a Discovered Address” on page 134
- “Deleting Elements from the Product” on page 135

Building the Topology View

After you discover elements, the management server requires you to build a topology view, which is a graphical representation of port-level connectivity information.

If a switch has more than one connection to an element, the number of connections is displayed above the line linking the switch and the element. For example, assume the number two is shown between a switch and a storage system. This means the elements have two connections to each other. To view the port details for the connection, right-click the element and select **Show Port Details** from the drop-down menu.

If the topology changes, you can update how the element is viewed in the topology by selecting the element and clicking the Get Topology for Selected button in the Get Topology for discovered elements page (click **Discovery** > **Topology**). The management server obtains just enough information about where the element is connected in the topology, for example a switch connected to a host.

The management server marks an element with a question mark in the topology if the management server detects an element but it cannot obtain additional information about it. To learn more about fixing detected and/or disconnected elements, see the topic, “Troubleshooting Topology Issues” on page 391.

Important: The user interface may load slowly while the topology is being recalculated. It may also take more time to log into the management server during a topology recalculation.

To obtain enough information to display the topology in System Explorer:

1. Click the **Discovery** menu in the upper-right corner.
2. Click **Topology** in the upper-right corner.
   The discovered elements are selected.
3. Select the discovery group from which you want to obtain the topology. If you are obtaining the topology for the first time, make sure **All Discovery Groups** is selected.
   You can use discovery groups to break up getting the topology or getting details. For example, instead of getting the topology for all of the discovered elements, you could specify that the management server gets the topology for only the elements in Discovery Group 1, thus, saving you time. You add an element to a discovery group by modifying the properties used to discover the element. See “Modifying the Properties of a Discovered Address” on page 134.
4. Click the **Get Topology** button.
   The management server obtains the topology for selected elements.

   The management server displays the Log Message page. After the management server builds the topology, a link appears to take you to System Explorer so you can verify the topology view. You can also access System Explorer by clicking **System Explorer** in the left pane.
5. If you see errors in the topology, look at the log messages, which can provide an indication of what went wrong. See the topic, “Viewing Log Messages” on page 104 for more information about the messages that appear in this tab. Look at Event Manager for additional information. Access Event Managerby clicking the **Event Manager** button in the left pane. To obtain troubleshooting information, see the topic, “Troubleshooting Topology Issues” on page 391.
   If the topology for an element in your network changes, select the element and click **Get Topology** (**Discovery** > **Topology**) to updated the information.

   The software obtains just enough information about where the element is connected in the topology, for example a switch connected to a host.
6. See the topics in Chapter 18, “Troubleshooting” on page 363 for more information on troubleshooting problems with discovery and building the topology.

Modifying the Properties of a Discovered Address

All elements are initially placed in the Default discovery group. You can then move elements from the Default discovery group to other discovery groups.You can use discovery groups to break up Get Details. For example, you could specify that the management server get Get Details for only the elements in Discovery Group 1, thus, saving you time. This feature is sometimes referred to as segmented replication because you can specify getting Get Details for a segment of the discovered elements.

You can modify the following properties for discovering an device:

- **User name and password** - You can change the user name and password the management server uses to access a device. Whenever a user name and/or password has changed on a device the management server monitors, the management server must be made aware of the change. For example, assume the password for a host was changed. You would need to updated the management server database with the new password. See “Modifying a Single IP Address Entry for Discovery” on page 75.
- **Discovery group** - All elements are initially placed in the Default discovery group. You can then move elements from the Default discovery group to other discovery groups.You can use discovery groups to break up getting the topology or Get Details. For example, you could specify that the management server gets the topology or Get Details for only the elements in Discovery Group 1, thus, saving you time. This feature is sometimes referred to as segmented replication because you can specify getting the topology or Get Details for a segment of the discovered elements.

Keep in mind the following:

- You can use this window to change the user name and password stored in the management server's database. It does not change the device's user name and password.
- Discovery groups cannot be renamed or created. You must use the existing discovery groups.
- You can also use the **Move to Discovery Group** button to move multiple elements to another discovery group. See “Moving Elements to Another Discovery Group” on page 147 for more information.

To change the discovery properties of an element:

1. Click **Discovery** > **Topology** or **Discovery** > **Details** in the upper-right pane.
2. Click the  button corresponding with the element you want to modify.
3. To move an element to another discovery group, select its new discovery group from the **Discovery Group** drop-down menu.

4. Click **OK** in the Edit Discovered Element window.

Deleting Elements from the Product

When you delete an element, all of its information is removed from the management server. This includes asset information, zoning, events, statistics, and fabrics assigned to switches.

To completely delete an element from the management server you must remove the elements, such as a switch or proxy that were used to discover the element. If you do not delete all switches and proxies that were used to discover the element, the element may reappear the next time you Get Details.

For example, assume you want to delete Switch_A. Switch_B and Switch_C were used to discover Switch_A. If you delete only Switch_B and Switch_A, Switch_A will most likely reappear when you Get Details because it is still accessible by Switch_C.

You can delete an element within the following tools:

- **System Explorer or Chargeback** - Gives you the option of deleting just the element or deleting the element and the elements that use the same switches and proxies for access.
- **Discovery Step 2 (Topology)** - Gives you the option of deleting multiple elements at a time. You are not given a detailed list of other elements you must delete; however, you can use the table on the Discovery screen to determine which switches and proxies provided access.

Deleting an Element Using System Explorer or Chargeback

To delete an element using System Explorer or Chargeback:

1. Do one of the following:
   - **In System Explorer** - Right-click an element and select **Delete Element** from the drop-down menu. Right-click an element and select **Delete Element** from the drop-down menu.
     If you are blocking pop-ups and you use the right-click menu to delete an element from System Explorer, the Delete window is blocked and you are unable to delete the element. You must disable the popup blocker before you can delete the element.
   - **In Chargeback** - Click the  button for the element you want to delete.

2. If the element has multiple access points, you are asked which want to delete. Do one of the following:
   - **Delete the element and its access points.** This option lists not only the switch you want to delete, but also the other elements that use the same switches and proxies as the element you want to delete. For example, assume you want to delete Switch_A. Switch_B was used to discover Switch_A. Let's assume Switch_B is also the only path to Switch_D. If you delete Switch_B, you will no longer have access to Switch_D. This option would list Switch_D as one of the other elements that need to be deleted. An access point is the intersection of the IP address and the provider that discovered the IP address. A provider is software that is used to gather information about an element.
   - **Delete the element.** The element may reappear the next time you obtain element details. This is because not all switches and proxies connected to the element have not been removed. For example, assume you want to delete Switch_A. Switch_B is connected to Switch_A. If you do not delete Switch_B, the next time you obtain element details Switch_B will most likely find Switch_A again.
3. Click **OK**.

Deleting Elements Using Discovery Step 2 (Topology)

To delete multiple elements using Discovery Step 2 (Topology):

1. Click **Discovery** > **Topology**.
2. Determine the access points for the element you want to delete. In the following figure QBrocade2 is accessed by two switches: 192.168.10.25 and 198.168.10.22. You must delete both access points to completely remove the element. As a result, the QBrocade5 switch will also be removed because it has the same access points as QBrocade2.

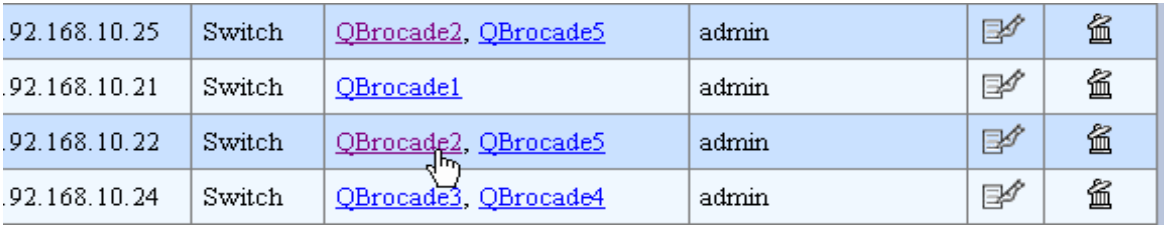


Figure 4-3: Deleting Elements from the Management Server

3. Select all of the access points for the element you want to delete. Then, click the **Delete** button just above the table.

For example, assume you want to delete QBrocade2 in the previous figure. You would select the two listings for QBrocade2 on the Discovered Elements tab and click the **Delete** button in the **Get Topology for Discovered Elements** table. If you delete only one of the listings, QBrocade2 and QBrocade5 still appear in the topology since they are still accessible from one of the switches.

When you are asked if you want to remove the access points and its associated elements, keep in mind these elements will not be deleted if they are accessible from an access point not listed in the Delete Access Points window. For example, assume you selected access point 192.168.10.25 to be deleted. You are then told that switch1 will be deleted along with the access point. Let's assume switch1 is accessible from another access point, 192.168.10.29. When you remove access point 192.168.10.25, switch1 will still be accessible because it can be accessed from another access point that has not been removed.

4. Click **OK** if you want to remove the access points listed in the Delete Access Points window.
   The access points are removed. If the elements listed have no other access points, they are no longer accessible from the management server.

Step 4 - Get Details

This section describes the following:

- Get Details on page 137
- Stopping the Gathering of Details on page 139
- Excluding EMC Symmetrix Storage Systems from Force Device Manager Refresh on page 140
- Excluding HDS Storage Systems from Force Device Manager Refresh on page 141

Get Details

Get Details is required to obtained detailed information from discovered elements. Get Details must be performed before you can do provisioning and/or obtain provisioning information, such as data about zone sets and LUN numbers.

Keep in mind the following:

- Get Details takes some time. You might want to perform this process when the network and the managed elements are not busy. To obtain a picture of device connectivity quickly, click the **Get Topology** button on the **Topology** tab.
- During Get Details the topology in System Explorer is recalculated. While the topology is being recalculated, the loading of the user interface may be slow. It may also take more time to log into the management server during a topology recalculation.
- If you have problems obtaining information from Connectrix and McDATA switches during Get Details, see the topic, “Step 2 - Discover Storage Systems, NAS Devices and Tape Libraries” on page 106.
- You can use discovery groups to break up getting the topology or Get Details. For example, instead of Get Details for all of the elements, you could specify that the management server Get Details for only the elements in Discovery Group 1, thus, saving you time. You add an element to a discovery group by modifying the properties used to discover the element. See “Moving Elements to Another Discovery Group” on page 147 for information on how to move one or more multiple elements to a discovery group. You can also move an element to another discovery group when you modify its discovery properties. See “Modifying the Properties of a Discovered Address” on page 134.
- When an element in a given discovery group is updated, its dependent elements are also updated. For example, assume Host_A is the only element in Discovery Group 1. Host_A is connected through a switch and storage system. When you Get Details for Discovery Group 1, you also obtain details from the switch and storage system.
- You can quarantine elements to exclude them from Get Details. See “Placing an Element in Quarantine” on page 148 for more information. Let us assume you want to discover all the elements in a discovery group, except for one. Perhaps the element you want to quarantine is being taken off the network for maintenance. You can use the quarantine feature to exclude one or more elements from discovery.
- If you want to receive status reports about Get Details, see “Configuring E-mail Notification for Get Details” on page 382 for information about how to configure this option.
- If the management server unable to obtain information from a UNIX host during Get Details as a result of a CIM Extension hanging, the management server places the access point where the CIM Extension is located in quarantine. The management server then moves onto getting details for the next element in the Get Details table. These UNIX hosts appear as missing until they are removed from quarantine. See “Removing an Element from Quarantine” on page 149 for information on how to remove an element from quarantine.

To obtain details about the devices on the network:

1. Click **Discovery** > **Details**.

2. Select **Include infrastructure details**, which gathers information about SAN details.
3. The management server obtains most of its information from device managers for storage systems with external databases, such as HP, HDS, and EMC storage systems. Select **Force Device Manager Refresh** if you want the management server to tell the device managers for your storage systems to obtain the latest information. If you do not select **Force Device Manager Refresh**, the management server gathers information from the external databases with the assumption the information in the external database is up to date. See the following topics for more information: “Excluding EMC Symmetrix Storage Systems from Force Device Manager Refresh” on page 140 and “Excluding HDS Storage Systems from Force Device Manager Refresh” on page 141.
4. Select the discovery group from which you want to obtain Get Details. If you are obtaining Get Details for the first time, make sure **All Discovery Groups** is selected.
5. Click the **Get Details** button.
   During Get Details, the software changes its status light from green to red. You can view the progress of gathering details by clicking **Discovery** > **View Logs**.

   When the software completes getting all elements details, it displays “GETTING ALL DETAILS COMPLETED” on the **View Logs** page.
6. See the User Guide for information about automating the gathering of all element details.

Stopping the Gathering of Details

Obtaining details takes some time. If the network and managed elements are busy, you might need to stop the gathering of details and reschedule it for another time.

Important: If you stop the gathering of details, you should reschedule it. This type of collection obtains detailed information of devices in the network.

To stop the gathering of details:

1. Click **Discovery** > **View Logs**.
2. On the **View Logs** page, click the “Click here” portion of the following message:
   `Click here if you wish to stop getting details.`
3. When you are asked if you are sure you want to stop Get Details, click **OK**.
   The management server stops gathering details.
4. Schedule a time to resume getting details.

Excluding EMC Symmetrix Storage Systems from Force Device Manager Refresh

The management server obtains most of its information about Symmetrix storage systems from the EMC Solutions Enabler (proxy server) it discovered. If the EMC Solutions Enabler does not have the latest information, the management server also displays the outdated information.

To make the management server aware of any changes, make sure the Solutions Enabler it discovered has the latest information. This can be done by forcing the Solutions Enabler to refresh its data. The management server is then made aware of these changes.

When the **Force Device Manager Refresh** option is selected, the management server refreshes discovered EMC Solutions Enabler (proxy server), unless specified. If you do not want an EMC Solutions Enabler to be refreshed, you must assign the Symmetrix storage systems that use the Solutions Enabler to the `cimom.emc.skipRefresh` property, as described in the steps in this section.

To exclude EMC Symmetrix storage systems from a forced refresh:

1. Select **Configuration** > **Product Health** > **Advanced**.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the following command. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.
   ```
   #cimom.emc.skipRefresh=000183500570,000183500575
   ```
4. Return to the Advanced page (**Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree).
5. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
6. Make sure the property is not commented out by removing the hash (#) symbol in front of the property. Add the serial numbers corresponding to the Symmetrix storage systems you want the refresh to skip. Separate additional serial numbers with a comma, as shown by the following example:
   ```
   cimom.emc.skipRefresh=000183500570,000183500575
   ```
   where `000183500570` and `000183500575` are serial numbers for Symmetrix storage systems. One of the ways to find the serial number is to double-click the storage system in System Explorer. Then, click the **Properties** tab.
7. When you are done, click **Save**.

8. Restart the service for the management server for your changes to take effect:
   a. Go to the Services window on the management server.
   b. Right-click **AppStorManager**.
   c. Select **Restart** from the drop-down menu.
   While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.
9. To perform the forced refresh, select the **Force Device Manager Refresh** option on the Get Details page.
10. Click **Get Details**.

Excluding HDS Storage Systems from Force Device Manager Refresh

The management server obtains most of its information about the HDS storage systems from the HiCommand Device Manager (proxy server) it discovered. If HiCommand Device Manager, does not have the latest information, the management server also displays the outdated information.

To make the management server aware of any changes, make sure the HiCommand Device Manager it discovered has the latest information. This can be done by forcing the HiCommand Device Manager to refresh its data. The management server is then made aware of these changes.

When the **Force Device Manager Refresh** option is selected, the management server refreshes discovered HiCommand Device Manager (proxy server), unless specified. If you do not want a HiCommand Device Manager to be refreshed, you must assign the HDS storage systems that use HiCommand Device Manager to the `cimom.HdsSkipRefresh` property, as described in the steps in this section.

Important: Before performing any provisioning operations, you should perform a forced refresh.

To exclude HDS storage systems from a forced refresh:

1. Select **Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree.
2. Click **Show Default Properties** at the bottom of the page.

3. Copy the following command. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.
   ```
   # cimom.HdsSkipRefresh=61038,61037
   ```
4. Return to the Advanced page (**Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree).
5. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
6. Make sure the property is not commented out by removing the hash (#) symbol in front of the property. Add the serial numbers corresponding to the HDS storage systems you want the refresh to skip. Separate additional serial numbers with a comma, as shown by the following example:
   ```
   cimom.HdsSkipRefresh=61038,61037
   ```
   where `61038` and `61037` are serial numbers for HDS storage systems. One of the ways to find the serial number is to double-click the storage system in System Explorer. Then, click the **Properties** tab.
7. When you are done, click **Save**.
8. Restart the service for the management server for your changes to take effect:
   a. Go to the Services window on the management server.
   b. Right-click **AppStorManager**.
   c. Select **Restart** from the drop-down menu.
   While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.
9. To perform the forced refresh, select the **Force Device Manager Refresh** option on the Get Details or page.
10. Click **Get Details**.

Troubleshooting Mode

Troubleshooting Mode can be used to assist you in identifying and resolving host configuration issues during discovery, as described in the following steps:

1. If errors occur during discovery, an error message will display at the top of the screen below the discovery step where the errors occurred. If you receive an error message, enable Troubleshooting Mode by selecting the **Enable Troubleshooting Mode** check box located near the top of the page for each discovery step.
2. A red icon will display in the **Problems** column for each host for which a problem was detected. Clicking this icon for a particular host will cause a list of troubleshooting tips to display below the **Enable Troubleshooting Mode** check box. Use these tips to assist in the resolution of configuration problems for that host.
3. You can also enter Troubleshooting Mode by clicking the link located in the error message for one of the discovery steps. For example, if you are on discovery step 3, you can click the “Discovery->Setup in Troubleshooting mode” link located in the step 1 error message. Clicking this link will bring you to the step 1 page with Troubleshooting Mode enabled.

Note: Step 3 Troubleshooting Mode only identifies quarantined hosts.

When Troubleshooting Mode is enabled during discovery step 2 or 3, the following additional information is provided to assist in the identification of configuration issues:

- Host OS
- CIM Extension Version
- HBA (Driver Version)
- Multipathing

Managing McDATA and EMC Connectrix Switches

This section describes the following:

- “About Managing McDATA and EMC Connectrix Switches” on page 144
- “Adding McDATA and EMC Connectrix Switches” on page 144
- “Removing McDATA and EMC Connectrix Switches” on page 145
- “Swapping McDATA and EMC Connectrix Switches” on page 145

About Managing McDATA and EMC Connectrix Switches

Whenever you add, remove or replace McDATA or EMC Connectrix switches in an already discovered service processor, you must make the management server aware of those changes. After you add these switches to the service processor, you must perform Get Details. The management server obtains information about the new switches from the service processor. See the topic, “Adding McDATA and EMC Connectrix Switches” on page 144 for more information about adding switches.

When you remove switches from the service processor, you must remove them from the management server as well. See the topic, “Removing McDATA and EMC Connectrix Switches” on page 145 for more information about removing switches. When you replace McDATA or EMC Connectrix switches, you add and remove the switches as described previously. See the topic, “Swapping McDATA and EMC Connectrix Switches” on page 145 for more information.

Adding McDATA and EMC Connectrix Switches

After you add switches to an existing service processor, you must perform Get Details, as described in the following steps. If you are adding switches to a service processor that has not been discovered yet, see the topic, “Discovering McDATA and EMC Connectrix Switches” on page 91.

Important: Obtaining details takes some time. You might want to perform this process when the network and the managed elements are not busy.

To Get Details:

1. Click **Discovery** > **Details**.
2. Click the **Get Details** button.
   During Get Details, the software changes its status light from green to red. You can view the progress of gathering details by accessing the logs. See “Viewing Log Messages” on page 104.

Removing McDATA and EMC Connectrix Switches

After removing switches from a service processor, perform the following steps to remove the switches from the management server database.

1. Deleted the switches from the user interface by doing the following. These should be the same switches you removed from the service processor.
   a. Click **System Explorer** in the left pane.
   b. Right-click the switch you want to delete.
   c. Select **Delete Element** from the drop-down menu.
   d. Select the following option:
      `Just delete Switch [switch_name]. It may reappear the next time you get topology information or element details.`
   e. Repeat Steps a through d for each switch you want to delete.
2. Verify the switches have been removed from the Elements List in Discovery Steps 2 and 3 by doing the following:
   a. To verify the switches have been removed from the element list in Discovery Step 3, click **Discovery** > **Details**.
   b. To verify the switches have been removed from the element list in Discovery Step 2, click **Discovery** > **Topology**.

Swapping McDATA and EMC Connectrix Switches

After replacing switches in the service processor, you must make the management server aware of your changes by removing the old switches from the user interface and then performing Get Details so the management server can discover the new switches. If you are adding switches to a service processor that has not been discovered yet, see the topic, “Discovering McDATA and EMC Connectrix Switches” on page 91.

Important: Get Details takes some time. You might want to perform this process when the network and the managed elements are not busy.

Perform the following steps in the management server to swap the switches:

1. Deleted the switches from the user interface by doing the following. These should be the same switches you removed from the service processor.
   a. Click **System Explorer** in the left pane.
   b. Right-click the switch you want to delete.
   c. Select **Delete Element** from the drop-down menu.
   d. Select the following option:
      `Just delete Switch [switch_name]. It may reappear the next time you get topology information or element details.`
   e. Repeat Steps a through d for each switch you want to delete.
2. Verify the switches have been removed from the Elements List in Discovery Steps 2 and 3 by doing the following:
   a. To verify the switches have been removed from the element list in Discovery Step 2, click **Discovery** > **Topology**.
   b. To verify the switches have been removed from the element list in Discovery Step 3, click **Discovery** > **Details**.
3. Click **Discovery** > **Details**.
4. Click the **Get Details** button.
   While Get Details, the software changes its status light from green to red. You can view the progress of gathering details by clicking **Discovery** > **View Logs**.

   When the software completes Get Details, it displays a message saying Get Details is complete on the **View Logs** page.

Assigning a File Extension in Netscape 7

Netscape 7 automatically assigns unknown files an HTML extension. To make Netscape 7 recognize the type of file, you must assign a file extension.

To assign a MIME type:

1. Click the download file link or button in the software.
2. Click the **Advanced** button in the lower-left corner.
3. In the **Description of type** field, delete the existing text and type a description of the file.
4. In the **File extension** field, delete the existing text and type the file extension.
5. Click **OK**.

The next time Netscape 7 sees the associated MIME type, it will assign the extension you typed in the **File Extension** field.

6. Click **OK**.

Filtering Discovery Groups

You can determine which discovery groups are displayed on the Topology (**Discovery** > **Topology**) and Discovery (**Discovery** > **Details**) pages by modifying the discovery filter, as described in the following steps:

1. Access the Topology (**Discovery** > **Topology**) or Get Details (**Discovery** > **Details**) page.
2. Click the **Custom** button.
3. Select the discovery groups you want to include in Get Details. Deselect the discovery groups you do not want to be included in Get Details.
4. Click **OK**.
   Elements in the selected discovery groups are selected on the Get Details page for Discovery. The management server obtains information from the selected elements during Get Details. To learn how to add an element to a different discovery group, see “Modifying the Properties of a Discovered Address” on page 134.

Moving Elements to Another Discovery Group

All elements are initially placed in the Default discovery group. You can then move elements from the Default discovery group to other discovery groups. You can use discovery groups to break up Get Details and getting the topology. For example, you could specify that the management server gets Get Details for only the elements in Discovery Group 1, thus, saving you time. This feature is sometimes referred to as segmented replication because you can specify getting Get Details for a segment of the discovered elements.

Keep in mind the following:

- Discovery groups cannot be renamed or created. You must use the existing discovery groups.
- You can also use move an element to another discovery group when you modify its discovery properties. See “Modifying the Properties of a Discovered Address” on page 134 for more information.

To move an element to another discovery group:

1. Select the check boxes for the elements you want to move in the Get Details page.
2. Click the **Move to Discovery Group** button.
3. In the Select Discovery Group window, select the new discovery group for the selected elements.
4. Click **OK**.
   The elements are moved to the new discovery group.

Placing an Element in Quarantine

When you click the **Get Details** button on the Get Details page, the management server automatically obtains details for the elements in the selected discovery group. Let us assume you want to discover all the elements in a discovery group, except for one. Perhaps the element you want to quarantine is being taken off the network for maintenance. You can use the quarantine feature to exclude one or more elements from discovery.

Note: After you perform Get Details for the discovery group containing the quarantined elements, the quarantined elements appear as missing throughout the product. The management server marks the quarantined elements as missing because it cannot obtain details from the quarantined element.

To quarantine an element:

1. Select the check boxes for the elements you want to quarantine on the Get Details page.
2. Click the **Set Quarantine** button.
3. When you are asked if you want to quarantine the selected elements, click **OK**.

The elements you quarantine appear with a flag ( ) in the Quarantined column on the Get Details page.

The elements are excluded from discovery until you clear them from quarantine.

Removing an Element from Quarantine

To remove an element from quarantine:

1. Select the check boxes for the elements you want to remove from quarantine on the Get Details page.

   Quarantined elements appear with a flag ( ) in the Quarantined column on the Get Details page.
2. Click the **Clear Quarantine** button.
3. When you are asked if you want to remove the selected elements from quarantine, click **OK**.
   The next time you perform Get Details for the element, the management server gathers data from the element.

Updating the Database with Element Changes

After you have initially discovered the elements, information about them might change. To update database with these changes, perform the steps described in this section.

Keep in mind the following:

- If you change the password of a host after you discover it, you must change the password for the host in the discovery list. Then, you must stop and restart the CIM Extension running on that host before you run a discovery.
- If you are adding, removing or replacing McDATA or Connectrix switches, you must perform different steps. See the topics, “Adding McDATA and EMC Connectrix Switches”

on page 144, “Removing McDATA and EMC Connectrix Switches” on page 145, and “Swapping McDATA and EMC Connectrix Switches” on page 145.

- Get Details takes some time. You might want to perform this process when the network and the managed elements are not busy. To obtain a picture of device connectivity quickly, click the **Get Topology** button on the **Topology** tab.

To update the database:

1. Click **Discovery** > **Details**.
2. Select **Include infrastructure details**, which gathers information about SAN details. **Include backup details** is used for gathering information for Protection Explorer. You do not need to select **Include backup details** unless you have already discovered hosts running backup applications and installed CIM Extensions on those hosts. See “Step 1 - Discovering Your Hosts” on page 285 for more information about discovering master backup servers. The **Include backup details** option gathers the latest information about your backup applications.
3. The management server obtains most of its information from device managers for storage systems with external databases, such as HP, HDS, and EMC storage systems. Select **Force Device Manager Refresh** if you want the management server to tell the device managers for your storage systems to obtain the latest information. If you do not select **Force Device Manager Refresh**, the management server gathers information from the external databases with the assumption the information in the external database is up to date. See the following topics for more information: “Excluding EMC Symmetrix Storage Systems from Force Device Manager Refresh” on page 140 and “Excluding EMC Symmetrix Storage Systems from Force Device Manager Refresh” on page 140.
4. Click the **Get Details** button on the Get Details page.
5. View the status of the gathering of element details by looking in the **View Logs** page. See the topic, “Viewing Log Messages” on page 104 for more information about the messages viewed in this tab.
6. Verify the topology is displayed correctly by accessing System Explorer. Access System Explorer clicking its button in the left pane.

Notifying the Software of a New Element

When you add a new element to the network, such as a host, perform discovery to make the management server aware of the new element.

Keep in mind the following while performing discovery:

- If you change the password of a host after you discover it, you must change the password for the host in the discovery list. Then, you must stop and restart the CIM Extension running on that host.
- If you started a CIM Extension on a Sun Solaris host with the `./start -users` command, a user name provided in the command must be used to discover the host. For example, if you use `./start -users myname:yourname` (where `myname` and `yourname` are valid UNIX accounts) to start the CIM Extension, `myname` or `yourname` and its password must be used to discover the host.
- If you have Brocade switches, download and install the Brocade SMI-S provider software from the following FTP site if this is a new installation of the management server.
  `ftp://ftp.compaq.com/pub/products/storageworks/smisproviders/brocade_provider.pdf`
  If you are upgrading to build 5.1 from any build prior to 4.2 of the management server your Brocade switches are discovered using the Brocade Fabric Access API after the upgrade. See “Important Information About Upgrading and Brocade Switches” on page 61.

  You must also verify that the Rapid program on the switch is set to 1. Rapid must be set to 1 so that the management server can communicate with the switch. See the topic, “Verifying Brocade Rapid Program Is Set to 1” on page 83 for more information.
- Additional steps are required for discovering McDATA switches, and the steps vary according to your network configuration. See the topic, “Discovering McDATA and EMC Connectrix Switches” on page 91 for more information.
- EMC CLARiiON storage systems require additional steps for discovery. See the topic, “Discovering EMC CLARiiON Storage Systems” on page 113 for more information.
- After you discover a McDATA or EMC Connectrix switch, the IP address displayed next to the name of the switch is actually the IP address of the service processor for the switch in the Get Details screens. To find the IP address of the switch, click the link for the switch in the Topology screen (**Discovery** > **Topology**) or Get Details screen (**Discovery** > **Details**) and then click the **Properties** tab. The **Properties** tab can also be accessed by double clicking the switch in System Explorer.

For additional information about adding switches, NAS devices, and storage systems, see:

- Table 4-1, “Discovery Steps for Switches, NAS Devices, and Storage Systems,” on page 68
- Chapter 16, “Discovering Applications and Hosts” on page 285

CHAPTER 5

Deploying and Managing CIM Extensions

This chapter describes the following:

- “About Remote CIM Extensions Management” on page 153
- “About the CIM Extensions Management Tool” on page 156

About Remote CIM Extensions Management

It is possible to install, upgrade, and manage CIM Extensions remotely across any number of hosts. The following operations can be initiated from the management server:

- Perform an installation or re-installation of the OpenSSH daemon (sshd) for Windows hosts only.
- Perform an installation or re-installation of the CIM Extension.
- Stop the CIM Extension
- Start the CIM Extension
- Obtain status information of the CIM Extension.

- Retrieve all related log files (cxws.log for Windows and Unix hosts; cxws.out from Unix hosts; Application Log File for Windows hosts).
- Retrieve host-specific configuration information for the CIM Extension.
- Update the host-specific configuration information for the CIM Extension.

CIM Extensions can be remotely managed through the command line interface (CLI). Refer to the *CLI Guide* for information about installing the CLI and using the available commands.

CIM Extensions can also be remotely managed through a graphical user interface called the CIM Extensions Management Tool. See “About the CIM Extensions Management Tool” on page 156 for more information.

About SSH

Each host being managed must be running a supported SSH daemon. The SSH daemon must support SFTP file transfers and the EXEC channel method of executing remote commands. The root or Administrator user must be allowed to log in for most operations.

The default SSH configuration on some hosts prohibits root login by default. Follow these steps to manually configure SSH to allow root login:

1. Use a text editor to open `etc/ssh/sshd_config`
2. Change the value of `PermitRootLogin` to `yes`.
3. Restart the SSH daemon.

Keep in mind the following when deploying OpenSSH on a Windows host:

- If you are using a domain, always specify user names so that they include the domain. For example, enter a user name of `<domain1>\<admin>`
  where
  - `domain1` is the domain name
  - `admin` is the username
- If you are not using a domain, don’t specify the host name when deploying OpenSSH. For example, enter a user name of `<admin>`
  where
  - `admin` is the user name

Copying the CIM Extensions to the Management Server

To remotely install the CIM Extensions, you must first copy the CIM Extensions installation files to the management server.

The following error message displays if the CIM Extensions installation files haven't been copied to the management server:

```
Unable to upload file to remote host
```

Important: Do not install the CIM Extension on the Management Server, a built-in CIM Extension is automatically installed on the Management Server during the installation process. If you install a standard CIM Extension on the management server, you must uninstall the mangagement server software and then re-install.

To copy the CIM Extensions installation files onto a Microsoft Windows server:

1. Go to the CIM Extensions CD-ROM.
2. Double-click **CopyExtensionFiles.exe**.

   Note: Do not change the default directory.

To copy the CIM Extensions installation files onto a Sun Solaris management server:

1. Log in as root.
2. Mount the CIM Extensions CD-ROM and change directory to where you mounted it.
3. Run **./CopyExtensionFiles.sh**. The CIM Extensions installation files will be copied to the appropriate place on the server.

Creating Default Logins for Hosts

You can create a default login for each type of host (HPUX, Solaris, Windows, Linux, AIX) that you intend to install CIM Extensions on.

To create default logins for hosts:

1. Create a text file named **cxws.default.login** with the following format:
   `-credentials <userid>:<password>`
2. Place the **cxws.default.login** file in the following directory on the management server:
   `%JBOSS4_DIST%\Extensions\[Platform]`
   where `[Platform]` is the directory of the host type.

For example, to create a default login for Windows with a user ID of “myname” and a password of “password” you would create the following file:

```
%JBOSS4_DIST%\Extensions\Windows\cxws.default.login
```

The **cxws.default.login** file would contain the following:

```
-credentials myname:password
```

About the CIM Extensions Management Tool

CIM Extensions can be remotely managed through a graphical user interface called the CIM Extensions Management Tool.

Each host being managed must be running a supported SSH daemon. See “About SSH” on page 154 for more information.

You must copy the CIM Extensions to the management server before you can use the CIM Extension Management Tool. See “Copying the CIM Extensions to the Management Server” on page 155 for more information.

Launching the CIM Extensions Management Tool

Follow these steps to launch the CIM Extensions Management Tool:

1. Go to the `%MGR_DIST%\Tools\cimeMgmt` directory on the management server.
2. Run `cimeMgmt.cmd`.

Adding Remote Hosts

Follow these steps to create a list of remote hosts on which you will be deploying and managing CIM Extensions:

1. In the **Hostname** field, type the name of the host.
2. In the **Username** field, type the username used for accessing the host.
3. In the **Password** field, type the password used for accessing the host.
4. Click the **Add** button to add the host to the table below.
5. Repeat steps 1 through 4 for each additional host you want to add.
6. Click the  button if you want to edit the entry for a host.
7. Click the  button if you want to delete a host from the list.

Managing CIM Extensions on Remote Hosts

Once you have added all the hosts that you want to manage, you can select any of the actions from the left panel. The following actions are available:

- **Display host operating system** - Attempts to determine the remote operating system.
- **Display Installed CIM Extension Version** - Fetches and displays the version of the CIM Extensions currently installed on the remote system.
- **Deploy CIM Extensions** - Installs the CIM Extensions on the remote system.
- **Deploy OpenSSH (Windows Only)** - Deploys OpenSSH on the remote Windows system.
- **Uninstall CIM Extensions** - Uninstalls the CIM Extensions on the remote system.
- **Upgrade CIM Extensions** - Upgrades the CIM Extensions on the remote system.
- **Start CIM Extensions** - Starts the CIM Extensions on the remote system.
- **Stop CIM Extensions** - Stops the CIM Extensions on the remote system.
- **Download configuration** - Downloads the configuration files from the CIM Extensions on the remote system.
- **Download logs** - Downloads the log files from the CIM Extensions on the remote system.
- **Configure** - Configures the CIM Extensions on the remote system. You can configure the TCP port to listen on, the IP address to bind to, and custom credentials for the extensions to use.

Note: You can only configure the IP address with a specific address if there is only one system in the list. If there is more than one system, you can only use “auto detect” mode, which instructs the host to listen on the IP address looked up from the same hostname used to connect to the host.

Configuring CIM Extensions

Click the **Go** button next to the **Configure** action to configure CIM Extensions on remote hosts.

The **Configure CIM Extensions** dialog box displays and allows you to configure all the hosts on the list with the specified settings. The tool will create a new CIM Extension configuration file for each indicated remote host. A backup copy will be saved on each host with its previous configuration.

The choices in this dialog box are all optional. If they are not specified, they will be omitted from the configuration files.

The **Auto-detect IP address** checkbox will cause the tool to use the hostname that was typed in the **Hostname** field to start the CIM Extensions.

Note: You can’t use the **IP Address** field when multiple hosts are listed.

The **Start Extensions on Custom Port** checkbox will start the CIM extension on the specified port.

Note: When setting up the collection of data from the management server, you must use the port with which you configured the extensions instead of the default port.

The **Use Custom Credentials** checkbox configures the CIM Extensions to use a username and password that you specify. This username and password is known only to the CIM Extensions, and is not a real user on the host system.

Note: When setting up the collection of data from the management server, you must use the credentials you configured the extensions with instead of the host's "root" or "administrator" user.

Status Icons

A status for each host displays in the column to the right of the host name. The following statuses are possible:

Table 5-1: Status Icons

Icon	Status
	The host has been added to the list, but no action as been selected.
	The action is waiting to begin or in progress.
	The last action completed with a warning.
	The last action completed successfully.
	The last action has failed.

CHAPTER 6

Installing the CIM Extension for IBM AIX

This chapter describes the following:

- About the CIM Extension for IBM AIX on page 162
- Prerequisites on page 163
- Verifying SNIA HBA API Support on page 164
- Installing the CIM Extension on page 165
- Setting Up Monitoring on page 166
- Starting the CIM Extension Manually on page 166
- How to Determine if the CIM Extension Is Running on page 167
- Configuring CIM Extensions on page 167
- Stopping the CIM Extension on page 171
- Stopping the CIM Extension on page 171
- Fulfilling the Prerequisites on page 171
- Rolling Over the Logs on page 172
- Removing the CIM Extension from AIX on page 173

Note: This chapter describes how to install and manage the CIM Extension directly on the host. You can also install and manage CIM Extensions remotely. See “Deploying and Managing CIM Extensions” on page 153.

Important: Make sure you have reviewed Table 1-1, “Roadmap for Installation and Initial Configurations,” on page 2 to ensure you are at the correct step.

About the CIM Extension for IBM AIX

The CIM Extension for IBM AIX gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

Install the CIM Extension on each host you want the management server to manage.

The CIM Extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBA API. For more information about the HBA API, see the following Web page at the SNIA Web Site: http://www.snia.org/tech_activities/hba_api/

The installation creates the following directories in the `/opt/APPQcime` directory:

- **jre** - The Java run time necessary to run the CIM Extension
- **lib** - The executables for the CIM Extension
- **tools** - The files to stop, start and show the status of the CIM Extension

Prerequisites

The installation checks for the following. If the installation fails, see “Fulfilling the Prerequisites” on page 171.

AIX 5.1

- Maintenance level 03 or later
- bos.rte.libc.5.1.0.36 or later

Both AIX 5.1 and 5.2

xlC.rte.5.0.2.1 or later

AIX 5.3

- bos.rte.libc 5.3.0.0
- xlC.rte 6.0.0.0

Required Disk Space

The CIM Extension for AIX requires 40 MB.

Network Port Must Be Open

The CIM Extension uses port 4673 by default to communicate with the management server. Verify the network port is open. Refer to the documentation accompanying your AIX host for more information. If you need to use a different port, see “Permanently Changing the Port a CIM Extension Uses (UNIX Only)” on page 367.

bos.perf.libperfstat Required for Performance Data

The file bos.perf.libperfstat is required for the management server to obtained performance data. Without bos.perf.libperfstat, the following occurs:

- 32-bit kernel - You do not receive information about the amount of virtual memory used.
- 64-bit kernel
  - You are shown zero on the navigation page for “Total Physical Memory.”
  - You are shown the following error message in the log:

```
bos.perf.libperfstat not installed - required for 64-bit Kernel to get disk
or cpu statistics.
```

- You do not obtain information for the following in Performance Explorer:
  - statistics on the operating system
  - disk (disk utilization, disk read, disk write)
  - CPU (processor utilization)

Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. You can run the hbatest program, which is accessible from the CIM Extension CD-ROM. The program, hbatest, lists the name and number for all HBA's that support the SNIA HBA API. In some instances hbatest may report it cannot find an HBA driver even though an HBA driver is installed. Try installing a different version of the HBA driver that is SNIA compliant.

To run hbatest:

1. Go to the `Aix/tools` directory on the CIM Extension CD-ROM.
2. Enter the following at the command prompt: `./hbatest`
   The program runs its diagnostics.

IBM Adapters FCXXXX SNIA comes from the package devices.common.IBM.fc.hba-api. To find its library, enter the following at the command prompt:

```
# more /etc/hba.conf
```

The following is displayed:

```
com.ibm.df1000f7 /usr/lib/libHBAAPI.a
com.ibm.df1000f9 /usr/lib/libHBAAPI.a
```

Installing the CIM Extension

Important: The following steps assume you know how to use smit. If you are unfamiliar with smit, refer to the documentation that accompanies the AIX host.

To upgrade the CIM Extension, first remove the previous version before installing the latest version. Builds 4.0 and later of the CIM Extension are compatible with this build of the management server.

To install the CIM Extension for AIX:

1. Insert the CIM Extensions CD-ROM into the CD-ROM drive.
2. Mount the CD-ROM drive by entering the following at the command prompt:
   `# mount -rv cdrfs /dev/cd0 /cdrom`
   where `/dev/cd0` is the name of the CD-ROM drive.

   If necessary, create a `/cdrom` directory first.
3. Enter the following at the command prompt:
   `# smit -C`
4. Select **Software Installation and Maintenance**.
5. Select **Install and Update Software**.
6. Select **Install Software**.
7. For INPUT device/directory for software, enter the following:
   `cdrom/Aix`
   where`/cdrom` is the directory where you mounted the CD-ROM.
8. To install the software, activate the list command (Esc+4) and select the following:
   `APPQcime`
9. Press **ENTER** to install.
10. If you see error messages when you install the CIM Extension for AIX, see “Fulfilling the Prerequisites” on page 171.
11. Unmount the CD-ROM by entering the following at the command prompt:
    `# umount /cdrom`
    where `/cdrom` is the name of the directory where you mounted the CD-ROM
12. Complete the following:
    - ☐ Turn on Monitoring. See “Setting Up Monitoring” on page 166.

- Start the CIM Extension. See “Starting the CIM Extension Manually” on page 166.
- (Optional) On some versions of AIX, the CIM Extension cannot start automatically after the host is rebooted. To see if your version of AIX supports the automatic startup, see “Fulfilling the Prerequisites” on page 171.

Setting Up Monitoring

If you want the management server to be able to monitor the AIX host, iostat must be set to true. When iostat is set to true, disk activity history is retained for all disks. The retention of disk activity is required for the management server to accurately monitor the AIX host.

To verify if disk activity history is being retained:

1. Enter the iostat command in the command prompt:
   ```
   # iostat
   ```
2. If you see the message “Disk history since boot not available”, enter the following at the command prompt to enable the retention of disk activity history:
   ```
   # chdev -l sys0 -a iostat=true
   ```

Starting the CIM Extension Manually

The management server can only obtain information from this host when the CIM Extension is running. To start the CIM Extension, type the following in the `/opt/APPQcime/tools` directory:

```
# ./start
```

Keep in mind the following:

- You must have root privileges to run the CIM Extension. The CIM Extension only provides the information within the privileges of the user account that started the CIM Extension. Only root has enough privileges to provide the information the management server needs. If you do not start the CIM Extension with root privileges, the management server will display messages resembling the following: `Data is late or an error occurred.`
- To configure UNIX CIM Extensions to run behind a firewall, see “Configuring UNIX CIM Extensions to Run Behind Firewalls” on page 369.

- If you see a “Fork Function Failed” message when you start the CIM Extension, the AIX host is running low on physical or virtual memory. See ““Fork Function Failed” Message on AIX Hosts” on page 408.

The following is displayed:

```
Starting CIM Extension for AIX...
```

How to Determine if the CIM Extension Is Running

You can determine if the CIM Extension is running by entering the following command at the command prompt:

```
# ./status
```

The CIM Extension is running when the following message is displayed:

```
CIM Extension Running: Process ID: 93
```

where 93 is the process ID running the CIM Extension

Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM Extension on start-up. The file is named `cim.extension.parameters` and is located in the `[Installation_Directory]/conf` directory on the host. This directory also contains a file named `cim.extension.parameters-sample`. This file contains samples of available parameters and can be copied into the `cim.extension.parameters` file and used as a template.

Changing the Port Number

The CIM Extension uses port 4673 by default. If the port is already used, follow these steps to change the port the CIM Extension will access:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:
   `-port 1234`
   where 1234 is the new port for the CIM Extension
3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

192.168.1.2:1234

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Configuring the CIM Extension to Listen on a Specific Network Card

Follow these steps to configure the CIM Extension to listen on a specific network card (NIC):

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:
   `-on 127.0.0.1,192.168.0.1`

   Note: If you want to configure the CIM Extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

   Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

The “-on” parameter may include a port specification. In that case, the CIM Extension listens on the indicated port of the indicated NIC, rather than the default port, for example:

```
-on 192.168.2.2:3456
```

The CIM Extension listens only on the NIC that has the IP address 192.168.2.2 on port 3456.

The management server assumes the CIM Extension is running on port 4673. The management server also listens on port 17000 for CIM Extensions from build 4.0.

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

192.168.1.2:1234

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file:

Table 6-1: Parameters for CIM Extensions

Parameter	Description
`-user`	The user defined in this parameter must be a valid user for the host. Only the user needs to be defined. The user name and password are provided from the management server during discovery. The user does not need to have root authority. A colon separated list can be used to specify multiple users.
`-credentials <username from the management server>:<password>`	The credentials defined by this parameter must match the values entered from the management server during discovery. They are not used as authentication on the host itself.
`-agentnic <ip address>`	Restricts the CIM Extension on multihomed systems to listen only on the designated IP address.
`-mgmtServerIP <ip address>`	Restricts the CIM Extension to listen only to a specific management server IP address.

Finding the Version of a CIM Extension

You can find the version number of a CIM Extension:

1. Go to the `/opt/APPQcime/tools` directory.
2. Type the following at the command prompt:
   ```
   # ./start -version
   ```
   You are shown the version number of the CIM Extension and the date it was built, as shown in the following example:

   ```
   CXWS for mof/cxws/cxws-aix.mof
   ```

```
CXWS version xxxx, built on Fri xx-March-xxxx 12:29:49 by dmaltz
```

Stopping the CIM Extension

To stop the background process for the CIM Extension, enter the following at the command prompt in the `/opt/APPQcime/tools` directory:

```
# ./stop
```

Keep in mind the following:

- You must have root privileges to stop the CIM Extension.
- When you stop the CIM Extension, the management server is unable to gather information about this host.

Fulfilling the Prerequisites

If your installation failed, you may be missing the following prerequisites. Refer to the information below on the required maintenance level and file sets.

Important: Installation of the `devices.common.IBM.fc.hba-api.5.1.0.0` file set is optional. If you do not install this file set, you will be able to discover the AIX host, but you will not see any information about your host bus adapters or any information they provide. For example, the Navigation page for the host will not show results for host bus adapters, HBA ports, or bindings. Also if you do not install the `devices.common.IBM.fc.hba-api.5.1.0.0` file set, the host is displayed in the topology, but devices attached to the host are not displayed, such as switches. This information also applies to the `devices.common.IBM.fc.hba-api.5.3.0.0` file set for AIX 5.3.

AIX 5.1

- **Maintenance level 03 or later** - This is required for the HBA API. The operating system level can be found by entering the following command at the command prompt:
  `oslevel -r`
- **bos.rte.libc.5.1.0.36 or later** - This is required for Java 1.4 support. The file can be downloaded from the IBM Technical Support Web site at the following URL:
  https://techsupport.services.ibm.com

Both AIX 5.1 and 5.2

xlC.rte.5.0.2.1 or later - The C++ runtime. To obtain the C++ runtime, go to the IBM Technical Support Web site at the following URL:
https://techsupport.services.ibm.com

AIX 5.3

- **bos.rte.libc 5.3.0.0*** - This is required for Java 1.4 support.
- **xlC.rte 6.0.0.0*** - The C++ runtime.

*Go to the IBM Technical Support Web site at the following URL to obtain information about obtaining these file:
https://techsupport.services.ibm.com

On the Web page do the following:

1. Under the **Refine Your Search Section** select **Tools/Utilities** from the **Limit by Type** drop-down menu.
2. Select **AIX** from the **Limit by Platform or Operating System** drop-down menu.
3. Select **5.0** from the **Limit by Version** drop-down menu.
4. In the **Limit by Adding Search** terms field, type the following:
   `Download the VisualAge C++ for AIX V5 Runtime libraries`
5. Install the `xlC.rte` file set, not the .rte file for AIX 4.x.

Rolling Over the Logs

The logging information for the CIM Extension is contained primarily in the cxws.log file, created by default in the `<Installation_directory>/tools` directory. The cxws.log file rolls over once it

becomes more than 100 MB. The information in cxws.log is moved to cxws.log.1. When the logs roll over again, cxws.log.1 is renamed to cxws.log.2 and the information that is in cxws.log is moved to cxws.log.1. The numbering for the files continues sequentially, for example, cxws.log.3, with there being a maximum of three backup logs.

- cxws.log - contains the latest logging information
- cxws.log.1 - contains logging information that was previously in cxws.log
- cxws.log.2 - contains logging information that was previously in cxws.log.1
- cxws.log.3 - contains logging information that was previously in cxws.log.2

The cxws.out file contains some logging information, such as the CIM Extension starting, which is recorded in case something unexpected happens with the Java Virtual Machine. The CIM Extension appends the cxws.out file and rolls it over.

Removing the CIM Extension from AIX

Make sure **preview** is set to **No**. Refer to your documentation for AIX for more information.

To remove the CIM Extension for AIX:

1. Stop the CIM Extension as mentioned in “Stopping the CIM Extension” on page 171.
2. Type the following at the command prompt:
   ```
   # smit  -C
   ```
3. Select **Software Installation and Maintenance**.
4. Select **Software Maintenance and Utilities**.
5. Select **Remove Installed Software**.
6. In the SOFTWARE name, press Esc+4 and select:
   `APPQcime`
7. On the same page you selected `APPQcime`, select “No” for Preview by pressing the tab key.
8. Press ENTER to remove the software.

CHAPTER 7

Installing the CIM Extension for SGI ProPack for Linux

This chapter describes the following:

- About the CIM Extension for SGI ProPack for Linux on page 176
- Prerequisites on page 176
- Verifying SNIA HBA API Support on page 177
- Installing the CIM Extension on page 178
- Starting the CIM Extension on page 179
- How to Determine if the CIM Extension Is Running on page 181
- Configuring CIM Extensions on page 181
- Rolling Over the Logs on page 184
- Stopping the CIM Extension on page 185
- Removing the CIM Extension from SGI ProPack for Linux on page 185

Note: This chapter describes how to install and manage the CIM Extension directly on the host. You can also install and manage CIM Extensions remotely. See “Deploying and Managing CIM Extensions” on page 153.

Important: Make sure you have reviewed Table 1-1, “Roadmap for Installation and Initial Configurations,” on page 2 to ensure you are at the correct step.

About the CIM Extension for SGI ProPack for Linux

The CIM Extension for SGI ProPack for Linux gathers information from the operating system and host bus adapters on an Altix host. It then makes the information available to the management server.

Important: Install the CIM Extension on each host you want the management server to manage.

The CIM Extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBA API. For more information about the HBA API, see the following Web page at the SNIA Web Site: http://www.snia.org/tech_activities/hba_api/

Prerequisites

SGI ProPack for Linux

The CIM Extension authenticates using PAM (Pluggable Authentication Module) and the password encryption mechanisms listed below are supported:

- Blowfish
- DES
- MD5

Note: All ProPacks require that pam-devel rpm is installed.

Network Port Must Be Open

The CIM Extension uses port 4673 by default to communicate with the management server. Verify the network port is open. Refer to the documentation accompanying your Altix host for more information. If you need to use a different port, see “Permanently Changing the Port a CIM Extension Uses (UNIX Only)” on page 367.

Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. You can run the hbatest program, which is accessible from the CIM Extension CD-ROM. The program, hbatest, lists the name and number for all HBA's that support the SNIA HBA API. In some instances hbatest may report it cannot find an HBA driver even though an HBA driver is installed. Try installing a different version of the HBA driver that is SNIA compliant.

1. Go to the `Irix/tools` directory on the CIM Extension CD-ROM.
2. Enter the following at the command prompt:
   If the host is SGI ProPack3, enter the following at the command prompt:
   `./hbatest_PP3`.

   If the host is SGI ProPack 4 or later, enter the following at the command prompt:
   `./hbatest`

On SGI ProPack 3, the SGI-branded HBA API library for QLogic and LSI HBAs is built into the operating system kernel.

On SGI ProPack 4 and later, contact your vendor for the vendor specific HBA API library for LSI HBA. Discovery of ProPack4 hosts with QLogic HBA is not supported.

Installing the CIM Extension

Important: You must have root privileges to install this software.

You are provided several installation options. One is an interactive option, which lets you select the installation directory. Another is a silent installation, which installs with no user input. The silent installation assumes the default installation directory. Both options install on computers with or without X Windows.

To upgrade the CIM Extension, first remove the previous version before installing the latest version. Builds 4.0 and later of the CIM Extension are compatible with this build of the management server.

To install a CIM Extension on SGI ProPack for Linux:

1. Go to the /Altix directory on the CIM Extensions CD-ROM by entering the following at the command prompt:
   ```
   # cd /cdrom/Altix
   ```
   where /cdrom is the directory where you mounted the CD-ROM.
2. To install the software, do one of the following:

   Important: If you receive a message saying there is not enough room in the temp directory to perform the installation, set the IATEMPDIR variable to another directory. The installation uses this directory to extract the installation files. Refer to the documentation for your operating system for information on how to set this variable.

   - **Interactive Installation (Without X Windows or telnet terminal session)** - You must type -i console; otherwise, you are shown a NoClassDefFoundError message. Enter the following at the command prompt:
     ```
     # ./InstallCIMExtensions.bin –i console
     ```
   - **Interactive Installation (With X Windows)** - Enter the following at the command prompt:
     ```
     # ./InstallCIMExtensions.bin
     ```
   - **Silent Installation (X Windows not required)** - Enter the following at the command prompt. Then, go to Step 4. You cannot change the installation directory.
     ```
     # ./InstallCIMExtensions.bin –i silent
     ```

The CIM Extension is automatically installed in the `/opt/APPQcime` directory.

3. During the installation you are asked for the installation directory. Choose the default installation directory for best results.
4. Go to a directory other than one on the CD-ROM.
5. Unmount the CD-ROM by entering the following at the command prompt:
   `# umount /cdrom`
   where `/cdrom` is the name of the directory where you mounted the CD-ROM
6. Use `chkconfig --list appqcime` to verify the installation.
7. Start the CIM Extension. See “Starting the CIM Extension” on page 179.
   You must restart the CIM Extension after you have rebooted the server. This is because there is no support for /etc/rc scripts, which the CIM Extension uses to start.

Starting the CIM Extension

The management server can only obtain information from this host when the CIM Extension is running.

Keep in mind the following:

- You must have root privileges to run the CIM Extension. The CIM Extension only provides the information within the privileges of the user account that started the CIM Extension. Only root has enough privileges to provide the information the management server needs. If you do not start the CIM Extension with root privileges, the management server will display messages resembling the following: `Data is late or an error occurred.`
- To configure UNIX CIM Extensions to run behind a firewall, see “Configuring UNIX CIM Extensions to Run Behind Firewalls” on page 369.

To start the CIM Extension, type the following in the /opt/APPQcime/tools directory:

1. Before starting the CIM Extension, make sure PCP is enabled by executing the following command:
   `ps -ef | grep pmcd`
   This should display a message resembling the following:

```
root      2699     1  0 14:42 ?        00:00:00 /usr/share/pcp/bin/pmcd
root      2831  1988  0 14:44 pts/1    00:00:00 grep pmcd
```

   The first line above indicates that pmcd is running. If not, execute the following commands:

```
chkconfig pcp on
service pcp start
```

These commands start the pmcd daemon and also ensure the pmcd daemon starts whenever the system reboots.

2. To start the CIM Extension, type the following at the command prompt:

```
# ./start
```

The following is displayed:

```
./start
```

The CIM Extension is ready to be contacted by the management server when it displays a message resembling the following:

```
Thu Jan 21 14:46:47 EDT xxxx
CXWS x.x.x.x on /192.168.1.5 now accepting connections
where
.. xxxx is the year.
.. x.x.x.x is the version of CIM Extension
.. 192.168.1.5 is the IP address of the host
```

A similar message is now displayed in the cxws.out file when the CIM Extension has completed startup.

```
STATUS | wrapper  | 2006/07/10 15:44:26 | --> Wrapper Started as Daemon
STATUS | wrapper  | 2006/07/10 15:44:26 | Launching a JVM...
INFO   | jvm 1    | 2006/07/10 15:44:27 | Wrapper (Version 3.1.2) http://
wrapper.tanukisoftware.org
INFO   | jvm 1    | 2006/07/10 15:44:27 |
INFO   | jvm 1    | 2006/07/10 15:45:55 |
INFO   | jvm 1    | 2006/07/10 15:45:55 | Mon Jul 10 15:45:55 EDT 2006
INFO   | jvm 1    | 2006/07/10 15:45:55 | CXWS 5.1.0.169 on /
16.118.238.196:4673 now accepting connections
```

Keep in mind the following:

- Depending on your terminal type and processor speed, the message, "`CXWS x.x.x.x on /192.168.1.5 now accepting connections`," may not display all the network interface IPs on the host. Use the `/opt/APPQcime/tools/cxws.out` file to view the output from the CIM Extension.
- When you start the CIM Extension, you can restrict the user accounts that can discover the host. You can also change the port number the CIM Extension uses. See the following topics for more information. You can also access information about these topics by typing the following:

```
./start -help
```

How to Determine if the CIM Extension Is Running

You can determine if the CIM Extension is running by entering the following command at the command prompt:

```
# ./status
```

The CIM Extension is running when a message resembling the following is displayed:

```
CIM Extension Running
```

Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM Extension on start-up. The file is named `cim.extension.parameters` and is located in the `[Installation_Directory]/conf` directory on the host. This directory also contains a file named `cim.extension.parameters-sample`. This file contains samples of available parameters and can be copied into the `cim.extension.parameters` file and used as a template.

Changing the Port Number

The CIM Extension uses port 4673 by default. If the port is already used, follow these steps to change the port the CIM Extension will access:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:
   `-port 1234`
   where 1234 is the new port for the CIM Extension
3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

192.168.1.2:1234

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Configuring the CIM Extension to Listen on a Specific Network Card

Follow these steps to configure the CIM Extension to listen on a specific network card (NIC):

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:
   `-on 127.0.0.1,192.168.0.1`

   Note: If you want to configure the CIM Extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

The “-on” parameter may include a port specification. In that case, the CIM Extension listens on the indicated port of the indicated NIC, rather than the default port, for example:

```
-on 192.168.2.2:3456
```

The CIM Extension listens only on the NIC that has the IP address 192.168.2.2 on port 3456.

The management server assumes the CIM Extension is running on port 4673. The management server also listens on port 17000 for CIM Extensions from build 4.0.

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

192.168.1.2:1234

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file:

Table 7-1: Parameters for CIM Extensions

Parameter	Description
`-user`	The user defined in this parameter must be a valid user for the host. Only the user needs to be defined. The user name and password are provided from the management server during discovery. The user does not need to have root authority. A colon separated list can be used to specify multiple users.
`-credentials <username from the management server>:<password>`	The credentials defined by this parameter must match the values entered from the management server during discovery. They are not used as authentication on the host itself.
`-agentnic <ip address>`	Restricts the CIM Extension on multihomed systems to listen only on the designated IP address.
`-mgmtServerIP <ip address>`	Restricts the CIM Extension to listen only to a specific management server IP address.

Rolling Over the Logs

The logging information for the CIM Extension is contained primarily in the cxws.log file, created by default in the `<Installation_directory>/tools` directory. The cxws.log file rolls over once it becomes more than 100 MB. The information in cxws.log is moved to cxws.log.1. When the logs roll over again, cxws.log.1 is renamed to cxws.log.2 and the information that is in cxws.log is moved to cxws.log.1. The numbering for the files continues sequentially, for example, cxws.log.3, with there being a maximum of three backup logs.

- cxws.log - contains the latest logging information
- cxws.log.1 - contains logging information that was previously in cxws.log
- cxws.log.2 - contains logging information that was previously in cxws.log.1
- cxws.log.3 - contains logging information that was previously in cxws.log.2

The cxws.out file contains some logging information, such as the CIM Extension starting, which is recorded in case something unexpected happens with the Java Virtual Machine. The CIM Extension appends the cxws.out file and rolls it over.

Stopping the CIM Extension

To stop the background process for the CIM Extension, enter the following at the command prompt in the `/opt/APPQcime/tools` directory:

```
# ./stop
```

Keep in mind the following:

- You must have root privileges to stop the CIM Extension.
- When you stop the CIM Extension, the management server is unable to gather information about this host.

Removing the CIM Extension from SGI ProPack for Linux

To remove the CIM Extension for SGI ProPack for Linux:

1. Go to the following directory by entering the following at the command prompt:
   `# cd [InstallationDirectory]/Uninstall_CIMExtensions`
   where `InstallationDirectory` is the directory containing the CIM Extension
2. Remove the CIM Extension by entering the following at the command prompt:
   `# ./Uninstall_SGI_CIMExtensions`

CHAPTER 8

Installing the CIM Extension for HP-UX

This chapter describes the following:

- About the CIM Extension for HP-UX on page 188
- Prerequisites on page 188
- Verifying SNIA HBA API Support on page 190
- Installing the CIM Extension on page 191
- Starting the CIM Extension Manually on page 192
- How to Determine if the CIM Extension Is Running on page 193
- Configuring CIM Extensions on page 193
- Stopping the CIM Extension on page 198
- Rolling Over the Logs on page 199
- Fulfilling the Prerequisites on page 199
- Removing the CIM Extension from HP-UX on page 200

Note: This chapter describes how to install and manage the CIM Extension directly on the host. You can also install and manage CIM Extensions remotely. See “Deploying and Managing CIM Extensions” on page 153.

Important: Make sure you have reviewed Table 1-1, “Roadmap for Installation and Initial Configurations,” on page 2 to ensure you are at the correct step.

About the CIM Extension for HP-UX

The CIM Extension for HP-UX gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

Important: Install the CIM Extension on each host you want the management server to manage.

The CIM Extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBA API. For more information about the HBA API, see the following Web page at the SNIA Web site: http://www.snia.org/tech_activities/hba_api/

Prerequisites

The installation checks for the following. If the installation fails, see “Fulfilling the Prerequisites” on page 199.

HP-UX 11i and 11.0

Software Requirements

Following software driver bundles must be installed on HP-UX 11i and 11.0 hosts. FC SNIA HBA API software is bundled with the driver and is installed at the same time the driver is installed.

HP-UX 11i

Driver Bundle Version

B.11.11.09 PCI/HSC FibreChannel;Supptd HW=A6684A,A6685A,A5158A,A6795A (FibrChanl-00 Bundle).

This driver Bundle is automatically selected for installation with the HP-UX 11i Operating Environments.

Driver Version = @(#) PATCH_11.11: libtd.a : Jun 28 2002, 11:08:35, PHSS_26799 or later

Driver Patch

Tachyon Fibre Channel Driver Patch: PHKL_23626 or later (only for HP-UX 11i)

HP-UX 11.0

Driver Bundle Versions

B.11.00.10 PCI Tachyon TL/TS Fibre Channel (Bundle A5158A).

B.11.00.10 PCI Tachyon TL/TS/XL2 Fibre Channel (Bundle A6795A)

Driver Version = @(#) PATCH_11.00: libtd.a : Jul 15 2002, 11:34:12, PHSS_26798

Driver Patch

Tachyon Fibre Channel Driver Patch: PHKL_23939 or later (only for HP-UX 11.00)

Required Disk Space

The CIM Extension for HP-UX requires 105 MB.

Network Port Must Be Open

The CIM Extension uses port 4673 by default to communicate with the management server. Verify the network port is open. Refer to the documentation accompanying your HP-UX host for more information. If you need to use a different port, see “Permanently Changing the Port a CIM Extension Uses (UNIX Only)” on page 367.

Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. You can run the hbatest program, which is accessible from the CIM Extension CD-ROM. The program, hbatest, lists the name and number for all HBA’s *that support the SNIA HBA API.* In some instances hbatest may report it cannot find an HBA driver even though an HBA driver is installed. Try installing a different version of the HBA driver that is SNIA compliant.

To run hbatest:

1. Go to the `HPUX/tools` directory on the CIM Extension CD-ROM.
2. Enter the following at the command prompt: `./hbatest`
   The program runs its diagnostics.

HP SNIA Adapters AXXXXA comes from fileset FC-FCD, FC-TACHYON-TL. Unless separated purposely during installing the operating system, filesets are there by default. To view the location of the library, enter the following at the command prompt:

```
# more /etc/hba.conf
```

The following is displayed:

```
com.hp.fcms32 /usr/lib/libhbaapihp.sl #32 bit lib names end in '32'
com.hp.fcms64 /usr/lib/pa20_64/libhbaapihp.sl #64 bit lib names end in
'64'
```

- com.hp.fcd32 /usr/lib/libhbaapifcd.sl
- com.hp.fcd64 /usr/lib/pa20_64/libhbaapifcd.sl

Installing the CIM Extension

Keep in mind the following:

- The instructions in this section apply if you are doing a local installation of the CIM Extension, as compared to a scripted or push installation. If you want to perform a scripted or push installation of the CIM Extension, first install the CIM Extension locally by using the instructions in this section. Then, perform the scripted or push installation. The instructions in this section only need to be performed once if you are doing a scripted or push installation. Contact customer support for information about performing a scripted or push installation.
- To upgrade the CIM Extension, first remove the previous version before installing the latest version. Builds 4.0 and later of the CIM Extension are compatible with this build of the management server.
- You must install the CIM Extension for HP-UX to the default directory.

To install the CIM Extension using CLI:

1. Login as root.
2. Place CIM Extension CD-ROM into the CD-ROM on HP-UX server.
3. Create the `/cdrom` directory on HP-UX host by entering the following at the command prompt:
   ```
   # mkdir /cdrom
   ```
4. Mount the CIM Extension CD-ROM by enter the following at the command prompt:
   ```
   # mount /dev/dsk/c#t#d#  /cdrom
   ```

where c, t and d numbers correspond to CD-ROM device numbers

To find out `c#t#d#` of your CD-ROM, run "`ioscan -fnC disk`" command on the HP-UX host.

5. To install the CIM Extension, enter the following at the command prompt:
   ```
   # swinstall -s /cdrom/HPUX/APPQcime.depot APPQcime
   ```
   The installation is complete when you are told the "`analysis and execution succeeded`."
6. Eject/unload the CD-ROM by unmounting the CD-ROM and pressing eject/unload button on the CD-ROM drive:
   ```
   # umount /cdrom
   ```
   where `/cdrom` is the name of the directory where you mounted the CD-ROM
7. Press the Eject button on the CD-ROM drive to take the CD out of the CD-ROM drive. The CIM Extension for HP-UX starts automatically at boot time by using `/sbin/rc2.d` scripts. The CIM Extension uses port 4673 when it starts automatically after a reboot. Type the following at the command prompt to find the status of the CIM Extension: `./status`

Starting the CIM Extension Manually

The management server can only obtain information from this host when the CIM Extension is running.

Keep in mind the following:

- You must have root privileges to run the CIM Extension. The CIM Extension only provides the information within the privileges of the user account that started the CIM Extension. Only root has enough privileges to provide the information the management server needs. If you do not start the CIM Extension with root privileges, the management server will display messages resembling the following: Data is late or an error occurred.
- To configure UNIX CIM Extensions to run behind a firewall, see "Configuring UNIX CIM Extensions to Run Behind Firewalls" on page 369.

To start the CIM Extension, type the following in the `/opt/APPQcime/tools` directory, where `/opt` is the directory into which you installed the CIM Extension:

```
# ./start
```

The following is displayed:

```
Starting CIM Extension for HP-UX...
```

Keep in mind the following:

- When you start the CIM Extension, you can restrict the user accounts that can discover the host. You can also change the port number the CIM Extension uses. See the following topics for more information. You can also access information about these topics by typing the following:
  `./start -help`

How to Determine if the CIM Extension Is Running

You can determine if the CIM Extension is running by entering the following command at the command prompt:

```
# ./status
```

The CIM Extension is running when the following message is displayed:

```
CIM Extension Running: Process ID: 93
```

where 93 is the process ID running the CIM Extension

Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM Extension on start-up. The file is named `cim.extension.parameters` and is located in the `[Installation_Directory]/conf` directory on the host. This directory also contains a file named `cim.extension.parameters-sample`. This file contains samples of available parameters and can be copied into the `cim.extension.parameters` file and used as a template.

Restricting the Users Who Can Discover the Host

The `-users` parameter provides greater security by restricting access. When you use the management server to discover the host, provide a user name that was specified in the `-users` parameter.

For example, assume you want to use the management server to discover a HP-UX host, but you do not want to provide the password to the root account. You can provide the password to another valid HP-UX user account that has less privileges, for example jsmythe. First, you would add the user to the parameters file. You would then logon to the management server, access the Discovery page, and provide the user name and password for jsmythe. Only the user name and password for jsmythe can be used to discover the HP-UX host.

Follow these steps to add a user to the parameters file:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:
   `-users myname`
   where myname is a valid HP-UX user name.

   Note: You can provide multiple users by separating them with a colon. For example `-users myname:jsymthe`.

3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

   Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

Changing the Port Number

The CIM Extension uses port 4673 by default. If the port is already used, follow these steps to change the port the CIM Extension will access:

1. Go to the `[Installation_Directory]/conf` directory.

2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:
   `-port 1234`
   where 1234 is the new port for the CIM Extension
3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

192.168.1.2:1234

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Configuring the CIM Extension to Listen on a Specific Network Card

Follow these steps to configure the CIM Extension to listen on a specific network card (NIC):

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:
   `-on 127.0.0.1,192.168.0.1`

   Note: If you want to configure the CIM Extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

   Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

The “-on” parameter may include a port specification. In that case, the CIM Extension listens on the indicated port of the indicated NIC, rather than the default port, for example:

```
-on 192.168.2.2:3456
```

The CIM Extension listens only on the NIC that has the IP address 192.168.2.2 on port 3456.

The management server assumes the CIM Extension is running on port 4673. The management server also listens on port 17000 for CIM Extensions from build 4.0.

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP

Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

192.168.1.2:1234

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file:

Table 8-1: Parameters for CIM Extensions

Parameter	Description
`-user`	The user defined in this parameter must be a valid user for the host. Only the user needs to be defined. The user name and password are provided from the management server during discovery. The user does not need to have root authority. A colon separated list can be used to specify multiple users.
`-credentials <username from the management server>:<password>`	The credentials defined by this parameter must match the values entered from the management server during discovery. They are not used as authentication on the host itself.
`-agentnic <ip address>`	Restricts the CIM Extension on multihomed systems to listen only on the designated IP address.
`-mgmtServerIP <ip address>`	Restricts the CIM Extension to listen only to a specific management server IP address.

Finding the Version of a CIM Extension

You can find the version number of a CIM Extension:

1. Go to the `/opt/APPQcime/tools` directory.
2. Type the following at the command prompt:
   `# ./start -version`
   You are shown the version number of the CIM Extension and the date it was built, as shown in the following example:

   ```
   Starting CIM Extension for HP-UX
   CXWS for mof/cxws/cxws-HPUX.mof
   CXWS version x.x.x.x, built on Fri 12-March-xxxx 12:29:49 by dmaltz
   ```

   where

   - `xxxx is the year.`
   - x.x.x.x is the version of the CIM Extension

Combining Start Commands

You can also combine the -users and -port commands as follows:

```
./start -users myname -port 1234
```

or

```
./start -port 1234 -users myname
```

where

- `myname` is the user name that must be used to discover this HP-UX host
- `1234` is the new port

Stopping the CIM Extension

To stop the CIM Extension, enter the following at the command prompt in the `/opt/APPQcime/tools` directory, where `/opt` is the directory into which you installed the CIM Extension:

```
# ./stop
```

Keep in mind the following:

- You must have root privileges to stop the CIM Extension.
- When you stop the CIM Extension, the management server is unable to gather information about this host.

Rolling Over the Logs

The logging information for the CIM Extension is contained primarily in the cxws.log file, created by default in the `<Installation_directory>/tools` directory. The cxws.log file rolls over once it becomes more than 100 MB. The information in cxws.log is moved to cxws.log.1. When the logs roll over again, cxws.log.1 is renamed to cxws.log.2 and the information that is in cxws.log is moved to cxws.log.1. The numbering for the files continues sequentially, for example, cxws.log.3, with there being a maximum of three backup logs.

- cxws.log - contains the latest logging information
- cxws.log.1 - contains logging information that was previously in cxws.log
- cxws.log.2 - contains logging information that was previously in cxws.log.1
- cxws.log.3 - contains logging information that was previously in cxws.log.2

The cxws.out file contains some logging information, such as the CIM Extension starting, which is recorded in case something unexpected happens with the Java Virtual Machine. The CIM Extension appends the cxws.out file and rolls it over.

Fulfilling the Prerequisites

Use the commands mentioned in this section to determine if you have the required software.

To verify driver bundle version, enter the following at the command prompt:

```
# swlist
```

To verify installed patches, enter the following at the command prompt:

```
# show_patches
```

To find the HBA driver version, after HBA software bundles are installed and patches applied to the operating system, enter the following at the command prompt:

```
# fcmsutil /dev/td0
```

If host has more than one HBA, enter the following at the command prompt:

```
# fcmsutil /dev/td1
```

Number in `td#` corresponds to the HBA number.

Removing the CIM Extension from HP-UX

To remove the CIM Extension for HP-UX as root:

1. Login as root.
2. Stop the CIM Extension, as described in “Stopping the CIM Extension” on page 198.
3. Make sure you are not in the APPQcime directory. As a precaution, go to the root directory.
4. Enter the following at the command prompt:
   ```
   # swremove APPQcime
   ```
   When you see the following message, the CIM Extension has been removed:
   ```
   * Beginning Execution
   * The execution phase succeeded for hpuxqaX.dnsxxx.com:/".
   * Execution succeeded..
   ```
5. To remove the APPQcime directory, enter the following at the command prompt:
   ```
   # rm -r APPQcime
   ```

CHAPTER 9

Installing the CIM Extension for SGI IRIX

This chapter describes the following:

- About the CIM Extension for SGI IRIX on page 202
- Prerequisites on page 202
- Verifying SNIA HBA API Support on page 203
- Installing the CIM Extension on page 203
- Starting the CIM Extension on page 204
- How to Determine if the CIM Extension Is Running on page 205
- Configuring CIM Extensions on page 205
- Stopping the CIM Extension on page 209
- Rolling Over the Logs on page 210
- Removing the CIM Extension from SGI IRIX on page 210

Note: This chapter describes how to install and manage the CIM Extension directly on the host. You can also install and manage CIM Extensions remotely. See “Deploying and Managing CIM Extensions” on page 153.

Important: Make sure you have reviewed Table 1-1, “Roadmap for Installation and Initial Configurations,” on page 2 to ensure you are at the correct step.

About the CIM Extension for SGI IRIX

The CIM Extension for SGI IRIX gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

Important: Install the CIM Extension on each host you want the management server to manage.

The CIM Extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBA API. For more information about the HBA API, see the following Web page at the SNIA Web Site: http://www.snia.org/tech_activities/hba_api/

Prerequisites

The installation requires the SGI Origin system and 120 MB of disk space. It also requires one of the following operating systems:

- IRIX version 6.5.22, limited to internal processors 27 and 35
- IRIX version 6.5.20, path required. Contact customer support for the patch.

Network Port Must Be Open

The CIM Extension uses port 4673 by default to communicate with the management server. Verify the network port is open. Refer to the documentation accompanying your IRIX host for more

information. If you need to use a different port, see “Permanently Changing the Port a CIM Extension Uses (UNIX Only)” on page 367.

Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. You can run the hbatest program, which is accessible from the CIM Extension CD-ROM. The program, hbatest, lists the name and number for all HBA's that support the SNIA HBA API. In some instances hbatest may report it cannot find an HBA driver even though an HBA driver is installed. Try installing a different version of the HBA driver that is SNIA compliant.

1. Go to the `Irix/tools` directory on the CIM Extension CD-ROM.
2. Enter the following at the command prompt: `./hbatest`
   The program runs its diagnostics.

SGI Branded QLogic SNIA Adapters are built into the operating system kernel starting with IRIX 6.5.22 and later. To find the library, enter the following at the command prompt:

```
# ls
```

The following is displayed:

```
/usr/include/sys/hba_api.h
```

Installing the CIM Extension

Important: To upgrade the CIM Extension, first remove the previous version before installing the latest version. Builds 4.0 and later of the CIM Extension are compatible with this build of the management server.

To install the CIM Extension for IRIX:

1. Insert the CIM Extensions CD-ROM into the CD-ROM drive.

2. Go to the CD-ROM by entering the following at the command prompt:
   `cd /CDROM`
3. Enter the following at the command prompt:
   `inst`
4. Enter the following at the Inst command prompt:
   `Inst> open`
5. When you are asked for the location of the installation, enter the following:
   `Inst> /CDROM/Irix`
6. Enter the following:
   `Inst> install`
7. When asked which subsystem, enter the following:
   `APPQcime`
8. To begin the installation, enter the following:
   `Inst> go`
   The IRIX CIM Extension is installed in the `/opt/APPQcime` directory.
9. Enter the following to restart the ELF files and to exit the installation program:
   `Inst> quit`
   You must start the CIM Extension for the management server to obtain information about the host. See “Starting the CIM Extension” on page 204

Starting the CIM Extension

The management server can only obtain information from this host when the CIM Extension is running.

Keep in mind the following:

- You must have root privileges to run the CIM Extension. The CIM Extension only provides the information within the privileges of the user account that started the CIM Extension. Only root has enough privileges to provide the information the management server needs. If you do not start the CIM Extension with root privileges, the management server will display messages resembling the following: `Data is late or an error occurred.`
- To configure UNIX CIM Extensions to run behind a firewall, see “Configuring UNIX CIM Extensions to Run Behind Firewalls” on page 369.

To start the CIM Extension, type the following in the `/opt/APPQcime/tools` directory:

```
# ./start
```

The following is displayed:

```
Starting CIM Extension for IRIX...
```

How to Determine if the CIM Extension Is Running

You can determine if the CIM Extension is running by entering the following command at the command prompt:

```
# ./status
```

The CIM Extension is running when a message resembling the following is displayed:

```
CIM Extension Running
```

Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM Extension on start-up. The file is named `cim.extension.parameters` and is located in the `[Installation_Directory]/conf` directory on the host. This directory also contains a file named `cim.extension.parameters-sample`. This file contains samples of available parameters and can be copied into the `cim.extension.parameters` file and used as a template.

Changing the Port Number

The CIM Extension uses port 4673 by default. If the port is already used, follow these steps to change the port the CIM Extension will access:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:

```
-port 1234
```

where 1234 is the new port for the CIM Extension

3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

192.168.1.2:1234

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Configuring the CIM Extension to Listen on a Specific Network Card

Follow these steps to configure the CIM Extension to listen on a specific network card (NIC):

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:
   ```
   -on 127.0.0.1,192.168.0.1
   ```

Note: If you want to configure the CIM Extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

The “-on” parameter may include a port specification. In that case, the CIM Extension listens on the indicated port of the indicated NIC, rather than the default port, for example:

```
-on 192.168.2.2:3456
```

The CIM Extension listens only on the NIC that has the IP address 192.168.2.2 on port 3456.

The management server assumes the CIM Extension is running on port 4673. The management server also listens on port 17000 for CIM Extensions from build 4.0.

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

192.168.1.2:1234

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file:

Table 9-1: Parameters for CIM Extensions

Parameter	Description
`-user`	The user defined in this parameter must be a valid user for the host. Only the user needs to be defined. The user name and password are provided from the management server during discovery. The user does not need to have root authority. A colon separated list can be used to specify multiple users.
`-credentials <username from the management server>:<password>`	The credentials defined by this parameter must match the values entered from the management server during discovery. They are not used as authentication on the host itself.
`-agentnic <ip address>`	Restricts the CIM Extension on multihomed systems to listen only on the designated IP address.
`-mgmtServerIP <ip address>`	Restricts the CIM Extension to listen only to a specific management server IP address.

Starting the CIM Extension by chkconfig

After installation, appqcime chkconfig is on by default. This means the appqcime service starts automatically after the host is rebooted. The appqcime service must be running for the management server to obtain information about the host. You can disable the appqcime service so that it does not start automatically after a reboot.

Note: You can only disable appqcime from starting automatically after a reboot if you are at run level 2.

To check the appqcime chkconfig status, enter the following at the command prompt:

```
# chkconfig | grep appqcime
```

If appqcime is capable of starting after a reboot, it is shown to be on, as displayed in the following output:

```
appqcime              on
```

To disable appqcime from starting after a reboot, enter the following at the command prompt:

```
# chkconfig appcime off
```

If you have disabled the automatic start-up of appqcime and you want to enable appqcime so it will start after a reboot, enter the following at the command prompt:

```
# chkconfig appqcime on
```

Finding the Version of a CIM Extension

You can find the version number of a CIM Extension:

1. Go to the `/opt/APPQcime/tools` directory.
2. Type the following at the command prompt:
   ```
   # ./start -version
   ```
   You are shown the version number of the CIM Extension and the date it was built, as shown in the following example:
   ```
   CXWS for mof/cxws/cxws-irix.mof
   CXWS version x.x.x.x, built on Fri 12-March-xxxx 12:29:49 by dmaltz
   ```
   where
   - x.x.x.x is the version of the CIM Extension
   - `xxxx is the year.`

Stopping the CIM Extension

To stop the background process for the CIM Extension, enter the following at the command prompt in the `/opt/APPQcime/tools` directory:

```
# ./stop
```

Keep in mind the following:

- You must have root privileges to stop the CIM Extension.
- When you stop the CIM Extension, the management server is unable to gather information about this host.

Rolling Over the Logs

The logging information for the CIM Extension is contained primarily in the cxws.log file, created by default in the `<Installation_directory>/tools` directory. The cxws.log file rolls over once it becomes more than 100 MB. The information in cxws.log is moved to cxws.log.1. When the logs roll over again, cxws.log.1 is renamed to cxws.log.2 and the information that is in cxws.log is moved to cxws.log.1. The numbering for the files continues sequentially, for example, cxws.log.3, with there being a maximum of three backup logs.

- cxws.log - contains the latest logging information
- cxws.log.1 - contains logging information that was previously in cxws.log
- cxws.log.2 - contains logging information that was previously in cxws.log.1
- cxws.log.3 - contains logging information that was previously in cxws.log.2

The cxws.out file contains some logging information, such as the CIM Extension starting, which is recorded in case something unexpected happens with the Java Virtual Machine. The CIM Extension appends the cxws.out file and rolls it over.

Removing the CIM Extension from SGI IRIX

To remove the CIM Extension for IRIX:

1. Stop the CIM Extension as mentioned in “Stopping the CIM Extension” on page 209.
2. Enter the following at the command prompt:

```
inst
```

3. Enter the following at the Inst command prompt:
   ```
   Inst> remove
   ```
4. When you are asked which subsystem you want to remove, enter the following:
   ```
   APPQcime
   ```
5. To begin the removal of the CIM Extension, enter the following at the Inst command prompt:
   ```
   Inst> go
   ```
   The CIM Extension is removed from IRIX.
6. To exit the Inst Main Menu, enter the following:
   ```
   Inst> quit
   ```

CHAPTER 10

Installing the CIM Extension for SUSE and Red Hat Linux

This chapter describes the following:

- About the CIM Extension for Red Hat Linux Advanced Server and SUSE Linux on page 214
- Prerequisites on page 214
- Verifying SNIA HBA API Support on page 215
- Installing the CIM Extension on page 217
- Starting the CIM Extension Manually on page 217
- How to Determine if the CIM Extension Is Running on page 218
- Configuring CIM Extensions on page 219
- Stopping the CIM Extension on page 222
- Rolling Over the Logs on page 222
- Removing the CIM Extension from Red Hat or SUSE Linux on page 223

Note: This chapter describes how to install and manage the CIM Extension directly on the host. You can also install and manage CIM Extensions remotely. See “Deploying and Managing CIM Extensions” on page 153.

Important: Make sure you have reviewed the table, Table 1-1, “Roadmap for Installation and Initial Configurations,” on page 2 in the Overview chapter to ensure you are at the correct step.

About the CIM Extension for Red Hat Linux Advanced Server and SUSE Linux

The CIM Extension for Red Hat and SUSE Linux gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

Important: Install the CIM Extension on each host you want the management server to manage.

The CIM Extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBA API. For more information about the HBA API, see the following Web page at the SNIA Web site:

http://www.snia.org/tech_activities/hba_api/

Prerequisites

Red Hat Linux Advanced Server 3.0 Update 2
(may just be i386.rpm on certain customer configurations)
requires glibc-2.3.2-95.20.i686.rpm (update2 CD2)
requires laus-0.1-54RHEL3.i386.rpm (update2 CD2)
requires compat-libstdc++-7.3-2.96.128.i386.rpm (update2 CD3)

requires libgcc-3.2.3-34.i386.rpm (update2 CD2)

Red Hat Linux Advanced Server 2.1 Update 4
(may just be i386.rpm on certain customer configurations)
requires glibc-2.2.4-32.15.i686.rpm (update4 CD1)
requires compat-libstdc++-6.2-2.9.0.16.i386.rpm (update4 CD1)

SUSE 8
compat-2003.1.10-0

SUSE 9
compat-2004.7.1-1.2

Required Disk Space

75 MB

Network Port Must Be Open

The CIM Extension uses port 4673 by default to communicate with the management server. Verify the network port is open. Refer to the documentation accompanying your Linux host for more information. If you need to use a different port, see “Permanently Changing the Port a CIM Extension Uses (UNIX Only)” on page 367.

Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. You can run the hbatest program, which is accessible from the CIM Extension CD-ROM. The program, hbatest, lists the name and number for all HBA's that support the SNIA HBA API.

To run hbatest:

1. Go to the `linux/tools` directory on the CIM Extension CD-ROM.
2. Enter the following at the command prompt: `./hbatest`
   The program runs its diagnostics.

Driver Information for Verifying SNIA Emulex Adapters on Red Hat Linux

Emulex Adapters SNIA comes from package HBAnyware. To view the library location, enter the following at the command prompt:

```
# more /etc/hba.conf
```

The following is displayed:

```
com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so
```

Driver Information for Verifying QLogic SNIA Adapters on Red Hat Linux

QLogic SNIA Adapters comes from package qlapi-vX.XXX-rel.tgz found in the QLogic driver. The adapters are installed separately after driver. To view the location of the library, enter the following at the command prompt:

```
# more /etc/hba.conf
```

The following is displayed:

```
qla2x00 /usr/lib/libqlsdm.so
```

Driver Information for Verifying QLogic SNIA Adapters on SUSE Linux

QLogic SNIA Adapters comes from package qlapi-vX.XXX-rel.tgz found in the QLogic driver. The adapters are installed separately after driver. To view the location of the library, enter the following at the command prompt:

```
# more /etc/hba.conf
```

The following is displayed:

```
qla2x00 /usr/lib/libqlsdm.so
```

Installing the CIM Extension

Keep in mind the following:

- The instructions in this section apply if you are doing a local installation of the CIM Extension, as compared to a scripted or push installation. If you want to perform a scripted or push installation of the CIM Extension, first install the CIM Extension locally by using the instructions in this section. Then, perform the scripted or push installation. The instructions in this section only need to be performed once if you are doing a scripted or push installation. Contact customer support for information about performing a scripted or push installation.
- To upgrade the CIM Extension, first remove the previous version before installing the latest version. Builds 4.0 and later of the CIM Extension are compatible with this build of the management server.

To install the CIM Extension:

1. Login as root.
2. Go to the Linux directory on the CIM Extension CD-ROM by entering the following at the command prompt:
   ```
   # cd /cdrom/linux
   ```
   where `/cdrom` is the name of the CD-ROM drive
3. Enter one of the following at the command prompt:
   - **For 64-bit Linux Itanium Servers**:
     ```
     # rpm -idvh APPQcimeIa64.rpm
     ```
   - **For all other servers**:
     ```
     # rpm -idvh APPQcime.rpm
     ```
   The installation is done when you are returned to the command prompt.

Starting the CIM Extension Manually

The management server can only obtain information from this host when the CIM Extension is running.

Keep in mind the following:

- You must have root privileges to run the CIM Extension. The CIM Extension only provides the information within the privileges of the user account that started the CIM Extension. Only root has enough privileges to provide the information the management server needs. If you do not start the CIM Extension with root privileges, the management server will display messages resembling the following: `Data is late or an error occurred.`
- To configure UNIX CIM Extensions to run behind a firewall, see “Configuring UNIX CIM Extensions to Run Behind Firewalls” on page 369.

To start the CIM Extension, type the following in the /opt/APPQcime/tools directory, where /opt is the directory into which you installed the CIM Extension:

```
# ./start
```

The following is displayed:

```
Starting CIM Extension for LINUX...
```

Keep in mind the following:

- When you start the CIM Extension, you can change the port number the CIM Extension uses. See “Configuring CIM Extensions” on page 219 for more information.

How to Determine if the CIM Extension Is Running

You can determine if the CIM Extension is running by entering the following command at the command prompt:

```
# ./status
```

The CIM Extension is running when the following message is displayed:

```
CIM Extension Running: Process ID: 93
```

where 93 is the process ID running the CIM Extension

Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM Extension on start-up. The file is named `cim.extension.parameters` and is located in the `[Installation_Directory]/conf` directory on the host. This directory also contains a file named `cim.extension.parameters-sample`. This file contains samples of available parameters and can be copied into the `cim.extension.parameters` file and used as a template.

Changing the Port Number

The CIM Extension uses port 4673 by default. If the port is already used, follow these steps to change the port the CIM Extension will access:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:
   `-port 1234`
   where 1234 is the new port for the CIM Extension
3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

192.168.1.2:1234

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Configuring the CIM Extension to Listen on a Specific Network Card

Follow these steps to configure the CIM Extension to listen on a specific network card (NIC):

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:
   `-on 127.0.0.1,192.168.0.1`

   Note: If you want to configure the CIM Extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

   Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

The “-on” parameter may include a port specification. In that case, the CIM Extension listens on the indicated port of the indicated NIC, rather than the default port, for example:

```
-on 192.168.2.2:3456
```

The CIM Extension listens only on the NIC that has the IP address 192.168.2.2 on port 3456.

The management server assumes the CIM Extension is running on port 4673. The management server also listens on port 17000 for CIM Extensions from build 4.0.

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP

Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

192.168.1.2:1234

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file:

Table 10-1: Parameters for CIM Extensions

Parameter	Description
`-user`	The user defined in this parameter must be a valid user for the host. Only the user needs to be defined. The user name and password are provided from the management server during discovery. The user does not need to have root authority. A colon separated list can be used to specify multiple users.
`-credentials <username from the management server>:<password>`	The credentials defined by this parameter must match the values entered from the management server during discovery. They are not used as authentication on the host itself.
`-agentnic <ip address>`	Restricts the CIM Extension on multihomed systems to listen only on the designated IP address.
`-mgmtServerIP <ip address>`	Restricts the CIM Extension to listen only to a specific management server IP address.

Finding the Version of a CIM Extension

You can find the version number of a CIM Extension:

1. Go to the `/opt/APPQcime/tools` directory.
2. Type the following at the command prompt:
   `# ./start -version`

You are shown the version number of the CIM Extension and the date it was built, as shown in the following example:

```
CXWS for mof/cxws/cxws-linux.mof
CXWS version 3.6.0.39, built on Thu 7-October-2004 03:05:44 by dmaltz
```

Stopping the CIM Extension

To stop the CIM Extension, enter the following at the command prompt in the `/opt/APPQcime/tools` directory, where `/opt` is the directory into which you installed the CIM Extension:

```
#  ./stop
```

Keep in mind the following:

- You must have root privileges to stop the CIM Extension.
- When you stop the CIM Extension, the management server is unable to gather information about this host.

Rolling Over the Logs

The logging information for the CIM Extension is contained primarily in the cxws.log file, created by default in the `<Installation_directory>/tools` directory.The cxws.log file rolls over once it becomes more than 100 MB. The information in cxws.log is moved to cxws.log.1. When the logs roll over again, cxws.log.1 is renamed to cxws.log.2 and the information that is in cxws.log is moved to

cxws.log.1. The numbering for the files continues sequentially, for example, cxws.log.3, with there being a maximum of three backup logs.

- cxws.log - contains the latest logging information
- cxws.log.1 - contains logging information that was previously in cxws.log
- cxws.log.2 - contains logging information that was previously in cxws.log.1
- cxws.log.3 - contains logging information that was previously in cxws.log.2

The cxws.out file contains some logging information, such as the CIM Extension starting, which is recorded in case something unexpected happens with the Java Virtual Machine. The CIM Extension appends the cxws.out file and rolls it over.

Removing the CIM Extension from Red Hat or SUSE Linux

To remove the CIM Extension for Red Hat or SUSE Linux as root:

1. Login as root.
2. Stop the CIM Extension, as described in the topic, “Stopping the CIM Extension” on page 222.
3. Enter the following at the command prompt:

   ```
   # rpm -e APPQcime
   ```

   The removal of the CIM Extension is complete, when you are returned to the command prompt.

CHAPTER 11

Installing the CIM Extension for Sun Solaris

This chapter describes the following:

- About the CIM Extension for Solaris on page 226
- Prerequisites on page 226
- Verifying SNIA HBA API Support on page 227
- Installing the CIM Extension on page 229
- Starting the CIM Extension Manually on page 230
- How to Determine if the CIM Extension Is Running on page 231
- Configuring CIM Extensions on page 231
- Stopping the CIM Extension on page 236
- Rolling Over the Logs on page 236
- Removing the CIM Extension from Solaris on page 237

Note: This chapter describes how to install and manage the CIM Extension directly on the host. You can also install and manage CIM Extensions remotely. See “Deploying and Managing CIM Extensions” on page 153.

Important: Make sure you have reviewed Table 1-1, “Roadmap for Installation and Initial Configurations,” on page 2 to ensure you are at the correct step.

About the CIM Extension for Solaris

The CIM Extension for Sun Solaris gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

Important: Install the CIM Extension on each host you want the management server to manage.

The CIM Extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBAAPI. For more information about the HBAAPI, see the following Web page at the SNIA Web site: http://www.snia.org/tech_activities/hba_api/

Prerequisites

The management server requires certain packages and patches. The installation checks for the required packages listed in the following section and verifies that Solaris 8 has been installed.

You need the core set SUNWCreq. If you have only the core environment packages installed, install the following manually in the **exact** order:

1. SUNWlibC - Sun Workshop Compilers Bundled libC
2. SUNWlibCf - SunSoft WorkShop Bundled libC (cfront version)
3. SUNWlibCx - Sun Workshop Bundled 64-bit libC

Important: Verify you have the latest patches installed. The patches can be obtained from the Sun Microsystems Web site at http://www.sun.com.

You must have the following space:

- **CIM Extension** - The CIM Extension requires 90 MB of disk space.
- **Logs** - Make sure you have 100 MB for log files.
- **File SRM** - If you plan to have File SRM scan this host, make sure you have 220 to 230 MB for each set of 1 million files.

Network Port Must Be Open

The CIM Extension uses port 4673 by default to communicate with the management server. Verify the network port is open. Refer to the documentation accompanying your Sun Solaris host for more information. If you need to use a different port, see “Permanently Changing the Port a CIM Extension Uses (UNIX Only)” on page 367.

Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. You can run the hbatest program, which is accessible from the CIM Extension CD-ROM. The program, hbatest, lists the name and number for all HBA's that support the SNIA HBA API. In some instances hbatest may report it cannot find an HBA driver even though an HBA driver is installed. Try installing a different version of the HBA driver that is SNIA compliant.

Important: (QLogic host bus adapters only) For Solaris SAN Foundation Suite, the firmware version reported on the HBA is not the same as what is reported using luxadm. The management server uses the result of the HBAAPI, while luxadm displays different values.

To run hbatest:

1. Go to the `Solaris/tools` directory on the CIM Extension CD-ROM.

2. Enter the following at the command prompt: `./hbatest`
   The program runs its diagnostics.

Driver Information for Verifying SNIA Emulex Adapters

The SNIA Library comes from a separate package HBAnyware. If you installed SNIA Emulex adapter, you can find its library by entering the following at the command prompt:

```
# more /etc/hba.conf
```

The following is displayed:

```
com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so
com.emulex.emulexapilibrary /usr/lib/sparcv9/libemulexhbaapi.so
```

Driver Information for QLogic Adapters

The SNIA HBA package comes from a separate package QLSDMLIB. If you installed the QLogic Adapter, you can find its library by entering the following at the command prompt:

```
# more /etc/hba.conf
```

The following is displayed:

```
qla2x00         /usr/lib/libqlsdm.so
```

Driver Information for AMCC/JNI Adapters

The SNIA HBA driver for AMCC/JNI adapters comes from a separate package JNIsnia. You can find its library by entering the following at the command prompt:

```
# more /etc/hba.conf
```

The following is displayed:

```
JniHbaLib /opt/JNIsnia/Solaris/Jni/32bit/JniHbaLib.so
JniHbaLib /opt/JNIsnia/Solaris/Jni/64bit/JniHbaLib.so
```

Driver Information for Sun Leadville branded QLogic or JNI Adapters

The SNIA HBA comes from the Sun StorEdge SAN Foundation Suite. Package SUNWfchba installed as part of suite. You can find its library by entering the following at the command prompt:

```
# more /etc/hba.conf
```

The following is displayed:

```
com.sun.fchba           /usr/lib/libsun_fc.so.1
com.sun.fchba64         /usr/lib/sparcv9/libsun_fc.so.1
```

Installing the CIM Extension

Keep in mind the following:

- The instructions in this section apply if you are doing a local installation of the CIM Extension, as compared to a scripted or push installation. If you want to perform a scripted or push installation of the CIM Extension, first install the CIM Extension locally by using the instructions in this section. Then, perform the scripted or push installation. The instructions in this section only need to be performed once if you are doing a scripted or push installation. Contact customer support for information about performing a scripted or push installation.
- The server must be running sh, ksh or bash shell. C shell is not supported.
- To upgrade the CIM Extension, first remove the previous version before installing the latest version. Builds 4.0 and later of the CIM Extension are compatible with this build of the management server.

To install the CIM Extension:

1. Login as root.
2. Go to the Solaris directory on the CIM Extension CD-ROM by entering the following at the command prompt:
   ```
   # cd /cdrom/cdrom0/Solaris
   ```
   where /cdrom/cdrom0 is the name of the CD-ROM drive
3. Enter the following at the command prompt:
   ```
   # pkgadd -d APPQcime.pkg APPQcime
   ```

The APPQcime package is added.

4. When you are asked for an installation directory, enter the path to the directory into which you want to install the CIM Extension.
   If you want to install the CIM Extension into the default directory (/opt), press ENTER.
5. When you are asked if you want to continue the installation, enter **y**.
   The CIM Extension is installed.
6. When you are asked if you want to add another package, enter **q** to quit the installation.
7. If you see error messages when you install the CIM Extension, see “Removing the CIM Extension from Solaris” on page 237.
8. Unmount the CD-ROM by entering the following at the command prompt:
   `# umount /cdrom`
   where `/cdrom` is the name of the directory where you mounted the CD-ROM
9. Start the CIM Extension. See “Starting the CIM Extension Manually” on page 230.

Starting the CIM Extension Manually

The management server can only obtain information from this host when the CIM Extension is running.

Keep in mind the following:

- You must have root privileges to run the CIM Extension. The CIM Extension only provides the information within the privileges of the user account that started the CIM Extension. Only root has enough privileges to provide the information the management server needs. If you do not start the CIM Extension with root privileges, the management server will display messages resembling the following: `Data is late or an error occurred.`
- To configure UNIX CIM Extensions to run behind a firewall, see “Configuring UNIX CIM Extensions to Run Behind Firewalls” on page 369.

To start the CIM Extension, type the following in the `/opt/APPQcime/tools` directory, where `/opt` is the directory into which you installed the CIM Extension:

```
# ./start
```

The following is displayed:

```
Starting CIM Extension for Solaris...
```

How to Determine if the CIM Extension Is Running

You can determine if the CIM Extension is running by entering the following command at the command prompt:

```
# ./status
```

The CIM Extension is running when the following message is displayed:

```
CIM Extension Running: Process ID: 93
```

where 93 is the process ID running the CIM Extension

Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM Extension on start-up. The file is named `cim.extension.parameters` and is located in the `[Installation_Directory]/conf` directory on the host. This directory also contains a file named `cim.extension.parameters-sample`. This file contains samples of available parameters and can be copied into the `cim.extension.parameters` file and used as a template.

Restricting the Users Who Can Discover the Host

The `-users` parameter provides greater security by restricting access. When you use the management server to discover the host, provide a user name that was specified in the `-users` parameter.

For example, assume you want to use the management server to discover a Solaris host, but you do not want to provide the password to the root account. You can provide the password to another valid Solaris user account that has less privileges, for example jsmythe. First, you would add the user to

the parameters file. You would then logon to the management server, access the Discovery page, and provide the user name and password for jsmythe. Only the user name and password for jsmythe can be used to discover the Solaris host.

Follow these steps to add a user to the parameters file:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:
   `-users myname`
   where myname is a valid Solaris user name.

   Note: You can provide multiple users by separating them with a colon. For example `-users myname:jsymthe`.

3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

   Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

Changing the Port Number

The CIM Extension uses port 4673 by default. If the port is already used, follow these steps to change the port the CIM Extension will access:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:
   `-port 1234`
   where 1234 is the new port for the CIM Extension
3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

192.168.1.2:1234

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Configuring the CIM Extension to Listen on a Specific Network Card

Follow these steps to configure the CIM Extension to listen on a specific network card (NIC):

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:
   `-on 127.0.0.1,192.168.0.1`

   Note: If you want to configure the CIM Extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

The “-on” parameter may include a port specification. In that case, the CIM Extension listens on the indicated port of the indicated NIC, rather than the default port, for example:

```
-on 192.168.2.2:3456
```

The CIM Extension listens only on the NIC that has the IP address 192.168.2.2 on port 3456.

The management server assumes the CIM Extension is running on port 4673. The management server also listens on port 17000 for CIM Extensions from build 4.0.

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

192.168.1.2:1234

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file:

Table 11-1: Parameters for CIM Extensions

Parameter	Description
`-user`	The user defined in this parameter must be a valid user for the host. Only the user needs to be defined. The user name and password are provided from the management server during discovery. The user does not need to have root authority. A colon separated list can be used to specify multiple users.
`-credentials <username from the management server>:<password>`	The credentials defined by this parameter must match the values entered from the management server during discovery. They are not used as authentication on the host itself.
`-agentnic <ip address>`	Restricts the CIM Extension on multihomed systems to listen only on the designated IP address.
`-mgmtServerIP <ip address>`	Restricts the CIM Extension to listen only to a specific management server IP address.

Finding the Version of a CIM Extension

You can find the version number of a CIM Extension:

1. Go to the `/opt/APPQcime/tools` directory.
2. Type the following at the command prompt:
   ```
   # ./start -version
   ```

You are shown the version number of the CIM Extension and the date it was built, as shown in the following example:

```
CXWS for mof/cxws/cxws-solaris.mof
CXWS version x.x.x.x, built on Fri 12-March-xxxx 12:29:49 by dmaltz
```

where

- x.x.x.x is the version for the CIM Extension
- xxxx is the year

Combining Start Commands

You can also combine the `-users` and `-port` commands as follows:

```
./start -users myname -port 1234
```

or

```
./start -port 1234 -users myname
```

where

`myname` is the user name that must be used to discover this Solaris host

`1234` is the new port

Stopping the CIM Extension

To stop the CIM Extension, enter the following at the command prompt in the `/opt/APPQcime/tools` directory, where `/opt` is the directory into which you installed the CIM Extension:

```
#  ./stop
```

Keep in mind the following:

- You must have root privileges to stop the CIM Extension.
- When you stop the CIM Extension, the management server is unable to gather information about this host.

Rolling Over the Logs

The logging information for the CIM Extension is contained primarily in the cxws.log file, created by default in the `<Installation_directory>/tools` directory. The cxws.log file rolls over once it becomes more than 100 MB. The information in cxws.log is moved to cxws.log.1. When the logs roll over again, cxws.log.1 is renamed to cxws.log.2 and the information that is in cxws.log is moved to

cxws.log.1. The numbering for the files continues sequentially, for example, cxws.log.3, with there being a maximum of three backup logs.

- cxws.log - contains the latest logging information
- cxws.log.1 - contains logging information that was previously in cxws.log
- cxws.log.2 - contains logging information that was previously in cxws.log.1
- cxws.log.3 - contains logging information that was previously in cxws.log.2

The `cxws.out` file contains some logging information, such as the CIM Extension starting, which is recorded in case something unexpected happens with the Java Virtual Machine. The CIM Extension appends the cxws.out file and rolls it over.

Removing the CIM Extension from Solaris

To remove the CIM Extension for Solaris as root:

1. Login as root.
2. Stop the CIM Extension, as described in the topic, “Stopping the CIM Extension” on page 236.
3. Enter the following at the command prompt:
   ```
   # pkgrm APPQcime
   ```
4. Enter **y** when you are asked if you want to remove the CIM Extension.
   When you see the following message, the CIM Extension has been removed:

   ```
   Removal of <APPQcime> was successful.
   ```

CHAPTER 12

Installing the CIM Extension for OpenVMS

This chapter describes the following:

- About the CIM Extension for OpenVMS on page 240
- Prerequisites on page 240
- Installing the CIM Extension for OpenVMS on page 242
- Starting the CIM Extension Manually on page 244
- Finding the Status of the CIM Extension on page 244
- Configuring CIM Extensions on page 245
- Finding the Version of a CIM Extension on page 248
- Stopping the CIM Extension on page 249
- Rolling Over the Log Files on page 250
- Increasing the Native Logging Level on page 251
- Removing the CIM Extension from OpenVMS on page 251

Note: This chapter describes how to install and manage the CIM Extension directly on the host. You can also install and manage CIM Extensions remotely. See “Deploying and Managing CIM Extensions” on page 153.

Important: Make sure you have reviewed Table 1-1, “Roadmap for Installation and Initial Configurations,” on page 2 to ensure you are at the correct step.

About the CIM Extension for OpenVMS

The CIM Extension for OpenVMS is compatible with OpenVMS for Alpha. The CIM Extension for OpenVMS gathers information from the operating system and host bus adapters (HBAs) and makes the information available to the management server.

Important: Install the CIM Extension on each host you want the management server to manage.

The CIM Extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBA API.

For more information about the HBA API, see the following Web page on the SNIA Web site:

http://www.snia.org/tech_activities/hba_api/

Prerequisites

The required prerequisites are listed below:

- **Supported OpenVMS (Alpha) versions and required ECOs**
  - To verify installed patches, enter the following at the command prompt:

    ```
    $ prod sh prod/full
    ```

  - **OpenVMS 7.3.2 (Alpha)**

OpenVMS (Alpha) 8.2 is also supported. The requirements for OpenVMS 8.2 are listed later in this Prerequisites section.

- **Mandatory ECOs for OpenVMS 7.3.2 (Alpha):**
  - `DEC-AXPVMS-VMS732_PCSI-V0100`
  - `DEC-AXPVMS-VMS732_UPDATE-V0400`
  - `DEC-AXPVMS-VMS732_SYS-V0700`
  - `DEC-AXPVMS-VMS732_FIBRE_SCSI-V0700` (Note that the FC SNIA HBA API software is bundled with the fibre_scsi patch.)
- **Optional ECO:**

  `VMS732_ACRTL-V0100`

  The optional ECO is recommended if your application uses files exclusively on an ODS-5 volume and your system has the latest C RTL ECO. The ECO lets you reduce the overhead of file name mapping. Whenever you eliminate a file name mapping option, you reduce the number of internal buffers that need to be allocated resulting in a smaller memory footprint for your application.

Note: VMS732_PCSI-V0100 and VMS732_UPDATE-V0400 need to be installed prior to the installation of VMS732_SYS-V0700 followed by installation of VMS732_FIBRE_SCSI-V0700. A reboot is required after the installation.

- **OpenVMS 8.2 (Alpha)**
  Upgraded to the following required patch level:

  `DEC-AXPVMS-VMS82A_FIBRE_SCSI-V0100`

  The CIM Extension for OpenVMS is compatible with OpenVMS 7.3.2 (Alpha) and OpenVMS 8.2 (Alpha). The requirements for OpenVMS 7.3-2 are listed earlier in this Prerequisites section.
- **60 MB of free disk space**
- **Open network port**
  By default, the CIM Extension uses port 4673 to communicate with the management server. Verify the network port is open. If you need to use a different port, see “Changing the Port Number” on page 246.
- **SNIA HBA API Support**
  The management server is only compatible with host bus adapters (HBAs) that support the

SNIA HBA API. The SNIA HBA API support for OpenVMS (Alpha) 7.3-2 and 8.2 is part of the FIBRE_SCSI ECO kits listed above: `DEC-AXPVMS-VMS732_FIBRE_SCSI-V0700` for OpenVMS (Alpha) 7.3-2 and `DEC-AXPVMS-VMS82A_FIBRE_SCSI-V0100` for OpenVMS (Alpha) 8.2.

To verify HBA API support, check the OpenVMS host for the following files in the path specified.

```
$ dir sys$common:[syslib]hba_vms.exe
$ dir sys$common:[syslib]hba.conf
```

Installing the CIM Extension for OpenVMS

This section covers the following CIM Extension installations for OpenVMS:

- “Installing the CIM Extension on a Standalone Host” on page 242
- “Installing the CIM Extension on a Cluster” on page 243

Installing the CIM Extension on a Standalone Host

This section describes how to install the CIM Extension for OpenVMS on standalone hosts.

- The CIM Extension on OpenVMS needs to be installed locally on each of the required hosts.
- You must be a superuser on each host to install the CIM Extension for OpenVMS.

Follow these steps:

1. Log in as system.
2. Verify the required ECOs and patches are installed; enter the following at the system prompt:

   ```
   $ prod sh prod/full
   ```

   See “Prerequisites” on page 240 if needed.
3. Verify that the HBA supports the SNIA HBA API; check the OpenVMS host for the following files in the path specified.

   ```
   $ dir sys$common:[syslib]hba_vms.exe
   $ dir sys$common:[syslib]hba.conf
   ```

4. If the CD is already mounted, dismount it by entering:
   ```
   $ DISMOUNT <CD-ROM device name>
   ```
5. Insert the CIM Extension CD-ROM in the CD-ROM drive.
6. Mount the CIM Extension CD-ROM by enter the following at the command prompt:
   ```
   $ MOUNT /MEDIA=CDROM /UNDEFINED_FAT=STREAM:32767/OVERRIDE=IDENTIFICATION
   DQB0 (or whichever is the CD-ROM device)
   ```
7. Change directory to the location where the OpenVMS Extension is available:
   ```
   $ SET DEF DQB0:[OVMS]
   ```
8. Run the Installation script by entering the following command.
   ```
   $ @OVMSINST
   ```
9. Press **Enter** when prompted for confirmation by the PCS as shown in the example below:
   ```
   **********
   The following product has been selected:
       HP AXPVMS APPQCIME V5.0                Layered Product

   Do you want to continue? [YES]

   ***********
   ```
   The installation is completed with the default values and the **APPQCIME** process starts.
10. Verify that the SE Agent process starts properly. You should see the following message:
    ```
    CXWS ready to accept connections
    ```
11. Verify that the APPQCIME process is running by typing:
    ```
    $ @sys$common:[opt.appqcime.tools]status
    ```
12. Dismount the CD-ROM by typing:
    ```
    $ DISMOUNT <CD-ROM device name>
    ```
13. Remove the CD. Press the Eject button on the CD-ROM drive to take the CD out of the CD-ROM drive.

Note: The CIM Extension starts during the local installation.

Installing the CIM Extension on a Cluster

Follow the steps in “Installing the CIM Extension on a Standalone Host” on page 242 to install the CIM Extension for OpenVMS on a Cluster system. The CIM Extension for OpenVMS must be installed on all nodes of the cluster.

Starting the CIM Extension Manually

This section provides instructions for manually starting the OpenVMS CIM Extension. When you start the CIM Extension, you can restrict the user accounts that can discover the host. You can also change the port number the CIM Extension uses. See the following topics for more information.

- Restricting the Users Who Can Discover the Host on page 245
- Additional Parameters on page 248

Be aware that the management server can only obtain information from a host when the CIM Extension is running on the host. You must be a superuser for the host system in order to start the CIM Extension.

The CIM Extension provides information within the privileges of the user account that started the CIM Extension. Only the system account has enough privileges to provide the information the management server needs.

To manually start the CIM Extension:

1. Log in as system on the OpenVMS host on which you want to start the CIM Extension.
2. Type the following command to start the CIM Extension.
   $ @sys$common:[opt.appqcime.tools]start

   The following message displays:

   ```
   STARTING OpenVMS CIME...
   ```

Finding the Status of the CIM Extension

You can check the status of the CIM Extension by entering the following in the `sys$common:[opt.appqcime.tools]` directory.

$ @status

The CIM Extension is running when the following message is displayed:

```
CIM Extension is running. Process id :001B0AEE
```

where 001B0AEE is the process ID running the CIM Extension.

Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM Extension on start-up. The file is named `cim.extension.parameters` and is located in the `[Installation_Directory]/conf` directory on the host. This directory also contains a file named `cim.extension.parameters-sample`. This file contains samples of available parameters and can be copied into the `cim.extension.parameters` file and used as a template.

Restricting the Users Who Can Discover the Host

The `-users` parameter provides greater security by restricting access. When you use the management server to discover the host, provide a user name that was specified in the `-users` parameter.

For example, assume you want to use the management server to discover a OpenVMS host, but you do not want to provide the password to the root account. You can provide the password to another valid OpenVMS user account that has less privileges, for example jsmythe. First, you would add the user to the parameters file. You would then logon to the management server, access the Discovery page, and provide the user name and password for jsmythe. Only the user name and password for jsmythe can be used to discover the OpenVMS host.

Follow these steps to add a user to the parameters file:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:
   `-users myname`
   where myname is a valid OpenVMS user name.

   Note: You can provide multiple users by separating them with a colon. For example `-users myname:jsymthe`.

3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

Changing the Port Number

The CIM Extension uses port 4673 by default. If the port is already used, follow these steps to change the port the CIM Extension will access:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:
   `-port 1234`
   where 1234 is the new port for the CIM Extension
3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

192.168.1.2:1234

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Configuring the CIM Extension to Listen on a Specific Network Card

Follow these steps to configure the CIM Extension to listen on a specific network card (NIC):

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:
   `-on 127.0.0.1,192.168.0.1`

   Note: If you want to configure the CIM Extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

   Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

The “-on” parameter may include a port specification. In that case, the CIM Extension listens on the indicated port of the indicated NIC, rather than the default port, for example:

```
-on 192.168.2.2:3456
```

The CIM Extension listens only on the NIC that has the IP address 192.168.2.2 on port 3456.

The management server assumes the CIM Extension is running on port 4673. The management server also listens on port 17000 for CIM Extensions from build 4.0.

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

192.168.1.2:1234

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file:

Table 12-1: Parameters for CIM Extensions

Parameter	Description
`-user`	The user defined in this parameter must be a valid user for the host. Only the user needs to be defined. The user name and password are provided from the management server during discovery. The user does not need to have root authority. A colon separated list can be used to specify multiple users.
`-credentials <username from the management server>:<password>`	The credentials defined by this parameter must match the values entered from the management server during discovery. They are not used as authentication on the host itself.
`-agentnic <ip address>`	Restricts the CIM Extension on multihomed systems to listen only on the designated IP address.
`-mgmtServerIP <ip address>`	Restricts the CIM Extension to listen only to a specific management server IP address.

Finding the Version of a CIM Extension

You can find the version number of a CIM Extension:

1. Navigate to the sys$common:[opt.appqcime.tools] directory.
2. Type the following at the command prompt:
   `$ @start -version`
   The version number is displayed as shown in the example below.

```
CXWS VERSION: 4.2.0.6
```

Combining Start Commands

You can combine the `-users` and `-port` commands as follows:

```
sys$common:[opt.appqcime.tools]start -users myname -port 1234
```

or

```
sys$common:[opt.appqcime.tools]start -port 1234 -users myname
```

Where myname is the user name that must be used to discover this OpenVMS host and 1234 is the new port.

Stopping the CIM Extension

To stop the CIM Extension:

1. Log in to the system as a superuser.
2. Navigate to the following directory:
   `sys$common:[opt.appqcime.tools]`
   Where `sys$common:[opt]` is the directory in which you installed the CIM Extension.
3. Type: **$ @stop** to stop the CIM Extension.

Note: Once the CIM Extension is stopped on the host, the management server will not be able to gather information about this host.

Rolling Over the Log Files

The logging information for the CIM Extension is contained primarily in the `cxws.log` file, created by default in the `<Installation_directory>/tools` directory. The cxws.log file rolls over once it becomes more than 100 MB. The information in cxws.log is moved to cxws.log.1. When the logs roll over again, cxws.log.1 is renamed to cxws.log.2 and the information that is in cxws.log is moved to cxws.log.1. The numbering for the files continues sequentially, for example, cxws.log.3, with there being a maximum of three backup logs.

- cxws.log - contains the latest logging information
- cxws.log.1 - contains logging information that was previously in cxws.log
- cxws.log.2 - contains logging information that was previously in cxws.log.1
- cxws.log.3 - contains logging information that was previously in cxws.log.2

The `cxws.out` file contains some logging information, such as the CIM Extension starting, which is recorded in case something unexpected happens with the Java Virtual Machine. The CIM Extension appends the cxws.out file and rolls it over.

The `cxws_native.log` contains logging information relative to OpenVMS native operations. The configuration information for `cxws_native.log` is maintained in `sys$specific:[opt.appqcime.conf]` where `sys$specific:[opt]` is the directory in which the node-specific files of the CIM Extension are present. When the log file size exceeds the LOG_SIZE parameter specified in the configuration file for the `cxws_native.log`, the file rolls over. The information in `cxws_native.log` is moved to `cxws_native.log.old`. If `cxws_native.log.old` already exists, it is deleted.

Increasing the Native Logging Level

The configuration information for `cxws_native.log` is maintained in `sys$specific:[opt.appqcime.config]cxws_native.cfg`. In order to increase the logging level, choose the log level accordingly in this file.

For example, `Set LOG_LEVEL to 3 in cxws_native.cfg` and restart the CIM Extension to increase the log level to 3.

Removing the CIM Extension from OpenVMS

This section includes information on removing (uninstalling) the CIM Extension. It covers the following topics:

- "Uninstalling the OpenVMS CIM Extension on a Standalone Host" on page 251
- "Uninstalling the OpenVMS CIM Extension on a Cluster Host" on page 252

Uninstalling the OpenVMS CIM Extension on a Standalone Host

To remove the CIM Extension for OpenVMS on a standalone host:

1. Login as system.
2. Enter the following at the command prompt:
   $ @sys$common:[opt.appqcime.scripts]appiq_local_uninstall.com
3. Press **Enter** to proceed with the uninstall as shown in the example below:

```
The following product has been selected:
HP AXPVMS APPQCIME V5.0                Layered Product
Do you want to continue? [YES]
```

   The CIM Extension is removed.

Uninstalling the OpenVMS CIM Extension on a Cluster Host

The OpenVMS CIM Extension must be uninstalled from all nodes on the cluster. Follow the steps in “Uninstalling the OpenVMS CIM Extension on a Standalone Host” on page 251 for each node on the cluster.

CHAPTER 13

Installing the CIM Extension for HP Tru64 UNIX

This chapter describes the following:

- About the CIM Extension for Tru64 UNIX on page 254
- Prerequisites on page 254
- Installing the CIM Extension on page 256
- Starting the CIM Extension Manually on page 258
- How to Determine if the CIM Extension Is Running on page 259
- Configuring CIM Extensions on page 259
- Finding the Version of a CIM Extension on page 263
- Stopping the CIM Extension on page 264
- Rolling Over the Logs on page 264
- Fulfilling the Prerequisites on page 265
- Removing the CIM Extension from Tru64 on page 265

Note: This chapter describes how to install and manage the CIM Extension directly on the host. You can also install and manage CIM Extensions remotely. See “Deploying and Managing CIM Extensions” on page 153.

Important: Make sure you have reviewed Table 1-1, “Roadmap for Installation and Initial Configurations,” on page 2 to ensure you are at the correct step.

About the CIM Extension for Tru64 UNIX

The CIM Extension for HP Tru64 UNIX gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

Important: Install the CIM Extension on each host you want the management server to manage.

The CIM Extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBA API. For more information about the HBA API, see the following Web page at the SNIA Web site: http://www.snia.org/tech_activities/hba_api/

Prerequisites

The installation for the CIM Extension verifies that the host is running at least Tru64 5.1B. If the installation fails, see “Fulfilling the Prerequisites” on page 265.

Also, verify the following before you install the CIM Extension:

- Software Requirements on page 255
- Required Disk Space on page 255
- SNIA HBA API Support on page 256

Software Requirements

Note: You do not need to install the FC-HBA shared libraries if you are running Tru64 UNIX version 5.1B-4.

If you are running Tru64 UNIX version 5.1B-3 or version 5.1B-2, you must install one of the following SNIA patches to obtain the FC-HBA shared libraries.

- For Tru64 UNIX version 5.1B-2 - Install T64KIT1000413-V51BB25-E-20060222.
- For Tru64 UNIX version 5.1B-3 - Install T64KIT1000414-V51BB26-E-20060222.

To obtain the patch:

1. Go to the IT Resource Center Web site at the following URL: http://www1.itrc.hp.com/.
2. Use the **Search** field at the Web site to find the patch number. When you search for the patch, make sure IT Resource Center (Compaq) is selected.

   Note: To save time, copy the patch number from the PDF or HTML Installation Guide and paste it into the **Search** field.

Required Disk Space

The CIM Extension for Tru64 requires 60 MB under /opt.

Network Port Must Be Open

The CIM Extension uses port 4673 by default to communicate with the management server. Verify the network port is open. Refer to the documentation accompanying your Tru64 host for more information. If you need to use a different port, see “Permanently Changing the Port a CIM Extension Uses (UNIX Only)” on page 367.

SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API.

Tru64 hosts need to have the hbaapi library installed on the host. See “Software Requirements” on page 255.

To verify if hbaapi is installed on the host, check for the presence of the file hba.conf under the `/etc` directory. The contents of the file would contain a line, such as the following:

```
com.hp.emulex    /usr/shlib/libemxhbaapi.so
```

Verify the presence of the shared library file mentioned in the hba.conf file.

Installing the CIM Extension

Important: You must install the CIM Extension for Tru64 in the default directory.

You can install the CIM Extension for Tru64 one of two ways:

- **On a Standalone Host** - See “Installing CIM Extension on a Standalone Host” on page 256.
- **On a Cluster** - See “Installing the CIM Extension on a Cluster” on page 257.

Installing CIM Extension on a Standalone Host

To install the CIM Extension using CLI:

1. Login as root.
2. Place the CIM Extension CD-ROM into the CD-ROM on the Tru64 server.
3. Create the /cdrom directory on Tru64 host by entering the following at the command prompt:
   ```
   # mkdir /cdrom
   ```
4. Mount the CIM Extension CD-ROM by enter the following at the command prompt:

```
# mount /dev/disk/cdromxx  /cdrom
```

where xx corresponds to the cdrom device number.

You can find the cdrom device number by entering the following at the command prompt:

```
# hwmgr -view devices
```

5. To install the CIM Extension:
   a. Go to the /cdrom/tru64/ directory, as shown in the following example:
      `# cd /cdrom/tru64/`
   b. Run the script /tru64_local_install.sh at the command prompt:
      #./tru64_local_install.sh

   The installation is complete when you are told the following:

   ```
   Installation of AppStorM Tru64 CIM Extensions was successful.
   ```

   Note: The `tru64_local_install.sh` command starts the CIM Extension.

6. Eject the CD-ROM by doing the following:
   a. Unmount the CD-ROM by entering the following at the command prompt:
      `# umount /cdrom`
      where `/cdrom` is the name of the directory where you mounted the CD-ROM
   b. Press the eject/unload button on the CD-ROM drive.
7. Press the **Eject** button on the CD-ROM drive to take the CD out of the CD-ROM drive. The CIM Extension for Tru64 starts automatically at boot time by using /sbin/rc3.d scripts. The CIM Extension uses port 4673 when it starts automatically after a reboot.
8. Type the following at the command prompt to find the status of the CIM Extension:
   `/opt/APPQcime/tools/status`

Installing the CIM Extension on a Cluster

The installation of the CIM Extension on a cluster is similar to the installation of the CIM Extension on a standalone node. However, on a cluster it is required to run the install script on only one node of the cluster. By default the install script (`tru64_local_install.sh`) starts the CIM Extension automatically on all nodes of the cluster after an installation. To install the CIM Extension on all nodes of the cluster, repeat the steps found in “Installing the CIM Extension” on page 256.

To install the CIM Extension on just the current node:

1. Go to the /cdrom/tru64/ directory, as shown in the following example:
   ```
   # cd /cdrom/tru64/
   ```
2. Run the command `./tru64_local_install.sh -curnode` at the command prompt:
   ```
   #./tru64_local_install.sh -curnode
   ```
3. You must start the CIM Extension manually as described in “Starting the CIM Extension Manually” on page 258.

Starting the CIM Extension Manually

The management server can only obtain information from this host when the CIM Extension is running.

Keep in mind the following:

- You must have root privileges to run the CIM Extension. The CIM Extension only provides the information within the privileges of the user account that started the CIM Extension. Only root has enough privileges to provide the information the management server needs. If you do not start the CIM Extension with root privileges, the management server will display messages resembling the following: Data is late or an error occurred.
- To configure UNIX CIM Extensions to run behind a firewall, see “Configuring UNIX CIM Extensions to Run Behind Firewalls” on page 369.

To start the CIM Extension, type the following in the /opt/APPQcime/tools directory, where /opt is the directory into which you installed the CIM Extension:

```
# ./start
```

The following is displayed:

```
Starting CIM Extension for Tru64...
```

Keep in mind the following:

- When you start the CIM Extension, you can restrict the user accounts that can discover the host. You can also change the port number the CIM Extension uses. See the following topics for more information. You can also access information about these topics by typing the following:

  ```
  /start -help
  ```

How to Determine if the CIM Extension Is Running

You can determine if the CIM Extension is running by entering the following command at the command prompt:

```
# ./status
```

The CIM Extension is running when the following message is displayed:

```
CIM Extension Running: Process ID: 93
```

where 93 is the process ID running the CIM Extension

Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM Extension on start-up. The file is named `cim.extension.parameters` and is located in the `[Installation_Directory]/conf` directory on the host. This directory also contains a file named `cim.extension.parameters-sample`. This file contains samples of available parameters and can be copied into the `cim.extension.parameters` file and used as a template.

Restricting the Users Who Can Discover the Host

The `-users` parameter provides greater security by restricting access. When you use the management server to discover the host, provide a user name that was specified in the `-users` parameter.

For example, assume you want to use the management server to discover a Tru64 host, but you do not want to provide the password to the root account. You can provide the password to another valid Tru64 user account that has less privileges, for example jsmythe. First, you would add the user to the parameters file. You would then logon to the management server, access the Discovery page, and provide the user name and password for jsmythe. Only the user name and password for jsmythe can be used to discover the Tru64 host.

Follow these steps to add a user to the parameters file:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:
   `-users myname`
   where myname is a valid Tru64 user name.

   Note: You can provide multiple users by separating them with a colon. For example `-users myname:jsymthe`.

3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

   Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

Changing the Port Number

The CIM Extension uses port 4673 by default. If the port is already used, follow these steps to change the port the CIM Extension will access:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:
   `-port 1234`
   where 1234 is the new port for the CIM Extension
3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

   Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

192.168.1.2:1234

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Configuring the CIM Extension to Listen on a Specific Network Card

Follow these steps to configure the CIM Extension to listen on a specific network card (NIC):

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:
   `-on 127.0.0.1,192.168.0.1`

   Note: If you want to configure the CIM Extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

   Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

The “-on” parameter may include a port specification. In that case, the CIM Extension listens on the indicated port of the indicated NIC, rather than the default port, for example:

```
-on 192.168.2.2:3456
```

The CIM Extension listens only on the NIC that has the IP address 192.168.2.2 on port 3456.

The management server assumes the CIM Extension is running on port 4673. The management server also listens on port 17000 for CIM Extensions from build 4.0.

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

192.168.1.2:1234

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file:

Table 13-1: Parameters for CIM Extensions

Parameter	Description
`-user`	The user defined in this parameter must be a valid user for the host. Only the user needs to be defined. The user name and password are provided from the management server during discovery. The user does not need to have root authority. A colon separated list can be used to specify multiple users.
`-credentials <username from the management server>:<password>`	The credentials defined by this parameter must match the values entered from the management server during discovery. They are not used as authentication on the host itself.
`-agentnic <ip address>`	Restricts the CIM Extension on multihomed systems to listen only on the designated IP address.
`-mgmtServerIP <ip address>`	Restricts the CIM Extension to listen only to a specific management server IP address.

Finding the Version of a CIM Extension

You can find the version number of a CIM Extension:

1. Go to the /opt/APPQcime/tools directory.
2. Type the following at the command prompt:

```
# ./start -version
```

You are shown the version number of the CIM Extension and the date it was built, as shown in the following example:

```
Starting CIM Extension for Tru64
Thu Sep 21 14:46:47 EDT xxxx
CXWS x.x.x.x on /192.168.1.5:4673 now accepting connections
```

where

- xxxx is the year.

- x.x.x.x is the version of CIM Extension
- 192.168.1.5 is the IP address of the host
- 4673 is the port used by the CIM extension

Stopping the CIM Extension

To stop the CIM Extension, enter the following at the command prompt in the /opt/APPQcime/tools directory, where /opt is the directory into which you installed the CIM Extension:

./stop

Keep in mind the following:

- You must have root privileges to stop the CIM Extension.
- When you stop the CIM Extension, the management server is unable to gather information about this host.

Rolling Over the Logs

The logging information for the CIM Extension is contained primarily in the cxws.log file, created by default in the `<Installation_directory>/tools` directory. The cxws.log file rolls over once it becomes more than 100 MB. The information in cxws.log is moved to cxws.log.1. When the logs roll over again, cxws.log.1 is renamed to cxws.log.2 and the information that is in cxws.log is moved to cxws.log.1. The numbering for the files continues sequentially, for example, cxws.log.3, with there being a maximum of three backup logs.

- cxws.log - contains the latest logging information
- cxws.log.1 - contains logging information that was previously in cxws.log
- cxws.log.2 - contains logging information that was previously in cxws.log.1
- cxws.log.3 - contains logging information that was previously in cxws.log.2

The `cxws_native.log` file contains logging information relative to Tru64 native operations. The configuration information for `cxws_native.log` is maintained in `/opt/APPQcime/conf/`

`cxws_native.cfg`. When the log file size exceeds the LOG_SIZE parameter specified in the configuration file for the `cxws_native.log`, the file rolls over. The information in `cxws_native.log` is moved to `cxws_native.log.old`. If `cxws_native.log.old` already exists, it is deleted.

Increasing the Native Logging Level

The `cxws_native.log` contains logging information relative to Tru64 system calls used. The configuration information for cxws_native.log is maintained in `/opt/APPQcime/config/cxws_native.cfg` where `/opt` is the directory into which you installed the CIM extension. More detailed logging information can be obtained by increasing the log level. Set LOG_LEVEL to 3 in `cxws_native.cfg` and restart the CIM Extension to increase the log level.

Fulfilling the Prerequisites

Use the commands mentioned in this section to determine if you have the required software.

To verify driver bundle version, enter the following at the command prompt:

setld -i

Ensure that the required patches listed in the prerequisites are present

Removing the CIM Extension from Tru64

This section describes the following:

- Removing the CIM Extension from a Standalone Host on page 266
- Removing the CIM Extension from a Cluster on page 266

Removing the CIM Extension from a Standalone Host

To remove the CIM Extension for Tru64:

1. Login as root.
2. Go to the `/opt/APPQcime/scripts` directory, where `/opt` is the directory into which you installed the CIM Extension.
3. Execute the following script: tru64_local_uninstall.sh
4. When you see the following message, the CIM Extension has been removed:
   `"UnInstallation of AppStorM Tru64 CIM Extensions was successful".`
5. To remove the APPQcime directory, go to the `/opt` and `/cluster/member/{memb}/opt` directories and enter the following at the command prompt:
   ```
   # rm -rf APPQcime
   ```

Removing the CIM Extension from a Cluster

The uninstall procedure from “Removing the CIM Extension from a Standalone Host” on page 266 needs to be executed on one node of the cluster only. The script ensures that the agent process is stopped on all nodes and the product is considered removed from all the nodes.

The node specific directory `/cluster/member/{memb}/opt/APPQcime` needs to be cleaned up on each node explicitly.

CHAPTER 14

Installing the CIM Extension for Microsoft Windows

This chapter describes the following:

- About the CIM Extension for Windows on page 268
- Verifying SNIA HBA API Support on page 268
- Upgrading a Host with the Latest CIM Extension on page 271
- Installation Steps on page 272
- Installing the CIM Extension Using the Silent Installation on page 273
- Configuring CIM Extensions on page 274
- Rolling Over the Logs on page 276
- Removing the CIM Extension from Windows on page 277

Note: This chapter describes how to install and manage the CIM Extension directly on the host. You can also install and manage CIM Extensions remotely. See “Deploying and Managing CIM Extensions” on page 153.

Important: Make sure you have reviewed Table 1-1, “Roadmap for Installation and Initial Configurations,” on page 2 to ensure you are at the correct step.

About the CIM Extension for Windows

The CIM Extension for Windows gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

Important: Install the CIM Extension on each host you want the management server to manage.

The CIM Extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBA API) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBA API. For more information about the HBA API, see the following Web page at the SNIA Web site: http://www.snia.org/tech_activities/hba_api/

Verifying SNIA HBA API Support

The Windows CIM Extension can only talk to host bus adapters (HBAs) that support the SNIA HBA API. You can run the hbatest program, which lists the name and number for all HBA's that support the SNIA HBA API.

To run hbatest:

1. Open a command prompt window and do one of the following:
   - **If you have not installed the CIM Extension** - Go to the `Windows\tools` directory on the CIM Extension CD-ROM.
   - **If you have installed the CIM Extension** - Go to the `<Installation_Directory>\CimExtensions\tools` directory on the host running the CIM Extension.
2. Enter the following at the command prompt: `hbatest.exe`
   The program lists the name and number for all HBA's that support the SNIA HBA API.
3. (Optional) To obtain additional diagnostics for debugging, enter the following at the command prompt:
   `hbatest -v`

The `-v` (verbose) option runs the same commands that the CIM Extension runs to retrieve all HBA information and displays the output.

Emulex Host Bus Adapters

The Windows CIM Extension requires the SNIA library (HBA API). Previous versions of HBAnyware provide the SNIA library; however, several later versions of HBAnyware do not ship with the SNIA library and rely upon Microsoft's SNIA library.

Your configuration may require you to run the setupelxhbaapi program, which modifies the registry so that SNIA libraries can be detected by the CIM Extension. To determine if your configuration requires you to run the setupelxhbaapi program go to the following Web site:

http://www.emulex.com/ts/downloads/windows/rel/hbaapi.

Important: If you run the setupelxhbaapi program, you do not need to install HBAnyware. The setupelxhbaapi program installs the SNIA library, which is required by the CIM Extension. If you do not run the setupelxhbaapi program, you must install the full HBAnyware package to obtain the SNIA library.

This program installs the hbaapi.dll and Emulex emulexhbaapi.dll files into the `program files\emulex\hbaapi` folder. The installation also creates a registry key with the absolute path to the `emulexhbaapi.dll` file.

Driver Information for Verifying IBM Branded QLogic Adapters

This section provides information for verifying IBM branded QLogic adapters.

The SNIA HBA comes from IBM MSJ (FastT Management Suite Java). The registry setting is most likely in the following location:

HKEY_LOCAL_MACHINE\SOFTWARE\SNIA\HBA\QL2XXX

The driver can be found in the following location:

C:\Program Files\IBM FASt MSJ\ql2xhai2.dll

Driver Information for Verifying QLogic Adapters

This section provides information for verifying QLogic adapters.

If you have QLogic Adapters:

When you install the SNIA HBA, it either came with the driver or SANsurfer, the registry setting is most likely in the following location, which varies by release:

HKEY_LOCAL_MACHINE\SOFTWARE\SNIA\HBA\QL2XXX

Newer drivers points to C:\WINNT\system32\ql2xhai2.dll, but they also have system32\qlsdm.dll available. Earlier drivers points to C:\WINNT\System32\qlsdm.dll

Driver Information for Verifying AMCC/JNI Adapters

The SNIA HBA comes from JNI SNIA 2.0. The SNIA Library is in a separate package without the drivers. The registry setting is the following:

HKEY_LOCAL_MACHINE\SOFTWARE\SNIA\HBA\JNI

The SNIA Library can be found in the following location:

C:\Program Files\JNI\JNIsnia\Jni\JniHbaLib.dll

Upgrading a Host with the Latest CIM Extension

To avoid the following issues from occurring after you upgrade the CIM Extension for Windows, perform the steps provided in this section:

- The Host CIM Extension Version Report in Reporter still displays the previous version.
- Host bus adapter data for the Windows host is removed from the management server database.
- If the Windows host has Emulex drivers, it is missing previously obtained data from switches and storage systems.
- FSRM scans are not possible.

Perform the following steps to avoid or resolve these issues:

1. Upgrade the management server.
2. Upgrade the CIM Extension on the Windows hosts.

   Note: You do not need to upgrade the CIM Extensions all at once. Keep in mind, however, that CIM Extensions from earlier versions do not return all information, such as FSRM data. It is strongly recommended you upgrade your CIM Extensions on Windows as soon as possible.

3. If hosts are not in the “Default” discovery group, you will need to restart AppStorManager, which is the service for the management server. To avoid restarting AppStorManager, you can move hosts to the “Default” discovery group.
   Do one of the following:

   - **For hosts that are not in the “Default” discovery group** - Restart AppStorManager, which is the service for the management server.

     Important: If you do Get Details immediately after a Windows host is upgraded without restarting the management server, you will have missing/incorrect data. You will also have missing and/or incorrect data until you finish the steps in this section.

   To avoid having to restart AppStorManager, see the following options.

- **For hosts that are in the "Default" discovery group** - Do a Step 1 discovery of the hosts.
- **For hosts that are not in the "Default" discovery group, move them there** - Do a Step 1 discovery of the hosts. All hosts may be moved to other discovery groups after Step 1 discovery.

4. Do Get Details.
   Your data appears.
5. Refresh reports to update report data.

Installation Steps

Keep in mind the following:

- If the installation fails with the message it cannot detect any supported HBAs and Emulex HBAs are installed on the host, install the full HBAnyware package. Contact Emulex at http://www.emulex.com for more information on how to obtain full HBAnyware package.
- You must have administrator privileges to install this software.
- You can install latest version of the Windows CIM Extension over the older version. Builds 4.0 and later of the CIM Extension are compatible with this build of the management server.
- On Microsoft Windows 2003 servers "Explorer Enhanced Security Settings" is enabled by default. If this setting is enabled, the "Authenticode signature not found" message is displayed during installation. Ignore the message or disabled the "Explorer Enhanced Security Settings".

Perform the following steps:

1. Insert the CD-ROM for the CIM Extensions, go to the Windows directory and then double-click **InstallCIMExtensions.exe**.
2. If you are asked if you want to install the product, click **Yes**.
3. When you see the introduction screen, click **Next**.
4. When you are asked for an installation directory, you can select the default or choose your own. To choose your own directory, click the **Choose** button. You can always display the default directory by clicking the **Restore Default Folder** button. When you are done, click **Next**.
5. Check the pre-installation summary. You are shown the following:

- Product Name
- Installation Folder
- Disk Space Required
- Disk Space Available

6. Do one of the following:
   - Click **Install** if you agree with the pre-installation summary.
   - Click **Previous** if you want to modify your selections.

   The CIM Extension is installed.
7. When you have been told the installation has been successful, click **Done** to quit the installation.

Important: Keep in mind that the CIM Extension automatically starts when the system is restarted. The management server can only obtain information from this host when the CIM Extension is running.

Installing the CIM Extension Using the Silent Installation

The CIM Extension for Windows provides a silent installation which installs the CIM Extension with no user interaction, all default settings are used.

Keep in mind the following:

- You must have administrator privileges to install this software.
- Make sure no other programs are running when you install the CIM Extension.
- Remove the previous version of the CIM Extension before you install the latest version.

To install the CIM Extension using the silent installation:

1. Insert the CD-ROM for the CIM Extensions.
2. Open a command prompt window and go to the Windows directory on the CD-ROM.
3. Enter the following at the command prompt:

```
E:\Windows>InstallCIMExtensions.exe -i silent
```

where `E` is the CD-ROM drive. The silent installation installs the CIM Extension in the default location.

Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM Extension on start-up. The file is named `cim.extension.parameters` and is located in the `[Installation_Directory]\conf` directory on the host. This directory also contains a file named `cim.extension.parameters-sample`. This file contains samples of available parameters and can be copied into the `cim.extension.parameters` file and used as a template.

Changing the Port Number

The CIM Extension uses port 4673 by default. If the port is already used, follow these steps to change the port the CIM Extension will access:

1. Go to the `[Installation_Directory]\conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:
   `-port 1234`
   where 1234 is the new port for the CIM Extension
3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

192.168.1.2:1234

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file:

Table 14-1: Parameters for CIM Extensions

Parameter	Description
`-user`	The user defined in this parameter must be a valid user for the host. Only the user needs to be defined. The user name and password are provided from the management server during discovery. The user does not need to have root authority. A colon separated list can be used to specify multiple users.
`-credentials <username from the management server>:<password>`	The credentials defined by this parameter must match the values entered from the management server during discovery. They are not used as authentication on the host itself.
`-agentnic <ip address>`	Restricts the CIM Extension on multihomed systems to listen only on the designated IP address.
`-mgmtServerIP <ip address>`	Restricts the CIM Extension to listen only to a specific management server IP address.

Rolling Over the Logs

The logging information for the CIM Extension is contained primarily in the cxws.log file, created by default in the `<Installation_directory>` directory. The cxws.log file rolls over once it becomes more than 100 MB. The information in cxws.log is moved to cxws.log.1. When the logs roll over again, cxws.log.1 is renamed to cxws.log.2 and the information that is in cxws.log is moved to cxws.log.1. The numbering for the files continues sequentially, for example, cxws.log.3, with there being a maximum of three backup logs.

- cxws.log - contains the latest logging information
- cxws.log.1 - contains logging information that was previously in cxws.log
- cxws.log.2 - contains logging information that was previously in cxws.log.1
- cxws.log.3 - contains logging information that was previously in cxws.log.2

The wrapper.log file contains some logging information, such as the CIM Extension starting, which is recorded in case something unexpected happens with the Java Virtual Machine. The CIM Extension appends starting/stopping/unexptected error conditions to the existing wrapper.log file.

Configuring the CIM Extension to Listen on a Specific Network Card

Follow these steps to configure the CIM Extension to listen on a specific network card (NIC):

1. Go to the `[Installation_Directory]\conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:
   `-on 127.0.0.1,192.168.0.1`

   Note: If you want to configure the CIM Extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

The “-on” parameter may include a port specification. In that case, the CIM Extension listens on the indicated port of the indicated NIC, rather than the default port, for example:

```
-on 192.168.2.2:3456
```

The CIM Extension listens only on the NIC that has the IP address 192.168.2.2 on port 3456.

The management server assumes the CIM Extension is running on port 4673. The management server also listens on port 17000 for CIM Extensions from build 4.0.

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**). In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

192.168.1.2:1234

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number
  If you have already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Removing the CIM Extension from Windows

To remove the CIM Extension for Windows:

1. Go to the Control Panel in Microsoft Windows.
2. Double-click **Add or Remove Programs**.

3. From the Currently installed programs list, select **Windows CIM Extension**.
4. Click the **Change/Remove** button.
5. When you are told the product is about to be uninstalled, click **Uninstall**.
6. When the program is done with removing the product, click **Done**.
7. It is highly recommended you reboot the host.

CHAPTER 15

Installing and Discovering the Windows Proxy

This chapter describes the following:

- Installing the Windows Proxy on page 280
- Discovering the Windows Proxy on page 281
- Configuring Windows Proxy Authentication on page 282
- Decreasing the Maximum Java Heap Size on page 284
- Removing the Windows Proxy on page 284

The Windows Proxy is required for the management server on Solaris to communicate with Microsoft Windows hosts using WMI. Microsoft Windows hosts managed via CXWS can be discovered directly and the Windows Proxy is not necessary. The CIM Extensions included with version 5.0 of the management server manage the host via CXWS.

Note: If a host with no agent or an old Windows agent is upgraded to use a CXWS agent, the host must be rediscovered.

After you install and discover the Windows Proxy, discover the hosts on which you have already installed the CIM Extension. See Chapter 16, “Discovering Applications and Hosts” on page 285 for more information.

Keep in mind the following:

- File Server SRM will not work if the hosts behind the Windows proxy are on a private network. If you want to use File Server SRM and your license lets you use this functionality, the Windows hosts cannot be on a private network.
- File Server SRM will also not work if the Windows proxy and the management server do not have network connectivity.
- The management server is unable to discover a database on a Windows host if the host is on a private network behind a Windows proxy. The management server can discover the Windows host through the Windows proxy, but the management server is not able to detect the database.
- If you run into problems with starting the Windows proxy, decrease the maximum Java heap size, as described in “Decreasing the Maximum Java Heap Size” on page 284.
- When the Windows proxy is installed on a new server, the Windows hosts must be re-discovered.

Installing the Windows Proxy

Important: If you are upgrading the Windows proxy, you can install the latest version of the Windows Proxy over the previous version.

To install the Windows proxy:

1. Insert the CD-ROM for the CIM Extensions, go to the Windows directory and then double-click **InstallWindowsProxy.exe**.
2. When you see the introduction screen, click **Next**.
3. When you are asked for an installation directory, you can select the default or choose your own. To choose your own directory, click the **Choose** button. You can always display the default directory by clicking the **Restore Default Folder** button. When you are done, click **Next**.
4. Read the important notes. Then, click **Next**.
5. Check the pre-installation summary. You are shown the following:
   - Product Name
   - Installation Folder

- Disk Space Required
- Disk Space Available

6. Do one of the following:
   - Click **Install** if you agree with the pre-installation summary.
   - Click **Previous** if you want to modify your selections.

   The Windows Proxy is installed.
7. When you have been told the installation has been successful, click **Done** to quit the installation.

Important: Keep in mind that the Windows Proxy automatically starts when the system is restarted. The management server on Solaris can only obtain information from the Windows hosts when the Windows Proxy (AppStorWinProxy service) is running.

8. If the Windows host running the Windows proxy has a private and a public network interface, you must modify the winproxy.conf file.
9. Discover the Windows proxy as described in the topic, “Discovering the Windows Proxy” on page 281.

Discovering the Windows Proxy

Important: Install the Windows proxy before you try the following steps.

Keep in mind the following:

- Install the Windows proxy before you try the following steps.
- The recommended workaround for entering an IP address into the discovery list as well as the Windows Proxy list is to use IP address in one user interface and DNS name in the other.

To discover a Windows proxy:

1. Select **Discovery** > **Setup** on the management server.

2. Click the **Windows Proxy** tab.
3. Enter the following information for the Windows proxy:

Important: A primary key violation error is displayed when you have the same IP address or DNS name listed in both the Discovery list (**Discovery** > **Setup**) and in the Windows Proxy list. If you have already entered the IP address for a host into the discovery list (**Discovery** > **Setup**), provide its DNS name in the Windows Proxy list. Likewise, if the DNS name for a host is listed in the Discovery list, provide its IP address in the Windows Proxy list.

   - **IP Address/DNS Name** - The IP address or DNS name used to access the host running the Windows proxy.
   - **User Name** - The user name of an account used to access the host running the Windows proxy.
   - **Password** - The password of an account used to access the host running the Windows proxy.
   - **Verify Password**
4. Click **OK**.
5. Click the **IP Addresses** tab.
6. Add the hosts and applications as described in the topic, Chapter 16, “Discovering Applications and Hosts” on page 285.
7. Click **Start Discovery** if you have already added your hosts and applications for discovery.

Configuring Windows Proxy Authentication

To discover the Windows proxy, the management server requires by default the password and user name of the administrator's account of the host. If you do not want to use the administrator's password for discovery, you can modify the `winproxy.conf` file so that another user name and password can be used. The following options are available to you:

- **Create another Windows account for the host** - You can provide a user name and password other than the administrator's for discovery. Just create a Windows account for

the host. You must then set the following properties in the `[install_directory]\WindowsProxy\winproxy.conf` file to true: `winproxy.allowAllWindowsUsers` and `winproxy.authenticateWindowsUsers`. After you modify the `winproxy.conf` file, you must restart the AppStorWinProxy service, which is the service for the Windows proxy. Refer to the following example:

```
wrapper.java.additional.7=-Dwinproxy.authenticateWindowsUsers=true
wrapper.java.additional.#=-Dwinproxy.allowAllWindowsUsers=true
```

where # is the next consecutive number in the list of properties, for example `wrapper.java.additional.7`. This number can change based on the number of properties under `# Java Additional Parameters` in the `winproxy.conf` file.

- **Create a user name and password in the winproxy.conf file** - If you do not want to use Windows authentication to create another user account, you can set a user name and password in the `winproxy.conf` file. Although this user name and password can be used to discover the Windows proxy, it cannot be used to log into the host running the Windows proxy. See the following steps for more information on how to set a user name and password in the `winproxy.conf` file.

To set a user name and password in the `winproxy.conf` file:

1. Open the `[install_directory]\WindowsProxy\winproxy.conf` file in a text editor, such as Notepad.
2. Add the following underlined examples after the last line in put in the application parameters as follows:

```
# Application parameters. Add parameters as needed starting from 1
wrapper.app.parameter.1=com.appiq.cxws.main.WmiMain
wrapper.app.parameter.2=-reloading
wrapper.app.parameter.3=-u
wrapper.app.parameter.4=username
wrapper.app.parameter.5=-p
wrapper.app.parameter.6=password
```

where

- `username` is the name of the user account
- `password` is the password for the user account

The numbering must be consecutive. For example, if the last line in `# Application Parameters` ends at 2 you must number the code as follows:

```
wrapper.app.parameter.3=-u
wrapper.app.parameter.4=username
wrapper.app.parameter.5=-p
wrapper.app.parameter.6=password
```

where

- `username` is the name of the user account
- `password` is the password for the user account

3. Restart the AppStorWinProxy service, which is the service for the Windows proxy.

Decreasing the Maximum Java Heap Size

If you run into problems with starting the Windows proxy on Windows XP, decrease the maximum Java heap size for the Windows proxy as follows:

1. Open the `[install_directory]\WindowsProxy\winproxy.conf` in a text editor, such as Notepad.
2. Change the value of the `wrapper.java.maxmemory` property from 1024 to 512 MB, as shown in the following example:
   `wrapper.java.maxmemory=512`
3. Save the `winproxy.conf` file.
4. Restart the AppStorWinProxy service, which is the service for the Windows proxy.

Removing the Windows Proxy

To remove the Windows proxy:

1. Go to the Control Panel in Microsoft Windows.
2. Double-click **Add or Remove Programs**.
3. From the Currently installed programs list, select **HDS Windows Proxy**.
4. Click the **Change/Remove** button.
5. When you are told the product is about to be uninstalled, click **Uninstall**.
6. When the program is done with removing the product, click **Done**.
7. It is highly recommended you reboot the host.

CHAPTER 16

Discovering Applications and Hosts

This chapter describes the following:

- “Step 1 - Discovering Your Hosts” on page 285
- “Step 2 - Setting Up Discovery for Applications” on page 293
- “Step 3 - Discovering Applications” on page 311
- “Changing the Oracle TNS Listener Port” on page 315
- “Adding/Modifying Microsoft Exchange Domain Controller Access” on page 316
- “Changing the Password for the Managed Database Account” on page 317
- “Obtaining Disk Drive Statistics from Engenio Storage Systems” on page 318

Step 1 - Discovering Your Hosts

Before you can discover your applications, you must discover their hosts. You discover hosts in the same way you discovered your switches and storage systems. You provide the host’s IP address, user name and password. The user name and password must have administrative privileges. Unlike switches and storage systems, you must have installed CIM Extension on the host if you want to obtain detailed information about the host.

The management server automatically detects files servers on hosts through discovery. Before you map the topology (Step 2 in Discovery Setup), make sure the option for File Server SRM is selected, as described in “Step B - Build the Topology” on page 291.

Keep in mind the following:

- If you change the password of a host after you discover it, you must change the password for the host in the discovery list. Then, you must stop and restart the CIM Extension running on that host.
- Make sure you have reviewed the table, Table 1-1, “Roadmap for Installation and Initial Configurations,” on page 2 to make sure you are at the correct step.
- If your license lets you discover UNIX and/or Linux hosts, the **Test** button for discovery reports SUCCESS from any UNIX and/or Linux hosts on which the management server can detect a CIM Extension. The CIM Extension must be running. The management server reports “SUCCESS” even if your license restricts you from discovering certain types of hosts. For example, assume your license lets you discover Solaris hosts but not AIX hosts. If you click the **Test** button, the management server reports “SUCCESS” for the AIX hosts. You will not be able to discover the AIX hosts. The IP address is not discoverable, because of the license limitation.
- You should have already installed a CIM Extension on the host you want to discover.
- If the management server is running on Sun Solaris, install and configure the Windows Proxy before starting the steps in this section.
- If you want to receive status reports about Get Details, see “Configuring E-mail Notification for Get Details” on page 382 for information about how to configure this option.
- Depending on your license, you may not be able to access File Server SRM and/or monitor certain applications may not be available. See the List of Features to determine if you have access toFile Server SRM and/or are able to monitor the other applications. The List of Features is accessible from the Documentation Center (**Help** > **Documentation Center**). To learn more about File Server SRM, refer to the File Servers Guide, which is also available from the Documentation Center.
- If you are unable to discover a UNIX host because of DNS or routing issues, see “Unable to Discover a UNIX Host Because of DNS or Routing Issues” on page 404.

Discovery of hosts consists of three steps:

- **Setting up** - Finding the elements on the network. See “Step A - Set Up Discovery for Hosts” on page 287.
- **Topology** - Mapping the elements in the topology. See “Step B - Build the Topology” on page 291.

- **Details** - Obtaining detailed element information. See “Step D - Obtain Details” on page 292.

Step A - Set Up Discovery for Hosts

Note: The steps listed in the following table provide an overview and do not directly correspond to the steps listed in this section.

1. Discover your hosts as described in this section.
2. Build the topology. See “Step B - Build the Topology” on page 291.
3. If you want to view the topology, you can access System Explorer. See “(Optional) Step C - View the Topology” on page 291.
4. Perform Get Details. See “Step D - Obtain Details” on page 292.

Table 16-1: Making the Management Server Aware of Hosts

Step	Description
1	If several of the elements in the same domain use the same name and password, click the **Set Default User name and Password** link and provide up to three user names and passwords.
2	To enter an IP address range, click the **IP Ranges** tab and then the **Add Range** button. If necessary, enter a user name and password for the devices in the range. During a scan of an IP range, the software uses ping; however, ping is not guaranteed to return a response from all devices. If the management server is not able to detect the device during a scan of the IP range, discover the device directly as described in Step 4.
3	Click the **Start Scanning** button. The management server detects targets it can ping and adds them to the IP Address tab automatically. Ping does not guarantee a response. When you start the discovery process, these addresses are included.

Table 16-1: Making the Management Server Aware of Hosts (Continued)

Step	Description
4	If a device was not found during an IP scan, enter an IP address by clicking the **IP Addresses** tab and then the **Add Address** button. If necessary, enter a user name and password for the device.
5	Click the **Start Discovery** button.
6	Run Get Details. See Get Details takes some time. You might want to perform this process when the network and the managed elements are not busy. Click **Discovery** > **Details**.

Keep in mind the following:

- If you started a CIM Extension on a Sun Solaris host with the ./start -users command, the user name provided in the command must be used to discover the host. For example, if you use ./start -users myname:yourname (where myname and yourname are valid UNIX accounts) to start the CIM Extension, myname or yourname and its password must be used to discover the host.
- If you try to discover a Solaris host with multiple IP address, the management server picks only one IP address for discovery.
- To access a Windows-based device, prefix the user name with domain_name\, as shown in the following example. This is required by the Windows login mechanism.
  `domain_name\username`
  where
  - `domain_name` is the domain name of the element
  - `username` is the name of the account used to access that element
- You can configure the management server to obtain information about your master backup servers at a set interval. See the topic, “Scheduling Backup Collection for Master Servers” in the HP SE User Guide for more information about collectors.

To make the software aware of the devices on the network:

1. Click **Discovery** > **Setup**.
2. If several of the elements in the same domain use the same name and password, click the **Set Default User Name and Password** link. Provide up to three user names and passwords.
   The management server tries the default user names and passwords for elements during discovery. For example, if you have a several hosts using the same user name and password, add their user name and password to the list of default user names and

passwords. If one of the hosts is connected to a storage system with another user name and password, you would also add this user name and password to the list. Do not specify the user name and password for the storage system in the individual range because that overrides the default user name and password.

To access a Windows-based device, prefix the user name with domain_name\, as shown in the following example. This is required by the Windows login mechanism.

`domain_name\username`
where

- `domain_name` is the domain name of the element
- `username` is the name of the account used to access that element

3. To add an IP address range to scan:
   a. Click the **IP Ranges** tab.
   b. Click the **Add Range** button.
   c. In the **From IP Address** field, type the lowest IP address in the range of the elements you want to discover.
   d. In the To IP Address field, type the highest IP address in the range of the elements you want to discover.
   e. In the User Name (Optional) field, type the user name.
   To access a Windows-based device, prefix the user name with the Windows domain name, as shown in the following example. It is required by the Windows login mechanism.

   `domain_name\username`
   where

   - `domain_name` is the domain name of the element
   - `username` is the name of the account used to access that element

   f. In the **Password (Optional)** field, type the password corresponding to the user name entered in the User Name field.
   g. Type the password from the previous step in the **Verify Password** field.
   h. In the **Comment** field, type a brief description of the servers. For example, Servers in Marketing.
   i. Click **OK**.
   j. Repeat steps b through i until all of the IP ranges have been entered.
   k. Click the **Start Scanning** button.

The elements the management server detects during the scan are added to the Addresses to Discover list on the IP Addresses tab.

4. To add a single IP address or DNS name to discover:
   a. Click the **IP Address** tab.
   b. Click the **Add Address** button.
   c. In the **IP Address/DNS Name** field, type the IP address or DNS name of the device you want to discover.
   d. In the **User Name (Optional)** field, type the user name.
   This field can be left blank if one or more of the following conditions are fulfilled:
      - The element's user name and password are one of the default user names and passwords.
      - The element does not require authentication.

      To access a Windows-based device, prefix the user name with the Windows domain name, as shown in the following example.

      `domain_name\username`
      where
      - `domain_name` is the domain name of the machine
      - `username` is the name of your network account

   e. In the **Password (Optional)** field, type the corresponding password for the user name entered in the previous step.
   This field can be left blank if one or more of the following conditions are fulfilled:
      - The element's user name and password are one of the default user names and passwords.
      - The element does not require authentication.

   f. If you typed a password in the previous step, retype the password in the **Verify Password** field.
   g. In the **Comment** field, type a brief description of the server. For example, Server Used for Nightly Backups.
   h. Click **OK**.
5. To start discovering elements on the network, click the **Start Discovery** button on the IP Addresses tab.
   The software discovers the IP addresses selected.

   During discovery, the following occurs:

   - The software changes the status light from green to orange.
   - You are shown the Log Messages page. To view the status of discovery, click **Discovery** > **View Logs**.

Discovery is complete when the software displays the DISCOVERY COMPLETED message in the Log Messages field.

Step B - Build the Topology

After you discover elements, the management server requires you build a topology view, which is a graphical representation of port-level connectivity information.

Important: The user interface may load slowly while the topology is being recalculated. It may also take more time to log into the management server during a topology recalculation.

To make the software aware of the devices on the network:

1. Click **Discovery** > **Topology**.
   The discovered elements are selected.
2. Click the **Get Topology** button.
   The management server obtains the topology for selected elements.

   The management server displays the Log Message page. After the management server builds the topology, a link appears to take you to System Explorer so you can verify the topology view. You can also access System Explorer by clicking System Explorer in the left pane.
3. If you see errors in the topology, look at the log messages, which can provide an indication of what went wrong. Look at Event Manager for additional information. Access Event Manager by clicking the Event Manager button in the left pane. To obtain troubleshooting information, see the “Troubleshooting Topology Issues” on page 391.
   If the topology for an element in your network changes, select the element and click **Get Topology** in **Discovery** > **Topology** to updated the information.

   The software obtains just enough information about where the element is connected in the topology, for example a switch connected to a host.

(Optional) Step C - View the Topology

Verify the topology is displayed correctly by accessing System Explorer.

To access System Explorer:

1. Click **System Explorer** button in the left pane.
2. When you are asked if you want to trust the signed applet, click **Always**.
   The **Always** option prevents this message from being displayed every time you access System Explorer, Capacity Explorer, and Performance Explorer.

   The elements are shown connected to each other in the topology.

   If you see a question mark above a host, the management server cannot obtain additional information about that element.

   If a switch has more than one connection to an element, the number of connections is displayed above the line linking the switch and the element. For example, assume the number two is shown between a switch and a storage system. This means the elements have two connections to each other. To view the port details for the connection, right-click the element and select Show Port Details from the drop-down menu. If the topology changes, you can update how the element is viewed in the topology by selecting the element and clicking the Get Topology for Selected button in the Get Topology for discovered elements page (**Discovery** > **Topology**). The management server obtains just enough information about where the element is connected in the topology, for example a switch connected to a host.

   The management server marks an element as “discovered” in the topology if the management server discovers an element but it cannot obtain addition information about it. To learn more about fixing discovered and/or disconnected elements, see the topic, “Troubleshooting Topology Issues” on page 391.

Step D - Obtain Details

After you obtain the topology of the network, you should obtained detailed information from the discovered elements. Get Detailsmust be performed before you can do provisioning and/or obtain provisioning information, such as data about zone sets and LUN numbers.

Keep in mind the following:

- Obtaining details takes some time. You might want to perform this process when the network and the managed elements are not busy. To obtain a picture of device connectivity quickly, click the **Get Topology** button on the Topology tab.
- During Get Details the topology in System Explorer is recalculated. While the topology is being recalculated, the loading of the user interface may be slow. It may also take more time to log into the management server during a topology recalculation.

- If Get Details includes an AIX host, the system log displays three SCSI errors (2 FSCSI error and 1 FCS error) per IBM adapter port. You can ignore these errors.
- You can quarantine elements to exclude them from Get Details. See “Placing an Element in Quarantine” on page 149 for more information. Let us assume you want to discover all the elements in a discovery group, except for one. Perhaps the element you want to quarantine is being taken off the network for maintenance. You can use the quarantine feature to exclude one or more elements from discovery.
- When an element in a given discovery group is updated, its dependent elements are also updated. For example, assume Host_A is the only element in Discovery Group 1. Host_A is connected through a switch and storage system. When you Get Details for Discovery Group 1, you also obtain details from the switch and storage system.
- If the management server unable to obtain information from a UNIX host during Get Details as a result of a CIM Extension hanging, the management server places the access point where the CIM Extension is located in quarantine. The management server then moves onto getting details for the next element in the Get Details table. These UNIX hosts appear as missing until they are removed from quarantine. See “Removing an Element from Quarantine” on page 150 for information on how to remove an element from quarantine.

To obtain details:

1. Click the **Discovery** > **Details** in the upper-right corner.
2. Click the **Get Details** button.
   During Get Details, the software changes its status light from green to red. You can view the progress of gathering details by clicking **Discovery** > **View Logs**.

   When the software completes getting all elements details, it displays GETTING ALL DETAILS COMPLETED on the View Logs page.

For additional information, see “Step 1 - Discover Switches” on page 78 for information on how to automate the gathering of all element details. If you run into problems with discovery, see “Troubleshooting” on page 363.

Step 2 - Setting Up Discovery for Applications

Keep in mind the following when discovering applications:

- Make a list of the applications you want to monitor. Configure your applications first as described in this section and then run discovery.
- You should have already installed a CIM Extension on the hosts that have the applications you want to discover. After you installed the CIM Extension, you should have already discovered the host. See “Step 1 - Discovering Your Hosts” on page 285.

You can configure the management server to monitor hosts and applications, such as Oracle, Microsoft Exchange server, and Sybase Adaptive Server Enterprise, in addition to Microsoft SQL servers and file servers. If you want to obtain detailed information about the host and its applications, you must install a CIM Extension on the host, as described in the previous chapters.

The following is an overview of what you need to do. It is assumed you have already discovered the hosts running your applications. See “Step 1 - Discovering Your Hosts” on page 285.

Then, set up the configurations for your applications on the management server. Some applications may require you to provide additional discovery information about the application. Finally, perform discovery, (discovery from SE only) map the elements in the topology, and then Get Details. Get Details takes some time. Perform this step when the network is not busy. More details about the steps mentioned above are provided later.

See the following topics for more information:

- “Monitoring Oracle” on page 294
- “Monitoring Microsoft SQL Server” on page 300
- “Monitoring Sybase Adaptive Server Enterprise” on page 306
- “Monitoring Microsoft Exchange” on page 310

Monitoring Oracle

To monitor and manage Oracle, you must do the following:

- “Step A - Create the APPIQ_USER Account for Oracle” on page 295
- “Step B - Provide the TNS Listener Port” on page 298
- “Step C - Set up Discovery for Oracle 10g” on page 298

After you complete these steps, you must discover Oracle, and perform Get Details. See “Step 3 - Discovering Applications” on page 311.

Important: Before you begin these steps, make sure you purchased the module that lets you monitor Oracle. Contact your customer support if you are unsure if you purchased this module.

Step A - Create the APPIQ_USER Account for Oracle

The management server accesses Oracle through the APPIQ_USER account. This account is created when you run the `CreateOracleAct.bat` script on Microsoft Windows or `CreateOracleAct.sh` on UNIX on the computer running the Oracle database you want to monitor. The account has create session and select dictionary privileges to be used with the management server.

Keep in mind the following:

- The `CreateOracleAct.bat` script must run under SYS user.
- Create APPIQ_USER account on Oracle Database you want to monitor, not on the management server.
- You should have already installed the database for the management server.
- Verify that the instance TNS (Transparent Name Substrate) listener is running so that the management server can find the Oracle installation and its instances. For example on Microsoft Windows 2000, you can determine if the instance TNS listener is running by looking in the Services window for OracleOraHome92TNSListener. The name of the TNS listener might vary according to your version of Oracle. Refer to the Oracle documentation for information about verifying if the instance TNS listener is running. You can also verify the listener is running by entering the following at the command prompt: lsnrctl status. If the listener is not running you can start it by typing lsnrctl start on command line.
- Make sure you have all the necessary information before you begin the installation. Read through the following steps before you begin.

To create the Oracle user for management server:

1. Do one of the following:
   - **To run the script on IBM AIX, SGI IRIX, HP-UX, Linux or Sun Solaris**, log into an account that has administrative privileges, mount the CIM Extensions CD-ROM (if not auto-mounted), and go to the `/DBIQ/Oracle/unix` directory by typing the following:

     ```
     # cd /cdrom/cdrom0/DBIQ/Oracle/unix
     ```

where `/cdrom/cdrom0` is the name of the CD-ROM drive

- **To run the script on Microsoft Windows**, go to the `DBIQ\Oracle\win` directory on the CIM Extensions CD-ROM.

Important: You must complete the following steps.

---

2. Verify you have the password to the SYS user account.
   You are prompted for the password for this user account when you run the script.
3. Run the `CreateOracleAct.bat` script on Microsoft Windows or `CreateOracleAct.sh` script on a UNIX operating system on the computer with the Oracle database.
   The script creates a user with create session and select dictionary privilege on a managed Oracle instance.

Note: You can use a remote Oracle client to run this script.

---

4. Specify the Oracle instance name, which must be visible to the client, as the first input when running the script. The script prompts you for the name of the Oracle instance on which to create user for Oracle management packages and the password of the SYS account.
   You are asked to specify the default and temporary tablespaces for APPIQ_USER during the installation. You can enter users as default and temp as temporary if these tablespaces exist in the Oracle Instance.
5. Repeat the previous step for each Oracle instance you want to manage.
   This script does the following in order:
   - Creates the APPIQ_USER account.
   - Grant create session and select on dictionary tables privileges to APPIQ_USER enabling management server to view statistics for the Oracle instances.

Removing the APPIQ_USER Account for Oracle

If you no longer want the management server to monitor an Oracle instance, you can remove the APPIQ_USER account for that Oracle instance by running the `UninstallOracleAct.bat` script on Windows or `UninstallOracleAct.sh` script on the Solaris platform.

Keep in mind the following:

- Before you remove the APPIQ_USER account for an Oracle instance, make sure no processes are running APPIQ_USER for that Oracle instance. The management server uses APPIQ_USER to obtain information about the Oracle database. For example, a process would be using APPIQ_USER if someone was using Performance Explorer to view monitoring statistics about that Oracle instance. One of the ways to make sure APPIQ_USER is not being used is to temporarily remove the host running Oracle (**Discovery** > **Topology**). After you removed the APPIQ_USER account for Oracle, discover and perform Get Details for the host if you want to continue monitoring it.
- If you receive a message about not being able to drop a user that is currently connected while you are removing the APPIQ_USER account for Oracle, re-run the script for removing APPIQ_USER.

To remove the APPIQ_USER account for that Oracle instance:

1. If you plan to remove the management software for Oracle from a Solaris host, do the following:
   a. Log into an account that has administrative privileges.
   b. Mount the CIM Extensions CD-ROM (if not auto-mounted).
   c. Go to the `/DBIQ/Oracle/unix` directory by typing the following:
   `# cd /cdrom/cdrom0/DBIQ/Oracle/unix`
   where /cdrom/cdrom0 is the name of the CD-ROM drive
2. If you plan to remove the management software for Oracle from a computer running Windows, go to the `\DBIQ\Oracle\win` directory on the CD-ROM.
3. Verify you have the password to the SYS user account.
   You are prompted for the password for this user account when you run the script.
4. Run the `UninstallOracleAct.bat` for Windows or UninstallOracleAct.sh script for UNIX platform on the computer with the Oracle database.
5. This script removes the management software for the specified Oracle instance.

   Note: You can use a remote Oracle client to run this script.

6. When you are asked for the Oracle instance name, enter the name of the Oracle instance you do not want the management server to monitor. The name must be visible to the client.
7. Provide the password for the SYS user account.
   The APPIQ_USER account for the specified Oracle instance is removed. The management server can no longer monitor that Oracle instance.

Step B - Provide the TNS Listener Port

If your Oracle instances use a different TNS Listener Port than 1521, change the port as described in the following steps:

1. Select **Discovery** > **Setup**. Then, click the **Applications** tab.
   The TNS Listener Port setting applies to all Oracle instances you monitor.
2. To assign a new port, click the **Create** button for the Oracle Information table.
3. Type the new port number and click **OK.**
4. If necessary, click the  button to remove the old port number.

Important: Monitoring Oracle 10g and Oracle clusters require an additional step. If you are not monitoring Oracle 10g and Oracle clusters, see “Step 3 - Discovering Applications” on page 311.

Step C - Set up Discovery for Oracle 10g

Note: If you are discovering an Oracle cluster, see “Discovering Oracle Clusters” on page 299.

To monitor Oracle 10g, provide additional information as described in the following steps:

1. Select **Discovery** > **Setup**. Then, click the **Applications** tab.
2. Click the **Create** button for the Database Information table.
3. In the **Host IP/DNS Name** field, type the IP address or DNS name of the host running Oracle.
   The **Management IP/DNS Name** field is optional.
4. In the **Server Name** field, type the Oracle System Identifier (SID) of the Oracle database you want to monitor.
5. In the **Port Number** field, type the monitored port.
   If you are not sure of the monitored port, check the listener.ora file of the monitored database application. You can find the listener.ora file in the following directory on the host of the monitored database. Do not look for the listener.ora file on the management server for this information.

```
%ORA_HOME%\network\admin\listener.ora
```

The port can be found in the following code:

```
LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS_LIST =
        (ADDRESS = (PROTOCOL = TCP)(HOST = localhost)(PORT = 1521))
        (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC0))
      )
    )
  )
```

6. Select **ORACLE** from the Database Type menu.
7. Click **OK**.

Discovering Oracle Clusters

Perform the following steps for each node in the cluster:

1. Install the CIM Extension on each node in the cluster.
2. Create the appiq_user account on each node in the cluster. See “Step A - Create the APPIQ_USER Account for Oracle” on page 295.
3. Click **Discovery** > **Setup**. Then, discover the host for the first node by clicking the **Add Address** button and providing the appropriate information for discovering the host, as described in “Adding a Single IP Address or DNS Name for Discovery” on page 73.
4. Discover first Oracle node as follows:
   a. Select **Discovery** > **Setup**. Then, click the **Applications** tab.
   b. Click the **Create** button for the Database Information table.
   c. In the **Host IP/DNS Name** field, type the IP address or DNS name of the host running Oracle.
      In the **Management IP/DNS Name** field, type the IP address the listener is listening on for the Oracle instance. The IP address can be a virtual IP or a host IP. You can find the IP address in the listener.ora file for the monitored database. You can find the listener.ora file in the following directory on the host of the monitored database. Do not look for the listener.ora file on the management server for this information.

      ```
      %ORA_HOME%\network\admin\listener.ora
      ```

   d. In the **Server Name** field, type the Oracle System Identifier (SID) of the Oracle database you want to monitor.

e. In the **Port Number** field, type the monitored port.
If you are not sure of the monitored port, check the listener.ora file of the monitored database application. You can find the listener.ora file in the following directory on the host of the monitored database. Do not look for the listener.ora file on the management server for this information.

Microsoft Windows:

```
%ORA_HOME%\network\admin\listener.ora
```

Sun Solaris:

```
$ORACLE_HOME/network/admin/listener.ora
```

The port can be found in the following code:

```
LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS_LIST =
        (ADDRESS = (PROTOCOL = TCP)(HOST = localhost)(PORT =
1521))
        (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC0))
      )
    )
  )
```

f. Select **ORACLE** from the Database Type menu.

g. Click **OK**.

5. Repeat Steps 3 and 4 for each node in the cluster.

Monitoring Microsoft SQL Server

To manage and monitor Microsoft SQL Servers, you must do the following:

- “Step A - Create the APPIQ_USER for the SQL Server” on page 301
- “Step B - Provide the Microsoft SQL Server Name and Port Number” on page 303

Important: Make sure the Microsoft SQL server database is in “Mixed Mode authentication.” To switch to mixed mode authentication, see “Switching to Mixed Mode Authentication” on page 301.

Switching to Mixed Mode Authentication

Important: Do not make security changes to your Microsoft SQL Server installation unless you are familiar with the security requirements of your site.

Microsoft SQL Server must be running in Mixed Mode Authentication. You can switch to Mixed Mode Authentication as follows:

1. Open SQL Server Enterprise Manager (**Start Menu** > **Programs** > **Microsoft SQL Server** > **Enterprise Manager**).
2. Expand the tree-control until you can see your server.
3. Right-click the server name.
   The SQL Server Properties (Configure) window appears.
4. Click the **Security** tab.
5. For “Authentication,” select **SQL Server and Windows**.
6. For “Startup service account,” select **System Account**

Step A - Create the APPIQ_USER for the SQL Server

The management server accesses SQL Server through the APPIQ_USER account. This account is created when you run the `CreateSQLServerAct.bat` script on Microsoft Windows on the computer running the SQL Server database you want to monitor. The account has create session and select dictionary privileges to be used with the management server.

Keep in mind the following:

- The script must run under SA user. To verify that the SA account is enabled, launch SQL Server’s Query Analyzer tool and attempt to connect to the database as SA with the SA user’s password.
- Obtain the SQL Server name before you run the script
- Create APPIQ_USER account on SQL Server database you want to monitor.
- You should have already installed the database for the management server.
- Make sure you have all the necessary information before you begin the installation. Read through the following steps before you begin.

To create the APPIQ_USER account for SQL Server:

1. To run the script on Microsoft Windows, go to the `DBIQ\sqlserver\win` directory on the CIM Extensions CD-ROM.

   Important: You must complete the following steps.

2. Verify you have the password to the SA user account.
   You are prompted for the password for this user account when you run the script.
3. Run the `CreateSQLServerAct.bat` script on Microsoft Windows on the computer with the SQL Server database.
   The script creates a user with login to master and select privilege on data dictionary tables on a managed SQL Server instance.

   Note: You can use a remote SQL Server isql to run this script.

4. Type the SQL Server instance name, which must be visible to the client, as the first input when running the script. The script prompts you for the name of the SQL Server on which to create user for SQL Server management packages and the password of the SA account. This script does the following in order:
   - Creates the APPIQ_USER account.
   - Grant create session and select on dictionary tables privileges to APPIQ_USER enabling management server to view statistics for the SQL Server.
5. To determine if the appiq_user user was added correctly to your SQL server:
   a. Open SQL Server Enterprise Manager.
   b. Expand the user interface for SQL Server Enterprise Manager. Then, expand the specific SQL Server and select **Security**.
   c. Double-click **Logins** and view the list of users authorized to access the SQL Server.
   d. If appiq_user is not listed, the management server is not able to discover the database.
6. To determine if the SQL Server is ready to accept connections from the management server:
   a. Connect to the SQL Server installation through Query Analyzer using the account “appiq_user” and the password “password.”
   b. Create a sample ODBC datasource for the SQL Server installation using the appiq_user account.

c. Click the **Test** button to test the datasource.

7. Repeat steps 4 through 6 for each SQL Server you want to manage.

Step B - Provide the Microsoft SQL Server Name and Port Number

The server name for the Microsoft SQL server and port number for managing a SQL database must be provided in the following steps:

Important: You must provide the host name in the Host IP/DNS Name field. You cannot use localhost or parenthesis.
If you have name resolutions issues, your server may be discovered; however, your applications will not be discovered. You can addressed the name resolution issues by adding entries within the hosts file on the management server for the systems in question.

When configuring the System Application Discovery Settings for SQL servers, the following needs to be specified as described in the steps within this section:

- **Host IP/DNS Name**: <IP Address>
- **Database Server**: <SQL Server Name>
- **Port Number**: <SQL Port #>
- **Database Type**: SQLSERVER

To add information for discovering a SQL server:

1. Select **Discovery** > **Setup**. Then, click the **Applications** tab.
2. Click the **Create** button for the Database Information table.
3. In the **Host IP/DNS Name** field, type the IP address or DNS name of the host running SQL Server.
4. You can leave the **Management IP/DNS Name** field blank. This field is for Oracle clusters. When you leave the **Management IP/DNS Name** field blank the management server automatically lists the DNS name or IP address of the host under the **Host IP/DNS Name** column and **Management IP/DNS Name** column.
5. In the Database Server field, type the SQL database server name you want to monitor.

The SQL Server name is either the Windows system name (default) or the name specified when the SQL server was installed.

SQL Enterprise Manager displays the SQL server name as one of the following:

- As the name specified at the time the SQL server was installed.
- As the Windows system name (Windows 2000)
- As the local name (Windows 2003)

For example, if a Windows 2003 server called SQLTEST has an IP address of 192.168.2.10 with the default SQL port (1433) and shows the name of (local) within SQL Enterprise Manager, the correct system application discovery settings on the management server would be the following:

- **Host IP/DNS Name**: 192.168.2.10
- **Database Server**: SQLTEST
- **Port Number**: 1433
- **Database Type**: SQLSERVER

6. In the **Port Number** field, type the port that SQL is using. If you do not provide a port number, the management server assumes the SQL server is using port 1433 (default). To determine the correct SQL Port Number that the SQL Server is using, follow these steps:
   a. Open SQL Server Enterprise Manager.
   b. Expand the user interface for SQL Server Enterprise Manager, and then select the specific SQL server. Right-click and then select **Properties** from the drop-down menu.
   c. Click the **Network Configurations** button. On the General Tab, select the TCP/IP entry under the Enabled Protocols section. 'Then, click the **Properties** button.
   d. The resulting window shows you the TCP/IP port your SQL server uses. Provide this port number in the **Port Number** field on the management server.
7. Select **SQLSERVER** from the Database Type menu.
8. Click **OK**.

Important: Perform Get Details for your inputs to take effect. See “Step 3 - Discovering Applications” on page 311.

Removing the APPIQ_USER Account for SQL Server

Important: Before you remove the APPIQ_USER account for the SQL Server databases on a host, make sure no processes are running APPIQ_USER for that SQL Server database. The management server uses APPIQ_USER to obtain information about a SQL Server database. One of the ways to make sure APPIQ_USER is not being used is to temporarily remove the host running SQL Server (**Discovery** > **Topology**). After you removed the APPIQ_USER account for SQL Server, discover and perform Get Details for the host if you want to continue monitoring it.

To remove the APPIQ_USER account for the SQL Server databases on a host:

1. To run the script on Microsoft Windows, go to the `DBIQ\sqlserver\win` directory on the CIM Extensions CD-ROM.

   Important: You must complete the following steps.

2. Verify you have the password to the server administrator user account.
   You are prompted for the password for this user account when you run the script.
3. Run the `UninstallSQLServerAct.bat` script on Microsoft Windows on the computer with the SQL Server database.
4. Type the name of the SQL Server server.
5. Type the password for the server administrator account.
   The account for APPIQ_USER is removed. The management server can no longer monitor the SQL Server databases on this host.

Deleting SQL Server Information

If you do not want the management server to monitor a SQL Server instance, you can remove its information, as described in the following steps:

1. Select **Discovery** > **Setup**. Then, click the **Applications** tab.
2. In the Database Information table, click the  button, corresponding to the SQL Server instance you do not want the management server to monitor.

3. Perform Get Details to make the management server aware of your changes.

Monitoring Sybase Adaptive Server Enterprise

If you want to monitor Sybase Adaptive Server Enterprise you must:

- Create APPIQ_USER account on the database for Sybase
- Provide the database server name and port number
- Discover the application.

The required drivers for Sybase Adapter Server Enterprise were automatically installed along with the management server.

Important: Before you begin these steps, make sure you purchased Sybase IQ, which is the module that lets you monitor Sybase Adaptive Server Enterprise. Contact your customer support if you are unsure if you purchased this module.

Step A - Create the APPIQ_USER account for Sybase

The management server accesses Sybase through the APPIQ_USER account. This account is created when you run the CreateSybaseAct.bat script on Microsoft Windows or CreateSybaseAct.sh on UNIX on the computer running the Sybase database you want to monitor. The account has create session and select dictionary privileges to be used with the management server.

Keep in mind the following:

- The script must run under SA user.
- Obtain the Sybase server name before you run the script
- Create APPIQ_USER account on Sybase Database you want to monitor.
- You should have already installed the database for the management server.
- Make sure you have all the necessary information before you begin the installation. Read through the following steps before you begin.

To create the APPIQ_USER account for the Sybase server:

1. Do one of the following:
   - **To run the script on IBM AIX, SGI IRIX, or Sun Solaris**, log into an account that has administrative privileges, mount the CIM Extensions CD-ROM (if not auto-mounted), and go to the /DBIQ/sybase/unix directory by typing the following:
     `# cd /cdrom/cdrom0/DBIQ/sybase/unix`
     where /cdrom/cdrom0 is the name of the CD-ROM drive
   - **To run the script on Microsoft Windows**, go to the \DBIQ\sybase\win directory on the CIM Extensions CD-ROM.

   Important: You must complete the following steps.

2. Verify you have the password to the SA user account.
   You are prompted for the password for this user account when you run the script.
3. Run the CreateSybaseAct.bat script on Microsoft Windows or CreateSybaseAct.sh script on the UNIX operating system on the computer with the Sybase database.
   The script creates a user with login to master and select privilege on data dictionary tables on a managed Sybase instance.

   Note: You can use a remote Sybase isql to run this script.

4. Type the Sybase instance name, which must be visible to the client, as the first input when running the script. The script prompts you for the name of the sybase server on which to create user for Sybase management packages and the password of the SA account.
5. Repeat the previous step for each Sybase server you want to manage.
   This script does the following in order:
   - Creates the APPIQ_USER account.
   - Grant create session and select on dictionary tables privileges to APPIQ_USER enabling management server to view statistics for the Sybase server.

Removing the APPIQ_USER Account for Sybase

Important: Before you remove the APPIQ_USER account for the Sybase databases on a host, make sure no processes are running APPIQ_USER for that Sybase database. The management server uses APPIQ_USER to obtain information about a Sybase database. One of the ways to make sure APPIQ_USER is not being used is to temporarily remove the host running Sybase (**Discovery** > **Topology**). After you removed the APPIQ_USER account for Sybase, discover and perform Get Details for the host if you want to continue monitoring it.

To remove the APPIQ_USER account for the Sybase databases on a host:

1. Do one of the following:
   - To run the script on IBM AIX, SGI IRIX, or Sun Solaris, log into an account that has administrative privileges, mount the CD-ROM (if not auto-mounted), and go to the /DBIQ/sybase/unix directory by typing the following:
     ```
     # cd /cdrom/cdrom0/DBIQ/sybase/unix
     ```
     where /cdrom/cdrom0 is the name of the CD-ROM drive
   - To run the script on Microsoft Windows, go to the \DBIQ\sybase\win directory on the CD-ROM.

   Important: You must complete the following steps.

2. Verify you have the password to the SA user account.
   You are prompted for the password for this user account when you run the script.
3. Run the UninstallSybaseAct.bat script on Microsoft Windows or UninstallSybaseAct.sh script on the UNIX operating system on the computer with the Sybase database.
4. Type the name of the Sybase server.
5. Type the password for the SA account.
   The account for APPIQ_USER is removed. The management server can no longer monitor the Sybase databases on this host.

Step B - Provide the Sybase Server Name and Port Number

You must provide the Sybase server name and port number for managing the Sybase database in the following steps:

To add information for discovering Sybase Adaptive Server Enterprise:

1. Select **Discovery** > **Setup**. Then, click the **Applications** tab.
2. Click the **Create** button for the Database Information table.
3. In the **Host IP/DNS Name** field, type the IP address or DNS name of the host running Sybase.
4. You can leave the **Management IP/DNS Name** field blank. This field is for Oracle clusters. When you leave the **Management IP/DNS Name** field blank the management server automatically lists the DNS name or IP address of the host under the **Host IP/DNS Name** column and **Management IP/DNS Name** column.
5. In the **Server Name** field, type the Sybase database you want to monitor.
6. In the **Port Number** field, type the port that Sybase is using.
7. Select **SYBASE** from the Database Type menu.
8. Click **OK**.

Important: Perform Get Details for your inputs to take effect. See “Step 3 - Discovering Applications” on page 311.

Deleting Sybase Information

If you do not want the management server to monitor a Sybase instance, you can remove its information, as described in the following steps:

1. Select **Discovery** > **Setup**. Then, click the **Applications** tab.
2. In the Database Information table, click the  button, corresponding to the Sybase instance you do not want the management server to monitor.
3. Perform Get Details to make the management server aware of your changes.

Monitoring Microsoft Exchange

To monitor Microsoft Exchange, you must make the management server aware of domain controller access. After information for controller access has been added, discover Microsoft Exchange, map the topology and perform Get Details. To save time, delay these steps until you have added the configurations for your other applications and hosts.

To monitor Microsoft Exchange, you must:

- Add information for Microsoft Exchange Domain Controller Access
- Discover the application.

Adding Microsoft Exchange Domain Controller Access

To obtain information about your Microsoft Exchange servers, you must provide the user name and password for at least a primary domain controller, in addition to a DNS name, as described in the following steps.

Important: The hosts should recognize the management server by name, as a reverse look-up is required by operating system security as well as Microsoft Exchange.

To provide information about the Microsoft Exchange servers:

1. Select **Discovery** > **Setup**. Then, click the **Applications** tab.
   The information you provide for the primary domain controller and backup domain controller apply to all Microsoft Exchange servers you discover.
2. In the Microsoft Exchange Configuration section, click the **Edit** button.
3. Under the Primary Domain Controller section, perform the following steps:
   a. In the **Host Name** field, type the fully qualified DNS name for the domain controller.
   b. In the **User Name** field, type the user name for accessing the Microsoft Exchange server.
   c. In the **Domain Password** field, type the corresponding password for accessing the Microsoft Exchange server.
   d. In the **Verify Password** field, re-type the password for verification.
4. Under the Backup Domain Controller section, perform the following steps:

a. In the **Host Name** field, type the fully qualified DNS name for the domain controller.
b. In the **User Name** field, type the user name for accessing the Microsoft Exchange server.
c. In the **Domain Password** field, type the corresponding password for accessing the domain controller.
d. In the **Verify Password** field, re-type the password for verification.

5. Click the **OK** button.

Important: You must discover the host running Microsoft Exchange. See “Step 3 - Discovering Applications” on page 311.

Deleting a Microsoft Exchange Domain Controller

To delete a Microsoft Exchange domain controller:

1. Select **Discovery** > **Setup**. Then, click the **Applications** tab.
2. Click the button, corresponding to the domain controller you want to remove.
3. Perform Get Details for your changes to take effect.

Step 3 - Discovering Applications

This step assumes you have already discovered your hosts and provided discovery information for your applications. To discover an application, do the following;

- Detect the application (“Step A - Detect Your Applications” on page 312)
- Obtain topology information about the application (“Step B - Obtain the Topology” on page 313)
- Perform Get Details (“Step C - Obtain Get Details” on page 313)

Keep in mind the following:

- This section assumes you have already set up the discovery configurations for your applications as described in “Step 2 - Setting Up Discovery for Applications” on page 293.

- Make sure you have reviewed the table, Table 1-1, “Roadmap for Installation and Initial Configurations,” on page 2 to make sure you are at the correct step.
- If DNS records for your Microsoft Exchange servers are outdated or missing, the discovery of Microsoft Exchange may fail because Microsoft Exchange is dependant on Active Directory, which is dependant on DNS. Since Active Directory is dependant on DNS, Active Directory replication and Active Directory lookups may fail or contain errors if DNS records are not accurate.
- The management server is unable to discover Oracle on a Windows host if the host is on a private network behind a Windows proxy. The management server can discover the Windows host through the Windows proxy, but the management server is not able to detect Oracle.

Discovery consists of three steps:

- **Setting up** - Finding the elements on the network.
- **Topology** - Mapping the elements in the topology.
- **Details** - Obtaining detailed element information.

Step A - Detect Your Applications

To make the software aware of the applications on the network:

1. Click the **Discovery** > **Setup**.
2. To start discovering elements on the network, click the **Start Discovery** button on the IP Addresses tab.
   The software discovers the IP addresses selected.

   During discovery, the following occurs:

   - The software changes the status light from green to orange.
   - You are shown the Log Messages page. To view the status of discovery, click **Discovery** > **View Logs**.

   Discovery is complete when the software displays the DISCOVERY COMPLETED message in the Log Messages field.

   Keep in mind the following:

   - If DNS records for your Microsoft Exchange Servers are outdated or missing, the discovery of Microsoft Exchange may fail because Microsoft Exchange is dependant on Active Directory, which is dependant on DNS. Since Active Directory is dependant

on DNS, Active Directory replication and Active Directory lookups may fail or contain errors if DNS records are not accurate.

- If you are having problems discovering an element, see “Troubleshooting Discovery and Get Details” on page 380.

Step B - Obtain the Topology

The user interface may load slowly while the topology is being recalculated. It may also take more time to log into the management server during a topology recalculation.

To obtain the topology:

1. Click **Discovery** > **Topology**.
   The discovered elements are selected.
2. Click the **Get Topology** button.
   The management server obtains the topology for selected elements.
3. Select the discovery group from which you want to obtain the topology. If you are obtaining the topology for hosts for the first time, make sure **All Discovery Groups** is selected. You can use discovery groups to break up getting the topology or getting details. For example, instead of obtaining the topology for all of the elements, you could specify that the management server gets the topology for only the elements in Discovery Group 1, thus, saving you time. You add an element to a discovery group by modifying the properties used to discover the element. See “Modifying the Properties of a Discovered Address” on page 135.
4. If you see errors in the topology, look at the log messages, which can provide an indication of what went wrong. Look at Event Manager for additional information. Access Event Manager by clicking the Event Manager button in the left pane. To obtain troubleshooting information, see the “Troubleshooting Topology Issues” on page 391.
   If the topology for an element in your network changes, select the element and click **Get Topology** in **Discovery** > **Topology** to updated the information.

   The software obtains just enough information about where the element is connected in the topology, for example a switch connected to a host.

Step C - Obtain Get Details

Obtain detailed information from the discovered applications as described in this section.

Keep in mind the following:

- Get Details takes some time. You might want to perform this process when the network and the managed elements are not busy.
- During Get Details the topology in System Explorer is recalculated. While the topology is being recalculated, the loading of the user interface may be slow. It may also take more time to log into the management server during a topology recalculation.
- To obtain a picture of device connectivity quickly, click the **Get Topology** button on the Topology tab.
- When you do Get Details that includes an AIX host, the system log displays three SCSI errors (2 FSCSI error and 1 FCS error) per IBM adapter port. You can ignore these errors.
- You can quarantine elements to exclude them from Get Details. See “Placing an Element in Quarantine” on page 149 for more information. Let us assume you want to discover all the elements in a discovery group, except for one. Perhaps the element you want to quarantine is being taken off the network for maintenance. You can use the quarantine feature to exclude one or more elements from discovery.
- If the management server unable to obtain information from an element during Get Details as a result of a CIM Extension hanging, the management server places the access point where the CIM Extension is located in quarantine. The management server then moves onto getting details for the next element in the Get Details table. These elements appear as missing until they are removed from quarantine. See “Removing an Element from Quarantine” on page 150 for information on how to remove an element from quarantine.

To obtain details:

1. Select **Discovery** > **Details**.
2. Select the discovery group from which you want to Get Details. If you are obtaining Get Details for hosts for the first time, make sure **All Discovery Groups** is selected.
   You can use discovery groups to break up getting the topology or Get Details. For example, instead of Get Details for all of the elements, you could specify that the management server gets the element details for only the elements in Discovery Group 1, thus, saving you time. You add an element to a discovery group by modifying the properties used to discover the element. See “Modifying the Properties of a Discovered Address” on page 135.
3. Click the **Get Details** button.
   During Get Details, the software changes its status light from green to red. You can view the progress of gathering details by clicking **Discovery** > **View Logs**.

   When the software completes getting all elements details, it displays GETTING ALL DETAILS COMPLETED on the View Logs page.

Important: If the management server cannot communicate with an application, it labels the application as “Discovered”. The management server could find the application, but it could not obtain additional information about it.

4. Refer to the topic, “Adding a Discovery Schedule” in the User Guide for information about automating the gathering of Get Details. If you run into problems with discovery, see “Troubleshooting” on page 363.

Changing the Oracle TNS Listener Port

The software uses port 1521 by default to communicate with the TNS Listener service on the Oracle server. If your port is different or you use multiple ports, you can assign a new port number.

Important: The hosts should recognize the management server by name, as a reverse look-up is required by operating system security as well as the Oracle Transparent Name Substrate (TNS).

To change this port number or to add ports:

1. Select **Discovery** > **Setup**. Then, click the **Applications** tab.
2. To assign a new port, click the **Create** for the **Oracle Information** table.
3. Type the new port number and click **OK**.
4. If necessary, click the  button to remove the old port number.
5. Verify all elements have been discovered by clicking the **Start Discovery** button.

See “Troubleshooting Discovery and Get Details” on page 380 for more information.

Adding/Modifying Microsoft Exchange Domain Controller Access

To obtain information about your Microsoft Exchange servers, you must provide the user name and password for at least a primary domain controller, in addition to a DNS name, as described in the following steps.

Keep in mind the following:

- The hosts should recognize the management server by name, as a reverse look-up is required by operating system security as well as Microsoft Exchange.
- Make sure you provide just the user name and not the domain name when discovering Microsoft Exchange servers.

To provide information about the Microsoft Exchange servers:

1. Select **Discovery** > **Setup**. Then, click the **Applications** tab.
2. In the Microsoft Exchange Configuration section, click the **Edit** button.
3. Under the **Primary Domain Controller** section, perform the following steps:
   a. In the **Host Name** field, type the fully qualified DNS name for the domain controller.
   b. In the **User Name** field, type the user name for accessing the Microsoft Exchange server.
   c. In the **Domain Password** field, type the corresponding password for accessing the Microsoft Exchange server.
   d. In the **Verify Password** field, re-type the password for verification.
4. Under the **Backup Domain Controller** section, perform the following steps:
   a. In the **Host Name** field, type the fully qualified DNS name for the domain controller.
   b. In the **User Name** field, type the user name for accessing the Microsoft Exchange server.
   c. In the **Domain Password** field, type the corresponding password for accessing the Microsoft Exchange server.
   d. In the **Verify Password** field, retype the password for verification.
5. Click the **OK** button.
6. Verify all elements have been discovered by clicking the **Start Discovery** button.
7. Update the database with element changes. See “Step 1 - Discover Switches” on page 78.

See “Troubleshooting Discovery and Get Details” on page 380 for more information.

Changing the Password for the Managed Database Account

The management server connects to database applications through the use of the APPIQ_USER account, an unprivileged account with read-only privileges. You can change the password the management server uses to connect to database applications, such as Oracle and Sybase. When you change the password of APPIQ_USER, you must change the password of all database applications.

Keep in mind the following:

- Change the password in all database applications before you change the password through the user interface. The passwords must also match.
- You must enter a password in the **Password** and **Verify Password** fields.

To change the password:

1. Select **Discovery** > **Setup**. Then, click the **Applications** tab.
2. Click the **Change Password** button.
3. Verify you have already changed the password of the databases listed on this page.
4. Type a new password in the **Password** field.
   The management server requires the password to have the following characteristics:
   - a minimum of three characters
   - starts with a letter
   - contains only letters, numbers and underscores (_)
   - does not start or end with an underscore (_)
5. Retype the password in the **Verify Password** field.
6. Click **OK**.
7. Verify that the management server can access the database applications by clicking the **Test** button for each database application.

Obtaining Disk Drive Statistics from Engenio Storage Systems

Important: Depending on your license, the ability to obtain disk drives statistics from Engenio storage systems may not be available. See the “List of Features” to determine if you have access to the additional statistics. The “List of Features” is accessible from the Documentation Center (**Help** > **Documentation Center**).

To obtain information about disk drive statistics from Engenio storage systems, you must install a CIM Extension on a host that can access the Engenio storage system. Ensure the proxy host has at least one LUN rendered by each controller of the array. Then, you must make the management server aware of that host, as described in the following steps:

1. Install the CIM Extension on a host that has access to the Engenio storage system.
2. Discover that host.
3. Select **Configuration** > **Performance** > **Data Collection**.
4. Verify the **Data Collection** tab is displayed.
5. Click the **Start** button corresponding with the disk drive statistics for an Engenio storage system.
6. Set the date and time.
7. Type a repeat interval and then select a unit of measurement from the drop-down menu. The repeat interval determines how often the collectors gather the data.
8. Select a proxy host by clicking the **Browse** button.
9. Select a proxy host from the drop-down menu and then click **OK**.
   The management server displays in the drop-down menu only hosts that are running a CIM Extension version 3.5 or later and have access to the corresponding Engenio storage system.

   Note: You can always change the proxy host by returning to this page or by going to the **Properties** tab for an Engenio storage system. Double-click the Engenio storage system in System Explorer. Click the **Properties** tab. Then, click the **Browse** button on the Properties tab.

10. Saving the proxy host may take time. When you are asked if you want to continue, click **OK**.
11. Click **OK** again to set the time for starting the collector.
12. If you do not see any hosts displayed verify you have the latest CIM Extension installed and running on a host that can access the Engenio storage system.

CHAPTER 17

Managing Security

Important: Depending on your license, role-based security may not be available. See the “List of Features” to determine if you have access to role-based security. The “List of Features” is accessible from the Documentation Center (**Help** > **Documentation Center**).

This chapter describes the following:

- About the Security for the Management Server on page 322
- Managing User Accounts on page 329
- Managing Roles on page 338
- Managing Organizations on page 341
- Changing the Password of System Accounts on page 348
- Using Active Directory/LDAP for Authentication on page 349

About the Security for the Management Server

The management server offers security based on roles and organizations. Role-based security determines access to certain functionality depending on the user account assigned to a role. Organizations determine if you can modify an element type, such as hosts. The management server ships with the Everything organization, which lets you modify all element types.

See the following topics for more information:

- “About Roles” on page 322
- “About Organizations” on page 325
- “Planning Your Hierarchy” on page 328
- “Naming Organizations” on page 329

About Roles

The management server ships with several predefined roles that are listed in the following table. These roles determine which components of the software a user can access.

For example, users assigned to the Help Desk role have access to Application Explorer and Event Manager, but not to System Explorer, Provisioning, Policy Manager and Reporter. Likewise, users assigned to the domain administrator role have access to all of the features, as shown in the following table.

Table 17-1: Default Role Privileges

Feature	CIO (Chief Information Officer)	Domain Administrator	Storage Administrator	Server Administrator	Application Administrator	Help Desk
Application Explorer	X	X			X	X
System Explorer	X	X	X	X	X	
Event Manager		X	X	X	X	X
Provisioning		X	X			
Provisioning Administration		X	X			
Capacity Explorer	X	X	X	X	X	
Policy Manager		X	X			
Chargeback	X	X	X			
Business Tools	X	X	X			
Reporter	X	X	X	X	X	
Global Reporter	X	X	X			
File Server SRM		X		X		
Performance Explorer	X	X	X	X	X	
Access CLI		X	X			
Custom Commands		X	X			
System Configuration		X				

Keep in mind the following:

- Users with access to Global Reporter can view all the elements throughout the enterprise, including those on the server running Global Reporter. Grant access to Global Reporter only to those, who should be allowed to view all elements. Users, who had privileges to

Reporter in builds earlier than 3.5, are automatically given access to Global Reporter and thus they can see all elements. You may want to disable this functionality for some users.

- Only users belonging to the Domain Administrators role can add, modify, and delete users, roles, and organizations.
- The domain administrator can only edit active organizations.
- Domain administrators can change the user names and roles of other domain administrators, but they cannot modify their own user name and roles while logged into the management server. Domain administrators can also edit their full name, e-mail, phone, and other details, as well assign and un-assign any organization.
- If the System Configuration option is selected for a role, all users assigned to that role will have administration capabilities, as shown in the following list. If you do not want users belonging to that role to have those capabilities, do not assign the System Configuration option:
  - Schedule discovery
  - Find the CIM log level
  - Save log files, e-mail log files
  - Save the database, backup the database, and schedule a database backup
  - Configure Event Manager, File Server SRM and Performance Explorer
  - Configure reports and traps
  - Set up the management server to send e-mail

Roles also restrict access to element properties, element records, and Provisioning, as shown in the following table.

Table 17-2: Default Role Privileges with Elements

Role	Application	Host	Switch	Storage System	Tape Library	Others
CIO	View	View	View	View	View	View
Domain Administrator	Full Control	Full Control	Full Control	Full Control	Full Control	Full Control
Storage Administrator	View	View	Full Control	Full Control	Full Control	Full Control
Server Administrator	View	Full Control	View	View	View	View

Table 17-2: Default Role Privileges with Elements (Continued)

Role	Application	Host	Switch	Storage System	Tape Library	Others
Application Administrator	Full Control	View	View	View	View	View
Help Desk	View	View	View	View	View	View

By selecting one of the following options, users belonging to that role are restricted access:

- **Full Control** - Lets you view and modify the record for the element (Asset Management tab) and perform provisioning if applicable.
- **Element Control** - Lets you view and modify the record for the element (Asset Management tab). Provisioning cannot be performed.
- **View** - Lets you only view element properties.

For example, if a user belongs to a role that only lets you view the element properties on storage systems, that user would not be allowed to perform provisioning on storage systems because their role does not have the **Full Control** option selected for storage systems. That same role could also have the **Full Control** option selected for switches, allowing the user to perform provisioning for switches. Thus, the user would not be able to provision storage systems, but the user would be able to provision switches.

You can modify roles and/or create new ones. For example, you can modify the Help Desk role so that the users assigned to this role can also view Reporter and modify servers.

About Organizations

You can specify which elements users can access. For example, you can specify that some users have only access to certain switches and hosts. However, these users must already be assigned to roles that allow them to see switches and hosts.

Users only assigned to the organization can see just the elements that belong to the organization. If users are assigned to more than one organization, they see all elements that belong to the organizations to which they are assigned. For example, assume you created two organizations: one called OnlyHosts that allowed access to only hosts and another called OnlySwitches that allowed

access to only switches. If you assigned a user to OnlyHosts and OnlySwitches, they would have access to hosts and switches because those elements are listed in at least one of the organizations.

Organizations can also contain other organizations. An organization contained within another is called a child. The organization containing a child organization is called a parent. In the following figure, the BostonWebHosts organization contains two child organizations, BostonWebHost_Windows and BostonWebHost_Solaris. BostonWebHosts is a parent because it contains two organizations.

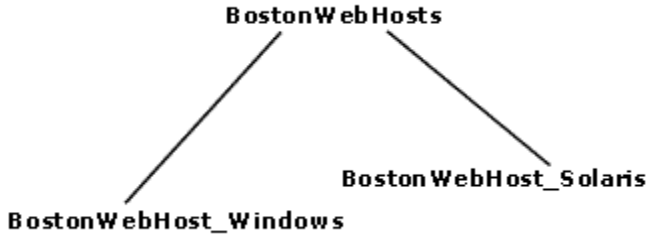


Figure 17-1: Parent-Child Hierarchy for Organizations

If a child contains organizations, it is also a parent. Let's assume you add two organizations called BostonWebMarketing and BostonWebProduction to BostonWebHost_Windows. BostonWebHost_Windows would become a parent because it now contains two organizations. It would also be a child because it is contained in BostonWebHosts.

Parent organizations allow access to all elements listed in their child organizations. For example, users assigned to the organization BostonWebHosts can access not only the elements in BostonWebHost_Windows, but also those in BostonWebHost_Solaris. This is because BostonWebHosts is a parent of the two child organizations.

The parent-child hierarchy for organizations saves you time when you add new elements. You need to add a new element only once. The change ripples through the hierarchy. For example, assume you add an element to BostonWebHost_Windows. Users not only assigned to BostonWebHost_Windows would see this addition, but also users assigned to any of the parent organizations containing BostonWebHost_Windows. For example, users assigned to BostonWebHosts would also see the addition because it contains BostonWebHost_Windows. Users, however, assigned to only BostonWebHost_Solaris would not see the addition.

A child organization can be in multiple parent organizations. As shown in the following figure BostonWebHosts and NYWebHosts are not only children of the WebHosts organization, but they are also children of the US East Coast organization. Assume you have a user that oversees all Web

hosts in the company, you could assign them to the WebHosts organization. Users managing hosts and storage systems on the east coast would be assigned to the US East Coast organization, which is a parent of BostonWebHosts, NYWebHosts, and StorageSystems organizations. Assume an element is added to NYWebHost_Solaris, users assigned to one or more of the following organizations would see the addition:

- NYWebHost_Solaris
- NYWebHosts
- WebHosts
- US East Coast

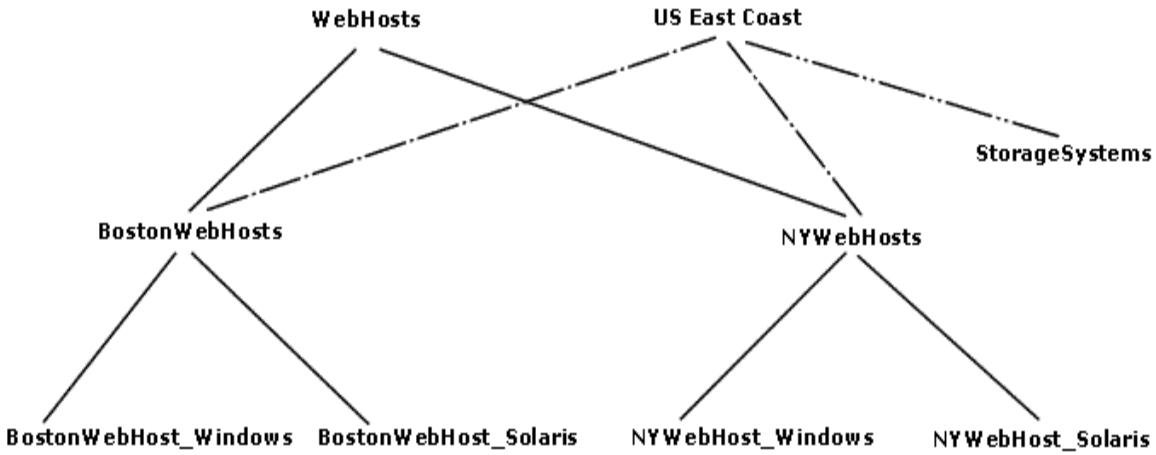


Figure 17-2: Children in Multiple Organizations

When you remove an element from an organization, users belonging to that organization or to one of its parents can no longer access that element if it is not a member of any other organization. For example, assume an element named MyHost was not only a member of BostonWebHost_Solaris, but also had mistakenly became a member of BostonWebHost_Windows. If you remove MyHost from BostonWebHost_Solaris, users belonging to BostonWebHost_Solaris can no longer access the element. Users belonging to the following organizations would still see the element because the element is still a member of BostonWebHost_Windows.

- BostonWebHosts
- WebHosts

- US East Coast

Keep in mind the following:

- You cannot edit the Everything organization.
- Users can only view all elements in the Discovery pages. In all other pages, only the members of the active organization are available.
- Discovery lists (**Discovery** tab) are not filtered. Users can see all elements in the discovery lists regardless of their affiliation with an organization.
- Event Manager displays events from all elements regardless of the user's organization.
- Domain administrators can change the user names and roles of other domain administrators, but they cannot modify their own user name and roles while logged into the management server. Domain administrators can also edit their full name, e-mail, phone, and other details, as well assign and un-assign any organization.
- Reports only display elements assigned to the user's organization, including child organizations. For example, if you attempt to view a Host Summary report and you do not have permission to access hosts through your organization, you are not given information about the hosts in the report. This is also true for e-mailing reports. Let's assume again you do not have permission to access hosts. The reports you e-mail will not contain information about hosts, including the host specific reports. If the users receiving your reports want to be able to view information about hosts, one of the following must happen:
  - The hosts in question must be added to your organization.
  - Someone else, who has the hosts in question already in their organization, must send the reports.

Planning Your Hierarchy

Before you begin creating organizations, plan your hierarchy. Do you want the hierarchy to be based on location, departments, hardware, software or tasks? Perhaps you want a combination of these options.

To help you with your task, create a table of users who manage elements on the network and the elements they must access to do their job. You might start seeing groups of users who oversee the same or similar elements. This table may help you in assigning users to the appropriate organizations.

Once you are done with planning your hierarchy, draw the hierarchy in an graphics illustration program, so you can keep track of which organizations are parents and children.

Create the child organizations first, then their parents. See the topic, “Adding an Organization” on page 341 for more information.

Naming Organizations

When you create an organization, give it a name that reflects its members. For example, you might want to use one or more of the following as a guideline:

- Type of elements that are members of the organization, such as switches, Sun Solaris hosts
- Location of the elements, such as San Jose
- Task, such as backup machines

You may find that it is easy to forget which containers are parents and children. When you name an organization, you might want to include a portion of the name of the dominant parent organization. For example, assume you have two types of Web hosts in Boston: Microsoft Windows and Sun Solaris. You might name the two children organizations BostonWebHost_Windows and BostonWebHost_Solaris and their parent, BostonWebHosts.

Managing User Accounts

This section discusses the following topics:

- Adding Users on page 329
- Editing a User Account on page 331
- Changing the Password for a User Account on page 332
- Changing Your Password on page 333
- Deleting Users on page 333
- Modifying Your User Profile on page 333
- Modifying Your User Preferences on page 334
- Viewing the Properties of a Role on page 336
- Viewing the Properties of an Organization on page 337

Adding Users

To access the management server, users must enter a user name and password. Only users belonging to the Domain Administrator role can add users.

Keep in mind the following:

- Only users belonging to the Domain Administrator role can add users.
- The user name and password should be alpha-numeric. They cannot exceed more than 256 characters. The user name cannot begin with a number.

To create an account:

1. Click **Security** > **Users**.
2. Click the **New User** button.
3. In the **Login Name** field, type a name for the user account, for example: jsmith
   This name becomes the user name for the account.
4. (Optional) In the **Full Name** field, type a full name for the account.
   This information is used to provide a correlation between an account name and a user.

   The full name can contain spaces, but it cannot be longer than 512 characters.
5. Assign the user account to a pre-existing role by selecting a role from the **Role** drop-down menu. See “About the Security for the Management Server” on page 322 for more information about roles.
6. (Optional) In the **E-mail** field, type the user's e-mail address.
7. (Optional) In the **Phone** field, type the user's phone number.
8. (Optional) In the **Notes** field, provide additional information about the user.
9. (Optional) In the **Password** field, type a password for the user account.

   Note: If you do not want to require the user to enter a password or the user will be using a password stored in Active Directory/LDAP, leave this field blank.

10. (Optional) In the **Verify Password** field, type the password you entered previously.
11. Assign the user account to one or more organizations.
    The organizations determine which elements the user can manage. To assign a user account to an organization, select the organizations from the table. See “About the Security for the Management Server” on page 322 for more information about roles and organizations, including the parent-child hierarchy.

12. Click **OK**.

Editing a User Account

Keep in mind the following:

- Only a user belonging to the Domain Administrator role is allowed to edit user accounts.
- The “admin” account acts differently than the other accounts. You cannot add or remove organizations from the “admin” account. You cannot remove the Everything organization from the “admin” account. New organizations are automatically added to the “admin” account when they are created.
- Although the domain administrator can see organization, user and role pages, the domain administrator can only edit active organizations.
- Domain administrators can change the user names and roles of other domain administrators, but they cannot modify their own user name and roles while logged into the management server. Domain administrators can also edit their full name, e-mail, phone, and other details, as well assign and un-assign any organization.
- This change takes effect immediately, even if the user is logged into the management server.
- You cannot change the password for a user account that has been authenticated against Active Directory/LDAP. To change the password for the user account, use Active Directory/LDAP. See “Step 3 - Add Users to the Management Server” on page 360.

If you want to change your password, follow the steps in “Changing Your Password” on page 333.

To modify a user account:

1. Click **Security** > **Users**.
2. Click the **Edit** button () corresponding to the user account you want to modify.
3. To change the account name, type a new name for the user account in the **Name** field, for example: jsmith
   This name becomes the user name for the account.
4. To change the name assigned to the user account, type a new full name for the account in the **Full Name** field.
   This information is used to provide a correlation between an account name and a user.
5. To change the role assign the user account, select a new role from the **Role** drop-down menu.

6. To change the e-mail address listed, type a new e-mail address in the **E-mail** field.
7. To change the phone number listed, type the user's new phone number in the **Phone** field.
8. Change or remove information from the **Notes** field if necessary.
9. To change the password:
   a. Click the **Change Password** button.
   b. Type a new password in the **Password** field.
   c. Type the password again In the **Verify Password** field.
   d. Click **OK**.
10. To change the organizations to which the user belongs, select or deselect the organizations from the table in the user interface.
    The Everything organization is the default organization that lets users access all current and future elements.
11. Click **OK**.

Changing the Password for a User Account

To change the password for accessing the management server:

Keep in mind the following:

- Only a user belonging to the Domain Administrator role is allowed to change the password of another user.
- This change takes effect immediately, even if the user is logged into the management server.
- If a user account has been authenticated against Active Directory/LDAP, you cannot use the management server to change that user's password. You must use Active Directory/ LDAP to change the password instead.

To modify a password:

1. Click **Security** > **Users**.
2. Click **Users** from the drop-down menu.
3. Click the **Edit** button () corresponding to the user account you want to modify.
4. Click the **Change Password** button.
5. Type a new password in the **New Password** field.
6. Type the password again in the **Verify Password** field.

7. Click **OK**.

Changing Your Password

Note: You cannot use the management server to change your password if your user name has been authenticated against Active Directory/LDAP. See “Step 3 - Add Users to the Management Server” on page 360 for more information.

To change your password used for accessing the management server:

1. Click the name of your account in the upper-left corner.
2. On the **User Profile** tab, click the **Change Password** button.
3. Type a new password in the **New Password** field.
4. Type the password again In the **Verify Password** field.
5. Click **OK**.
6. Click the **Save Changes** button on the **User Profile** tab.
   Your password used to access the management server is changed immediately.

Deleting Users

Keep in mind the following:

- You cannot delete the admin account.
- Only users belonging to the Domain Administrator role can delete users.

To delete a user account:

1. Click **Security** > **Users**.
2. Click the corresponding **Delete** button ().
   The user account is deleted.

Modifying Your User Profile

While you are logged into the management server, you can change the following aspects of your user profile:

- Full Name
- E-mail address
- Phone number
- Password

However, you are not allowed to modify the following information:

- Login Name
- Role
- Organization affiliation

If you want this information modified, contact your domain administrator. Your domain administrator makes these changes.

To modify your user profile, do the following:

1. Click the name of your account in the upper-left corner.

Figure 17-3: Changing Your User Profile

2. On the **User Profile** tab, modify one or more of the following:
   - **Full Name**
   - **E-mail address**
   - **Phone number**
   - **Password** - To change the password, click the **Change Password** button. See “Changing Your Password” on page 333. This feature is not available if your user name has been authenticated against Active Directory or LDAP. Use Active Directory/ LDAP to change your password instead.
3. When you are done with your modifications, click the **Save Changes** button.

Modifying Your User Preferences

Use the **User Preference** tab to modify your user preferences for System Explorer, Element Topology, and Event Manager. The **User Preference** tab controls what is displayed for your user account.

To access the **User Preferences** tab:

1. Click the name of your account in the upper-left corner.

Figure 17-4: Accessing the User Preferences Tab

2. Click the **User Preferences** tab.

Note: You can also access the **User Preference** tab by clicking the **Preferences** link in Event Manager.

System Explorer and Element Topology Preferences

To change the severity icons you view in System Explorer and in the element topology, select a severity level from the **Display Severity icons with this severity level or higher drop-down** menu.

If you want events refreshed within a time period, select the **Refresh events automatically** field. Then, enter in minutes how often you want the event information on the screen updated. If this option is set to every five minutes, the management server refreshes the severity icons displayed in System Explorer and the element topology every five minutes.

Event Manager Preferences

Preferences for Event Manager can also be accessed from the **Preferences** link in Event Manager.

Use the following table as a guideline for changing your user preferences for Event Manager.

Table 17-3: Changing User Preferences for Event Manager

If you want...	Do the following...
To be reminded whenever you change a filter	Select the option, **Always remind me to apply filters when I change them**.
Events refreshed automatically	Select the option, **Refresh events automatically**. Then, enter how often in minutes you want events refreshed.
Change the number of events displayed on each page	Select the number of events to appear on a page from the **Number of Events** combo box.
Change the severities to be included	Select a severity level you want displayed in Event Manager from the **Severities to be Included** drop-down menu. If you want to customize the filter for the severity levels, click the **Custom** button.
Change the element types to be included	Select the element types you want to be included from the **Element types to be included** drop-down menu. Events from these elements are displayed in Event Manager. If you want to customize the filter for the element types, click the **Custom** button.

Warnings for Slow Systems Operations

By default, the management server warns you when it encounters issues with handling large amounts of data from storage systems, such as long load times.

If you do not want to be warned, clear the **Warn about slow storage system operations** option on the **User Preferences** tab. See “Modifying Your User Preferences” on page 334 for information on how to access the **User Preferences** tab.

Viewing the Properties of a Role

You can quickly determine which components a user can access by viewing the properties of the user's role. Only users belonging to the Domain Administrator role can view the properties of roles.

To view the properties of a role:

1. Click **Security** > **Users**.
2. In the **Role** column, click the name of the role.

This page displays the following information:

- **Role Name** - The name of the role. This name appears in the users table (**Security** > **Users**)
- **Role Description** - A description of the role.
- **Access Level** - Determines how much access the user has to a type of element, such as hosts, storage systems, switches, and applications. See “About the Security for the Management Server” on page 322 for more information.
- **Access to the <product name>** - Determines which components in the management server the user can access, where `<product name>` is the name of your product.

To learn how to edit a role, see the topic, “Editing Roles” on page 339.

Viewing the Properties of an Organization

You can quickly determine which elements a user can access by viewing the properties of the user's organization. Only users belonging to the Domain Administrator can view the properties of an organization.

1. Click **Security** > **Users**.
2. In the **Organization** column, click the name of a organization.
3. To determine which elements are in a child organization, click the link of the child organization.
4. To learn more about an element, click the element's link.

This page displays the following information:

- **Name** - The name of the organization. This name appears in the users table (**Security** > **Users**)
- **Description** - A description of the organization

- **Organization Members** - Determines which elements the user can access. See “About the Security for the Management Server” on page 322 for more information.

To learn how to edit an organization, see the topic, “Editing Organizations” on page 343.

Managing Roles

This section discusses the following topics:

- Adding Roles on page 338
- Editing Roles on page 339
- Deleting Roles on page 340

Adding Roles

The management server ships with several roles. You can add roles to accommodate your organization. For example, you might want to add a role for quality assurance. See the topic, “About the Security for the Management Server” on page 322 for more information about roles and organizations.

Keep in mind the following:

- The **Role Name** and **Description** fields do not accept special characters, except spaces and the following characters: $, -, ^, ., and _
- Only users belonging to the Domain Administrator role can add roles.

To add a role:

1. Select **Security** > **Roles**.
2. Click the **New Role** button.
3. In the **Role Name** field, type a name for the role. For example: Quality Assurance.
   The name can contain spaces, but it cannot be longer than 256 characters.
4. In the **Description** field, type a description for the role. For example: Role for those in quality assurance.
   You cannot type more than 1024 characters in the **Description** field.

5. Select an access level for each element type:
   - **Full Control** - Lets you view and modify the record for the element (Asset Management tab) and perform provisioning.
   - **Element Control** - Lets you view and modify the record for the element (Asset Management tab).
   - **View** - Lets you view element properties.

   For example, if a user belongs to a role that only lets you view the element properties on storage systems, that user would not be allowed to perform provisioning on storage systems because their role does not have the **Full Control** option selected for storage systems. That same role could also have the **Full Control** option selected for switches, allowing the user to perform provisioning for switches. Thus, the user would not be able to provision storage systems, but the user would be able to provision switches.
6. Select the features you want a user to be able to access. For example, if you want a user to have access to System Explorer, select System Explorer from the list.
   See “Management Server Components” on page 7 for more information about these features.
7. Click **OK**.

Editing Roles

The software lets you modify the default roles and/or the roles you have created. See the topic, “About the Security for the Management Server” on page 322 for more information about roles and organizations.

Keep in mind the following:

- Only users belonging to the Domain Administrator role can modify roles.
- Domain administrators can change the user names and roles of other domain administrators, but they cannot modify their own user name and roles while logged into the management server. Domain administrators can also edit their full name, e-mail, phone, and other details, as well assign and un-assign any organization.
- After you click the **OK** button in the Edit Role window, any users assigned to the role you edited are logged out of the management server. Users see the changes when they log back into the management server.
- The **Role Name** field does not accept special characters, except spaces and the following characters: $, -, ^, ., and _

To edit a role:

1. Select **Security** > **Roles**.
2. Click the **Edit** button ().
3. To edit the name of the role, change the name In the **Role Name** field.
   The name can contain spaces, but it cannot be longer than 256 characters.
4. To edit the description of the role, change the description in the **Description** field.
   You cannot type more than 1024 characters in the **Description** field.
5. To change the access level, change the options selected in the table.
   - **Full Control** - Lets you view and modify the record for the element (Asset Management tab) and perform provisioning.
   - **Element Control** - Lets you view and modify the record for the element (Asset Management tab).
   - **View** - Lets you view element properties.

   For example, if a user belongs to a role that only lets you view the element properties on storage systems, that user would not be allowed to perform provisioning on storage systems because their role does not have the **Full Control** option selected for storage systems. That same role could also have the **Full Control** option selected for switches, allowing the user to perform provisioning for switches. Thus, the user would not be able to provision storage systems, but the user would be able to provision switches.
6. Select the features you want a user to be able to access. For example, if you want a user to have access to System Explorer, select System Explorer from the list.
   See “Management Server Components” on page 7 for more information about these features.
7. Click **OK**.

Deleting Roles

Keep in mind the following:

- A role cannot be deleted if it contains a user.
- Only users belonging to the Domain Administrator role can delete roles.

To delete a role:

1. Select **Security** > **Roles**.
2. Click **Roles** from the drop-down menu.

3. Click the corresponding **Delete** button ().
   The role is deleted.

Managing Organizations

This section discusses the following topics:

- Adding an Organization on page 341
- Viewing Organizations on page 343
- Editing Organizations on page 343
- Deleting an Organization on page 344
- Removing Members from an Organization on page 345
- Filtering Organizations on page 346

Adding an Organization

You can create new organizations to restrict access to certain elements. For example, assume you do not want the help desk to have access to elements belonging to a certain group. You could create an organization that does not allow access to those elements. Once you assign users to that organization, they would only be able to access the elements you specified.

See the topic, “About the Security for the Management Server” on page 322 for more information about roles and organizations.

Keep in mind the following:

- Create child organizations first, then their parents.
- Event Manager displays events from all elements regardless of the user’s organization.
- Only users belonging to the Domain Administrator role can add organizations. Only active organizations can be edited.
- All discovered elements are accessible in Business Tools, regardless of a user's restrictions. For example, assume your account belongs to an organization that has only hosts as members. If you run the business tool Switch Risk Analysis, the management server still provides information about whether the switches are a risk in your environment.

To add an organization:

1. Select **Security** > **Organizations**.
2. Click the **New Organizations** button.
3. In the **Name** field, type a name for the organization.
   The name of an organization has the following requirements:
   - Can contain spaces.
   - Can add digits to the beginning of an organization's name.
   - Cannot be longer than 256 characters.
   - Cannot contain the carot (^) symbol—currently the system allows the carot symbol to be entered, but the carot symbol should not be included in an organization's name.
4. In the **Description** field, type a description for the organization.
   You cannot type more than 1024 characters in the **Description** field.
5. Click the **Add or Remove Members** button to determine which elements the user will see.
6. To add elements, expand the Element Types node in the tree. Select the element type that you would like to add. Then, in the right-hand pane, select the elements you would like to add by clicking the appropriate check boxes. Next, click the **Add** button and the selected elements are added to the Organization Members pane. If you would like to add storage volumes to the organization, see the topic "Adding Storage Volumes to an Organization" on page 342.
7. To add organizations, select the Organizations node. Then, in the right-hand pane, select the organizations you would like to add by clicking the appropriate check boxes. Next, click the **Add** button and the selected organizations are added to the Organization Members pane. The organizations in the Organization Members pane are listed as child organizations because they are now contained within the organization you are creating. See the topic, "About the Security for the Management Server" on page 322 for more information.
8. Once you are done adding the elements and organizations, click **OK**.

Adding Storage Volumes to an Organization

Only users belonging to the Domain Administrator role can add storage volumes to an organization.

To add storage volumes to an organization:

1. Click the **Add or Remove Members** button.
2. Expand the Element Types node in the tree and select the Storage Systems node.

3. In the right-hand pane, click the **Storage Volumes** tab and select a storage system from the **Showing Volumes for Storage System** drop-down menu.
4. If you want to filter the list of volumes for a storage system, click the **Show Volume Filter** link, select the appropriate filter criteria, and click the **Submit Query** button.
5. Select the storage volumes you want to add to the organization. Click the **+Ports** link in the **Ports** column if you want to see a list of the ports associated with a particular volume.
6. When you are finished selecting volumes, click the **Add** button located at the top of the pane. The selected volumes are added to the Organization Members pane. Click the **OK** button.

Viewing Organizations

The Setup Organizations page lists the organizations and their descriptions, in addition to the number of top-level elements, users and child organizations assigned to each organization.

Only users belonging to the Domain Administrator role can view organizations.

The No. of Top Level Elements column provides the total number of elements assigned to an organization, not including those within the child organization. An organization containing only child organizations displays 0 under the No. of Top Level Elements column; however, users assigned to that organization would have access to the elements assigned to its child organizations.

Assume an organization contains only two child organizations. As a result, 0 would be displayed under the No. of Top Level Elements column. Users assigned to that organization can access the elements assigned to the two child organizations.

Access the Setup Organizations page by clicking **Security** > **Organizations**.

You can access information about child organizations by clicking their link under the Child Organization column.

Editing Organizations

See the topic, “About the Security for the Management Server” on page 322 for more information about roles and organizations.

When elements are removed from an organization, users belonging only to that organization are no longer able to access the removed elements.

Keep in mind the following:

- Depending on your license, role-based security may not be available. See the “List of Features” to determine if you have access to role-based security. The “List of Features” is accessible from the Documentation Center (**Help** > **Documentation Center**).
- Only users belonging to the Domain Administrator role can edit organizations. Only active organizations can be edited.
- The **Name** and **Description** fields in the Edit Organization window do not accept special characters, except spaces and the following characters: $, -, ., and _
- The organization name can contain spaces, but it cannot be longer than 256 characters.
- You cannot edit the Everything organization.

To edit an organization:

1. Select **Security** > **Organizations**.
2. Click the  button.
3. To change the name of the organization, type a new name in the **Name** field.
   The name of an organization has the following requirements:
   - Can contain spaces.
   - Can add digits to the beginning of an organization’s name.
   - Cannot be longer than 256 characters.
   - Cannot contain the carot (^) symbol—currently the system allows the carot symbol to be entered, but the carot symbol should not be included in an organization’s name.
4. To change the description of the organization, type a new description in the **Description** field.
   You cannot type more than 1024 characters in the **Description** field.
5. Click the **Add or Remove Members** button.
6. Add and remove elements as described in the topics, “Adding an Organization” on page 341 and “Removing Members from an Organization” on page 345.
7. Once you are done adding or removing elements, click **OK** in the Add Organization page.
8. In the Edit Organization page, click **OK**.

Deleting an Organization

When an organization is removed, users assigned only to that organization are no longer able to access the elements in the removed organization. For example, assume you belong to two organizations, onlyHosts and onlySwitchesandHosts. The organization onlyHosts contains only hosts, and the organization onlySwitchesandHosts contains only switches and hosts. If you delete the onlySwitchesandHosts organization, you will still have access to hosts because you still belong to the onlyHosts organization.

Keep in mind the following:

- You cannot remove the Everything organization, which is the default organization.
- You cannot delete an organization that contains a user, who belongs to no other organizations. For example, assume you create an organization named Org1 that contains two users: User1 and User2. User1 belongs to two other organizations, while User2 only belongs to the organization you just created. You will not be able to delete Org1 because the organization contains User2, who only belongs to the organization you are trying to delete.
- Only users belonging to the Domain Administrator role can delete organizations.

Depending on your license, role-based security may not be available. See the “List of Features” to determine if you have access to role-based security. The “List of Features” is accessible from the Documentation Center (**Help** > **Documentation Center**).

To delete an organization:

1. Click **Security** > **Organizations**.
2. Click the button corresponding to the organization you want to remove.
   The software removes the organization.

Removing Members from an Organization

When you remove an element from an organization, users belonging to that organization or to one of its parents can no longer access that element if it is not a member of any other organization. For example, assume an element named MyHost was not only a member of BostonWebHost_Solaris, but also had mistakenly became a member of BostonWebHost_Windows. If you remove MyHost from BostonWebHost_Solaris, users belonging to BostonWebHost_Solaris can no longer access the element. Users belonging to the BostonWebHost_Windows organization or to its parent would still see the element.

Important: Depending on your license, role-based security may not be available. See the “List of Features” to determine if you have access to role-based security. The “List of Features” is accessible from the Documentation Center (**Help** > **Documentation Center**).

Use one of the following methods to remove an element from an organization:

- In the Edit Organization window, click the  button corresponding to the element or child organization you want to remove from the organization.
- In the Add or Remove Organization Members window, select the element or child organization you want to remove by clicking the appropriate check box. Next, click the **Remove** button.
- Only users belonging to the Domain Administrator role can remove members from an organization. Only active organizations can be edited.

Filtering Organizations

The management server provides a filtering feature that lets you designate which organizations are active in your view. For example, assume you belong to an organization name Hosts and this organization contains two organizations: “Windows Hosts” and “Solaris Hosts.” If you want to view elements only in “Windows Hosts” and not in “Solaris Hosts” organizations, you could use the filtering feature to activate only the “Windows Hosts” organization.

Keep in mind the following:

- Users assigned to the “admin” account cannot filter organizations because the “admin” account belongs to the Everything organization by default. As a result, these users do not have access to filtering feature for organizations.
- If you do not want to view an element, deselect all child organizations containing the element. You must also deselect all parent organizations containing the child organization that has that element. For example, assume you do not want to view all Solaris hosts and all Solaris hosts are in the “Solaris Hosts” organization. The “Solaris Hosts” organization is contained in the Hosts organization. You must deselect the “Solaris Hosts” organization and the Hosts organization if you do not want to see Solaris hosts.
- The filter for organizations does not appear in Event Manager. Event Manager displays events from all elements regardless of the user’s organization.

- If you do not select any organizations for filtering, you do not see any elements in the topology.

To filter organizations:

1. Click the button at the top of the screen, or click the link listing the organizations you can view.

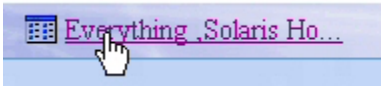


Figure 17-5: Clicking the Organization Link

2. Deselect the organizations containing the elements you do not want to obtain information about. Assume you want to view only the elements in the “Windows Hosts” organization, you would select only “Windows Hosts.” Let's assume you have a parent organization named “Hosts” that contains “Solaris Hosts” and “Windows Hosts.” You would need to deselect “Solaris Hosts” and “Hosts.” “Hosts” would need to be deselected because it contains organizations other than “Windows Hosts.”
   Links are displays for the organizations if you belong to the Domain Administrator role. To learn more about the contents of an organization, click its link.

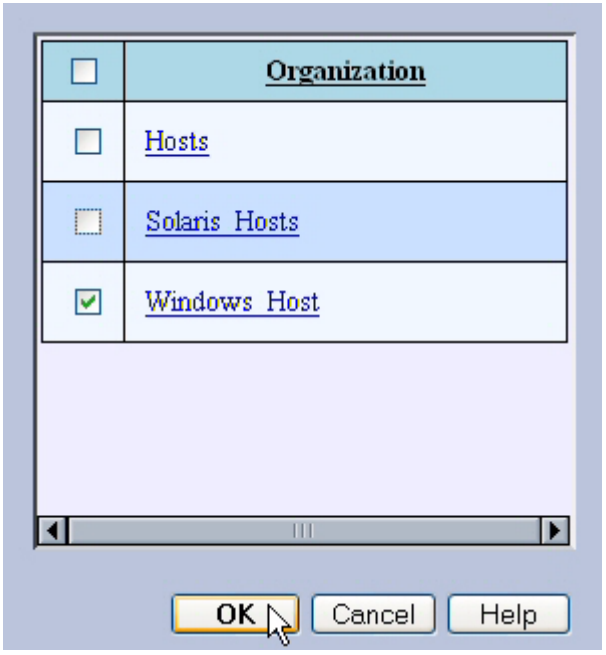


Figure 17-6: Filtering Organizations

3. Click **OK**.
   You can now only obtain information about elements in the active organizations. The active organizations are listed in the link next to the filter button, as shown in the following figure.

Figure 17-7: Active Organization

Changing the Password of System Accounts

The management server uses the following accounts to access and manage the database for the management server. You should change the passwords to these accounts to prevent unauthorized access.

- **SYS** - Used for the management server database creation and upgrade. Default password: `change_on_install`
- **SYSTEM** - Used for management server database creation and upgrade, in addition to database import, export and re-initialization. Default password: `manager`
- **RMAN_USER** - Used for RMAN backup and restore. This user has sys privilege. Default password: `backup`
- **DB_SYSTEM_USER** - Used for all the database activity, including establishing a connection to the management server database. Default password: `password`

You must change the passwords of the SYS, SYSTEM, RMAN_USER, and DB_SYSTEM_USER accounts by using the `dbadmin.bat` tool, so the management server is aware of the changes. Do not change the password for one of these accounts by using Oracle. Make sure you keep the new passwords in a safe location, as it is your responsibility to remember the Oracle passwords.

The management server requires the password to have the following characteristics:

- a minimum of three characters
- starts with a letter
- contains only letters, numbers and underscores (_)
- does not start or end with an underscore (_)

To change the password of a system account:

1. Stop the AppStorManager service.
2. To access the database utility on Solaris, do the following on the management server:

a. Set the display if you are accessing the dbAdmin tool remotely.

b. The dbAdmin tool uses Perl. To set Perl in your path, enter the following command at the command prompt:
`eval `/opt/productname/install/uservars.sh``

where `/opt/productname` is the directory containing the software. It is defined by $APPIQ_DIST.

Important: You must include the back quotes around the full path to uservars.sh in the command.

c. Go to the `$APPIQ_DIST/Tools/dbAdmin` directory and then enter the following at the command prompt:
`perl dbAdmin.pl`

The full path to Perl is the following:
`$APPIQ_DIST/JBossandJetty/server/appiq/remoteScripts/perl/bin/perl`

3. To access the database utility on Windows, go to the `%MGR_DIST%\Tools\dbAdmin` directory on the management server and double-click `dbAdmin.bat`, where `[Install_Dir]` is the directory into which you installed the management server.
4. Click **Change Passwords** in the left pane.
5. Select an account name from the **User Name** combo box.
6. Type the current password in the **Old Password** field.
7. Type the new password in the **New Password** field.
8. Retype the password in the **Confirm Password** field.
9. Click **Change**.
The Database Admin Utility changes the password for the specified account.

Using Active Directory/LDAP for Authentication

The management server supports external authentication through Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) directory services. When you configure the management server to use external authentication, user credentials are no longer stored in the management server database. This configuration centralizes all security related requirements to the

enterprise AD/LDAP infrastructure, such as password expiration, resets, and complexity requirements.

When a user attempts to log into the management server, the management server authenticates the user name and password against AD/LDAP for credential verification. If AD/LDAP verifies this user has the correct credentials, the management server allows this user access to the application.

Keep in mind the following:

- The `login-handler.xml` file contains configuration information for Active Directory and LDAP. It is important you enable either Active Directory or LDAP. You cannot enable both.
- If you want to go back and forth between internal and external (AD/LDAP) authentication, rename the `login-handler.xml` file before you modify it. This way you can easily switch back to internal authentication by changing the file name back to `login-handler.xml`.

To use AD/LDAP to authenticate your users, complete the following sections:

- “Step 1 - Configure the Management Server to Use Active Directory or LDAP” on page 350
- “Step 2 - Restart the AppStorManager Service and Login as the Designated Admin Account” on page 359
- “Step 3 - Add Users to the Management Server” on page 360
- “Step 4 - Provide Login Information to Your Users” on page 360

Step 1 - Configure the Management Server to Use Active Directory or LDAP

You must modify the `login-handler.xml` file if you want to use Active Directory/LDAP. How you modify the `login-handler.xml` file depends on whether you plan to use LDAP or Active Directory.

See the one of the following sections depending on whether you want to use Active Directory or LDAP:

- “Active Directory” on page 351
- “LDAP” on page 355

Active Directory

Active Directory allows by default connections with domain\username, instead of the distinguished name (DN) used by a generic LDAP server. However, you can use the generic LDAP server setup to authenticate with Active Directory, as described in “LDAP” on page 355.

To specify the management server to use Active Directory, do the following:

1. Before switching to Active Directory (AD) authentication mode, the management server needs to be configured with a designated Active Directory user and other AD specific credentials. At startup, the designated Active Directory user is mapped to the built-in “admin” user and overrides it with the Active Directory user information.

   Important: Make sure the administrator account has already been created in Active Directory before you add it to the `login-handler.xml` file.

   a. On the management server look in one of the following locations:
      - **Windows:** %MGR_DIST\Data\Configuration
      - **Solaris:** $MGR_DIST\Data\Configuration

   Note: If you want to go back and forth between internal and external (AD/LDAP) authentication, rename the `login-handler.xml` file before you modify it. This way you can easily switch back to internal authentication by changing the file name back to `login-handler.xml`.

   b. In the `login-handler.xml` file, change the value of the `<AdminAccountName>` tag to the name of a user account in Active Directory, as shown in the following example:

```
<AdminAccountName>domain\PrimaryUser</AdminAccountName>
```

   where `PrimaryUser` is the name of the user account that is designated as the primary user in Active Directory.

   Keep in mind the following:

   - For security reasons, it is recommended that the designated user not be the AD Domain Administrator
   - If you are using Active Directory, prefix the user name with the domain name, for example: `domain\PrimaryUser`

2. In the `login-handler.xml` file, comment out the section that contains `com.appiq.security.server.BasicLoginhandler`, which enables internal authentication mode. Only one login handler is allowed at a time.
   ```
   <!--LoginHandlerClass>com.appiq.security.server.BasicLoginHandler</
   LoginHandlerClass-->
   ```
3. Comment out the `<LoginHandlerType>Default</LoginHandlerType>` tag as follows:
   ```
   <!--LoginHandlerType>Default</LoginHandlerType-->
   ```
4. Uncomment the line containing the class name and login handler type so that it appears as follows:
   ```
   <LoginHandlerClass>com.appiq.security.server.ActiveDirectoryLoginH
   andler</LoginHandlerClass>
   <LoginHandlerType>ActiveDirectory</LoginHandlerType>
   ```
5. Replace `directory.hp.com` with the IP address or the fully qualified DNS name of your primary Domain Controller server in the `login-handler.xml` file, as shown in the following example:
   ```
   <PrimaryServer port="389">192.168.10.1</PrimaryServer>
   ```
   where
   - `192.168.10.1` is the IP address of the primary Domain Controller server running Active Directory.
   - `389` is the port on which Active Directory is running on the server.
6. Replace `directory2.hp.com` with the IP address or the fully qualified DNS name of your secondary Domain Controller server, if available.
   ```
   <SecondaryServer>192.168.10.2</SecondaryServer>
   ```
   where `192.168.10.2` is the IP address of the secondary Domain Controller server running Active Directory.
7. If you want the password to be saved in the management server database, change the value of the `<ShadowPassword>` tags to true, as shown in the following example:
   ```
   <ShadowPassword>true</ShadowPassword>
   ```
   Saving the passwords in the management server database lets a user still log into the management server if the management server is changed back to local mode. This, however, is not recommended as it defeats the purpose of externalizing a user's credentials.

   The `login-handler.xml` file contains two sets of `<ShadowPassword>` tags: one for Active Directory and one for LDAP. Make sure you change the value of the `<ShadowPassword>` tags that are children of the `<ActiveDirectory>` tag.
8. If you want the user name to be case sensitive, change the value of the `<CaseSensitiveUserName>` tag to true, as shown in the following example:

```
<CaseSensitiveUserName>true</CaseSensitiveUserName>
```

If you change the value of `<CaseSensitiveUserName>` to true, the management server becomes case-sensitive to user names. The management server sees MyUserName and myusername as different users.

Important: AD servers are not case sensitive for user names so changing this tag to "true" for AD authentication is not recommended.

The `login-handler.xml` file contains two sets of `<CaseSensitiveUserName>` tags: one for Active Directory and one for LDAP. Make sure you change the value of the `<CaseSensitiveUserName>` tags that are children of the `<ActiveDirectory>` tag.

9. Provide the Active Directory search base in which you want the management server to look up AD/LDAP user attributes. Allow no spaces between commas and put in all components of fully qualified domain name, for example, `hds.usa.com` would be `DC=hds,DC=usa,DC=com`.
   The search base is used to specify the starting point for the search. It points to a distinguished name of an entry in the directory hierarchy.

   ```
   <SearchBase> dc=MyCompanyName,dc=COM</SearchBase>
   ```

10. Save the `login-handler.xml` file with your changes.
    The following is an example of a modified `login-handler.xml` file for use with AD server authentication. Underlined text is information that was modified:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<LoginHandler>
<AdminAccountName>domain\primaryuser</AdminAccountName>
<!-- for the default, using database for authentication -->
<!--LoginHandlerClass>com.appiq.security.server.BasicLoginHandler</
LoginHandlerClass-->
<!--LoginHandlerType>Default</LoginHandlerType-->
<!-- uncomment the following to enable Active Directory login-->
<LoginHandlerClass>com.appiq.security.server.ActiveDirectoryLoginHandler</
LoginHandlerClass>
<LoginHandlerType>ActiveDirectory</LoginHandlerType>

<ActiveDirectory>
<PrimaryServer port="389">IP address of Primary Domain Controller</
PrimaryServer>
<SecondaryServer>IP Address of Secondary Domain Controller</
SecondaryServer>
<ssl>false</ssl>
<ShadowPassword>false</ShadowPassword>
```

```
<CaseSensitiveUserName>false</CaseSensitiveUserName>
<!-- provide SearchBase if full name and email attribute are to be
synchronized
between ActiveDirectory and the database.-->
<SearchBase>DC=domain extension1,DC=domain extension2,DC=COM</SearchBase>
<FullNameAttribute>displayName</FullNameAttribute>
<EmailAttribute>mail</EmailAttribute>
</ActiveDirectory>
<!-- uncomment the following for generic LDAP login
<LoginHandlerClass>com.appiq.security.server.LdapLoginHandler
</LoginHandlerClass>
<LoginHandlerType>LDAP</LoginHandlerType>
-->
<LDAP>
<!-- same as java.naming.provider.url ldap://ldap.companyname.com:389
-->
<Server port="389">IP address of LDAP server</Server>
<!-- LDAP env can be added, an example is shown below...
<LDAPEnv
name="java.naming.factory.initial">com.sun.jndi.ldap.LdapCtxFactory</
LDAPEnv>
-->
<ssl>false</ssl>
<ShadowPassword>false</ShadowPassword>
<CaseSensitiveUserName>false</CaseSensitiveUserName>
<!-- multiple DN entries are allowed, they will be tried one at a time -->
<DN>CN=$NAME$,OU=Engineering,DC=HP,OU=US,DC=COM</DN>
<!-- provide FullNameAttribute and EmailAttribute if full name and email
attribute
are to be synchronized between LDAP and the database -->
<FullNameAttribute>displayName</FullNameAttribute>
<EmailAttribute>mail</EmailAttribute>
</LDAP>
</LoginHandler>
```

When you are done with your changes, the login-handler.xml file, may resemble the following:

```
<LoginHandler>
  <AdminAccountName>domain\primaryuser</AdminAccountName>
  <LoginHandlerClass>
    com.appiq.security.server.ActiveDirectoryLoginHandler
  </LoginHandlerClass>
  <LoginHandlerType>ActiveDirectory</LoginHandlerType>
  <ActiveDirectory>
    <PrimaryServer>IP address of primary domain controller</PrimaryServer>
    <SecondaryServer>IP address of secondary domain controller</
SecondaryServer>
```

```
<ssl>false</ssl>
<ShadowPassword>false</ShadowPassword>
<CaseSensitiveUserName>false</CaseSensitiveUserName>
<SearchBase>DC=MyCompanyName,DC=COM</SearchBase>
    <FullNameAttribute>displayName</FullNameAttribute>
    <EmailAttribute>mail</EmailAttribute>
  </ActiveDirectory>
</LoginHandler>
```

LDAP

The LDAP server requires a distinguished name (DN) and credentials. The DN can be configured, allowing name substitution and support for multiple DN configurations.

To configure the management server to use LDAP:

1. Before switching to LDAP authentication mode, the management server needs to be configured with a designated LDAP user through the `<AdminAccountName> tag`. At startup, the designated LDAP user is mapped to the built-in “admin” user and overrides it with the LDAP user information.

   Important: Make sure the administrator account has already been created in LDAP before you add it to the `login-handler.xml` file.

   a. On the management server look in one of the following locations:
      - **Windows:** %MGR_DIST\Data\Configuration
      - **Solaris:** $MGR_DIST\Data\Configuration

   Note: If you want to go back and forth between internal and external (AD/LDAP) authentication, rename the `login-handler.xml` file before you modify it. This way you can easily switch back to internal authentication by changing the file name back to login-handler.xml.

   b. In the `login-handler.xml` file, change the value of the `<AdminAccountName>` tag to the name of a user account in LDAP, as shown in the following example:

```
<AdminAccountName>Administrator</AdminAccountName>
```

where Administrator is the name of a user account in LDAP.

2. In the `login-handler.xml` file, comment out the section that contains `com.appiq.security.server.BasicLoginhandler`, which enables internal authentication mode. Only one login handler is allowed at a time.
   `<!--LoginHandlerClass>com.appiq.security.server.BasicLoginHandler</LoginHandlerClass-->`
3. Comment out the `<LoginHandlerType>Default</LoginHandlerType>` tag as follows:
   `<!--LoginHandlerType>Default</LoginHandlerType-->`
4. Uncomment the line containing the class name and login handler type so that it appears as follows:

```
<LoginHandlerClass>com.appiq.security.server.LdapLoginHandler</LoginHandlerClass>
<LoginHandlerType>LDAP</LoginHandlerType>
```

5. Replace `directory.hp.com` with the IP address or the fully qualified name of your LDAP server in the `login-handler.xml` file, as shown in the following example:
   `<Server port="389">192.168.10.1</Server>`
   where
   - `192.168.10.1` is the IP address of the server running LDAP.
   - `389` is the port on which LDAP is running on the server.
6. If you want the password to be saved in the management server database, change the value of the `<ShadowPassword>` tags to true, as shown in the following example:
   `<ShadowPassword>true</ShadowPassword>`
   Saving the passwords in the management server database lets a user still log into the management server if the management server is changed back to local mode. This, however, is not recommended as it defeats the purpose of externalizing a user's credentials.

   The `login-handler.xml` file contains two sets of `<ShadowPassword>` tags: one for Active Directory and one for LDAP. Make sure you change the value of the `<ShadowPassword>` tags that are children of the `<LDAP>` tags.
7. If you want the user name to be case sensitive, change the value of the <CaseSensitiveUserName> tag to true, as shown in the following example:
   `<CaseSensitiveUserName>true</CaseSensitiveUserName>`
   If you change the value of `<CaseSensitiveUserName>` to true, the management server becomes case-sensitive to user names. The management server sees MyUserName and myusername as different users.

   The login-handler.xml file contains two sets of `<CaseSensitiveUserName>` tags: one for Active Directory and one for LDAP. Make sure you change the value of the `<CaseSensitiveUserName>` tags that are children of the `<LDAP>` tags.

8. Provide the LDAP search base in which you want the management server to look up AD/ LDAP user attributes. Allow no spaces between commas and put in all components of fully qualified domain name, for example, `hds.usa.com` would be `DC=hds,DC=usa,DC=com`.
   `The search base is used to specify the starting point for the search. It points to a distinguished name of an entry in the directory hierarchy.`
   `<SearchBase>CN=$NAME$,dc=MyCompanyName,dc=COM</SearchBase>`
   or:
   `<SearchBase>CN=$NAME$,OU=NetworkAdministration, dc=MyCompanyName,ou=US,dc=COM</SearchBase>`
   The management server searches only those users in the company who are part of the NetworkAdministration organization (OU=NetworkAdministration) and in the United States (ou=US).

   Important: Different LDAP implementations may be using different keynames for CN. The appropriate key should be mentioned in `login-handler.xml`. Refer to the documentation for your LDAP server to determine how to obtain the appropriate keyname. Your keyname may start with uid instead of `CN, for example,: uid=$NAME$,ou=<Optional org unit if applicable>, dc=windows,dc=hp,dc=com`

9. Save the `login-handler.xml` file.
   The following is an example of a modified `login-handler.xml` file for use with an LDAP server. Underlined text is information that was modified:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<LoginHandler>
<AdminAccountName>domain\admin</AdminAccountName>
<!-- for the default, using database for authentication -->
<!--LoginHandlerClass>com.appiq.security.server.BasicLoginHandler</
LoginHandlerClass-->
<!--LoginHandlerType>Default</LoginHandlerType-->
<!-- uncomment the following to enable Active Directory login>
<LoginHandlerClass>com.appiq.security.server.ActiveDirectoryLoginHandler</
LoginHandlerClass>
<LoginHandlerType>ActiveDirectory</LoginHandlerType-->

<ActiveDirectory>
<PrimaryServer port="389">IP address of Primary Domain Controller</
PrimaryServer>
<SecondaryServer>IP Address of Secondary Domain Controller</
SecondaryServer>
```

```
<ssl>false</ssl>
<ShadowPassword>false</ShadowPassword>
<CaseSensitiveUserName>false</CaseSensitiveUserName>
<!-- provide SearchBase if full name and email attribute are to be
synchronized
between ActiveDirectory and the database.-->
<SearchBase>DC=domain extension1,DC=domain extension2,DC=COM</SearchBase>
<FullNameAttribute>displayName</FullNameAttribute>
<EmailAttribute>mail</EmailAttribute>
</ActiveDirectory>
<!-- uncomment the following for generic LDAP login-->
<LoginHandlerClass>com.appiq.security.server.LdapLoginHandler</
LoginHandlerClass>
<LoginHandlerType>LDAP</LoginHandlerType>
<LDAP>
<!-- same as java.naming.provider.url ldap://ldap.companyname.com:389 -
->
<Server port="389">IP address or DNS name of LDAP server</Server>
<!-- LDAP env can be added, an example is shown below...
<LDAPEnv
name="java.naming.factory.initial">com.sun.jndi.ldap.LdapCtxFactory</
LDAPEnv>
-->
<ssl>false</ssl>
<ShadowPassword>false</ShadowPassword>
<CaseSensitiveUserName>false</CaseSensitiveUserName>
<!-- multiple DN entries are allowed, they will be tried one at a time -->
<DN>CN=$NAME$,OU=Engineering,DC=mycompanyname,OU=US,DC=COM</DN>
<!-- provide FullNameAttribute and EmailAttribute if full name and email
attribute
are to be synchronized between LDAP and the database -->
<FullNameAttribute>displayName</FullNameAttribute>
<EmailAttribute>mail</EmailAttribute>
</LDAP>
</LoginHandler>
```

When you are done with your changes, the `login-handler.xml` file, may resemble the following:

```
<LoginHandler>
  <AdminAccountName>Administrator</AdminAccountName>
  <LoginHandlerClass>
    com.appiq.security.server.LdapLoginHandler
  </LoginHandlerClass>
  <LoginHandlerType>LDAP</LoginHandlerType>
  <LDAP>
    <Server port="389">IP address of LDAP server</Server>
```

```
    <ssl>false</ssl>
    <ShadowPassword>false</ShadowPassword>
    <CaseSensitiveUserName>false</CaseSensitiveUserName>
    <DN>CN=$NAME$,OU=Engineering,DC=HP,OU=US,DC=COM</DN>
    <FullNameAttribute>displayName</FullNameAttribute>
    <EmailAttribute>mail</EmailAttribute>
  </LDAP>
</LoginHandler>
```

Step 2 - Restart the AppStorManager Service and Login as the Designated Admin Account

In this section, you will restart the AppStorManager service and login as the designated Admin account.

1. After you modify the `login-handler.xml` file, you must restart the AppStorManager service, which is the service for the management server for your changes to take effect.

   Important: The service must be running for users to access the management server.

   On Microsoft Windows:

   a. Go to the **Services** window, usually accessible from the Control Panel.
   b. Right-click **AppStorManager**.
   c. Select **Stop** from the drop-down menu.
   d. To start the management server, right-click **AppStorManager** and select **Start** from the drop-down menu.

   On Sun Solaris:

   a. Open a command prompt window.
   b. Enter the following at the command prompt to stop the management server:
      `/etc/init.d/appstormanager stop`
   c. To start the management server, enter the following at the command prompt:
      `/etc/init.d/appstormanager start`
2. Login as the designated administrator account you specified in “Step 1 - Configure the Management Server to Use Active Directory or LDAP” on page 350.
   For example, the user name would be the following:

- **Active Directory** - domain\PrimaryUser
- **LDAP** - PrimaryUser

where `PrimaryUser` is the name of the user account in LDAP or is the designated primary user in Active Directory.

The password would be the following: [NTdomainpassword].

Step 3 - Add Users to the Management Server

You must now add your Active Directory/LDAP users to the management server. This step is required to prevent accidental access to the management server from other AD/LDAP users. Until the user is authenticated against Active Directory/LDAP, the management server views the user as an internal user, whose password can be changed within the management server.

Once a user is authenticated against Active Directory/LDAP, the user is tagged as an external user and the user's password must be managed through Active Directory/LDAP.

1. Log onto the management server by using the designated Admin account specified in "Step 1 - Configure the Management Server to Use Active Directory or LDAP" on page 350.
2. Create your users as described in "Adding Users" on page 329.
   Keep in mind the following:
   - **(Active Directory)** Prefix the user name with the domain name, for example: domain\newuser.
   - The user names you create by using the management server must match the user names in Active Directory/LDAP.
   - It is not necessary to create a password since passwords used for login are those already configured on either the AD or LDAP server.

Step 4 - Provide Login Information to Your Users

Users are now able to log into the management server with the user name and password specified in Active Directory/LDAP.

Important: Tell your users not to give the password they use to access the management server to anyone. Since user credentials are now stored in Active Directory/LDAP, the password used to access the management server may also be used to access other accounts. In some instances, it may be their network user name and password.

CHAPTER 18

Troubleshooting

This chapter describes the following:

- “Data is late or an error occurred” Message on page 364
- appiq.log Filled with Connection Exceptions on page 364
- Receiving “HTTP ERROR: 503" When Accessing the Management Server on page 365
- Permanently Changing the Port a CIM Extension Uses (UNIX Only) on page 367
- Configuring UNIX CIM Extensions to Run Behind Firewalls on page 368
- Volume Names from Ambiguous Automounts Are Not Displayed on page 376
- Solaris Management Server Suddenly Restarts on page 376
- Installing the Software Security Certificate on page 377
- Troubleshooting After Upgrading on page 379
- Troubleshooting Discovery and Get Details on page 380
- Troubleshooting Topology Issues on page 391
- Troubleshooting Provisioning on page 405
- Troubleshooting Hardware on page 407

“Data is late or an error occurred” Message

If you see the message “Data is late or an error occurred” when you try to obtain information from a UNIX host, verify you were logged in as root when you started the CIM Extension (`./start`). You must be logged in as root if you want to use the `./start` command, even if you are using the `./start -users username` command, where `username` is a valid UNIX account.

The CIM Extension only provides the information within the privileges of the user account that started the CIM Extension. This is why you must use root to start the CIM Extension. Only root has enough privileges to provide the information the management server needs.

If you continue to see the message, contact customer support.

appiq.log Filled with Connection Exceptions

When an Oracle REDO log becomes corrupt, the management server is unable to connect to the database. Whenever the management server is unable to connect to the Oracle database, it writes to the appiq.log file. Many exceptions may cause the Application Log on Windows to become full.

To fix the problem, stop the management server and Oracle. Then, remove the corrupted REDO log, as described in the following steps:

1. Stop the AppStorManager service, which is the service the management server uses.

   Note: While the service is stopped, the management server cannot monitor elements and users cannot access the management server.

2. To find the corrupt log file, look in the alert_APPIQ.log file, which can be found in one of the following locations:
   - **Windows:** \oracle\admin\APPIQ\bdump
   - **Solaris:** $ORACLE_BASE\admin\APPIQ\bdump

You can verify if the REDO log listed in the alert_APPIQ.log file is corrupt by looking for a “redo block corruption” error in the REDO log.

3. On the management server, enter the following at the command prompt:
   ```
   Sqlplus /nolog
   ```
4. Enter the following:
   ```
   Sql> connect sys/change_on_install as sysdba
   ```
5. Enter the following:
   ```
   Sql> startup mount;
   ```
6. Enter the following:
   ```
   Sql> ALTER DATABASE CLEAR UNARCHIVED LOGFILE
   'C:\ORACLE\ORADATA\APPIQ\REDO02.LOG';
   ```
   where `C:\ORACLE\ORADATA\APPIQ\REDO02.LOG` is the corrupted log file and its path.
7. Enter the following:
   ```
   Sql> alter database open
   ```
8. Enter the following:
   ```
   Sql> shutdown immediate;
   ```
9. Enter the following:
   ```
   Sql> startup
   ```

Receiving “HTTP ERROR: 503" When Accessing the Management Server

If you receive a message resembling the following when you try to access the management server, make sure your database for the management server is running. If it is not, start the database.

```
Receiving HTTP ERROR: 503 javax.ejb.EJBException: null;
```

Refer to the following sections for more information about how to start database for the management server.

Windows

Access the Services window to make sure the OracleOraHome92TNSListener service has started and is set to automatic. Refer to the Windows documentation for information on how to access the Services window.

If the OracleOraHome92TNSListener service has not started but the AppStorManager service has started, start the OracleOraHome92TNSListener service and then restart AppStorManager.

Solaris

To verify the Oracle service has started, enter the following at the command prompt:

```
# ps -ef | grep ora
```

Output resembling the following is displayed if the service has started:

```
/opt/oracle/product/9.2.0.1.0/bin/tnslsnr LISTENER -inherit
 ./appstormservice /opt/productname/ManagerData/conf/solaris-wrapper.
  oracle   356     1  0   Jul 30 ?        0:01 ora_pmon_APPIQ
  oracle   358     1  0   Jul 30 ?        0:26 ora_dbw0_APPIQ
  oracle   360     1  0   Jul 30 ?        1:13 ora_lgwr_APPIQ
  oracle   362     1  0   Jul 30 ?        0:39 ora_ckpt_APPIQ
  oracle   364     1  0   Jul 30 ?        0:10 ora_smon_APPIQ
  oracle   366     1  0   Jul 30 ?        0:00 ora_reco_APPIQ
  oracle   368     1  0   Jul 30 ?
```

If you find your service for the Oracle has not started, you can start the service by entering the following at the command prompt:

```
# /etc/rc3.d/S98dbora start
```

If you need to stop the service for Oracle, enter the following at the command prompt:

```
# /etc/rc3.d/S98dbora stop
```

Important: If you are starting the services manually, start the Oracle service before the service for the management server.

Errors in the Logs

If you access the logs, you are shown messages resembling the following. The complete text has been shorten as a result of space constraints:

```
Aug 04 2004 11:59:07] INFO
[com.appiq.service.policyManager.policyService.PolicyService] Creating

[Aug 04 2004 11:59:07] INFO
[com.appiq.service.policyManager.policyService.PolicyService] Created

[Aug 04 2004 11:59:07] INFO
[com.appiq.service.policyManager.policyService.PolicyService] Starting

[Aug 04 2004 11:59:07] INFO
[com.appiq.service.policyManager.policyService.PolicyService] Starting
Policy Factory

[Aug 04 2004 11:59:11] ERROR
[com.appiq.security.DatabaseSecurityManager] DatabaseSecurityManager
Error:

org.jboss.util.NestedSQLException: Could not create connection; -
nested throwable: (java.sql.SQLException: ORA-01033: ORACLE
initialization or shutdown in progress

); - nested throwable: (org.jboss.resource.ResourceException: Could
not create connection; - nested throwable: (java.sql.SQLException:
ORA-01033: ORACLE initialization or shutdown in progress

))
```

Permanently Changing the Port a CIM Extension Uses (UNIX Only)

CIM Extensions on UNIX use port 4673 by default. You can start a CIM Extension on another port by entering `./start -port 1234`, where 1234 is the new port. With this method, you must always remember to provide the nondefault port when starting the CIM Extension.

You can configure a CIM Extension to remember the nondefault port, so you only need to enter `./start` to start the CIM Extension:

1. Go to the /opt/APPQcime/conf directory.
2. Open the `cim.extension.parameters` file in a text editor, and provide the following line:

   ```
   -credentials username:password
   -port 1234
   ```

Important: The values for -credentials and –port must be on separate lines, as shown in the example.

where

- username is the user that is used to discover the CIM Extension. You will need to provide this user name and its password when you discover the host.
- password is the password of username.
- 1234 the new port for the CIM Extension

3. Save the file.
4. Restart the CIM Extension for your changes to take effect.

Note: The CIM Extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

5. The management server assumes the CIM Extension is running on port 4673. The management server also listens on port 17000 for CIM Extensions from build 4.0. If you change the port number, you must make the management server aware of the new port number.
   In the IP Address/DNS Name field in the Add Address for Discovery page (**Discovery** > **Setup** > **Add Address**), type a colon and then the port number after the IP address or DNS name, as shown in the following example:

   ```
   192.168.1.2:1234
   ```

   where

   - 192.168.1.2 is the IP address of the host
   - 1234 is the new port number

   If you have already added the host to the discovery list (**Discovery** > **Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Configuring UNIX CIM Extensions to Run Behind Firewalls

In some instances you will need to discover a host behind a firewall. Use the following table as a guideline. Assume the management server wants to discover HostA, which has three network interface cards on three separate networks with three separate IPs: 10.250.250.10, 172.31.250.10, and 192.168.250.10. In the following table different configurations are presented:

- The “Manual Start Parameters for CIM Extensions” column provides what you would enter to start the CIM Extension manually on the host. See the Installation Guide for more information on how to start a CIM Extension manually.
- The “If Mentioned in cim.extension.parameters” column provides information on how you would modify the `cim.extension.parameters` file. See “Permanently Changing the Port a CIM Extension Uses (UNIX Only)” on page 367.
- The “Step 1 Discovery (**Discovery** > **Setup**) and RMI Registry Port” column - Provides information about what IP addresses are required for the discovery list. The RMI Registry port is the port the CIM Extension uses. Keep in mind that when a port other than 4673 is used for the CIM Extension, the port must be included in the discovery IP. For example, 192.168.1.1:1234, where 192.168.1.1 is the IP for the host and 1234 is the port the CIM Extension uses.

Table 18-1: Troubleshooting Firewalls

Configur-ation	Manual Start Parameters for CIM Extension	If Mentioned in cim.extension.parameters	Step 1 Discovery and RMI Registry Port
Firewall port 4673 opened between host and management server	start		10.250.250.10 OR 172.31.250.10 OR 192.168.250.10 Communication Port: 4673
Firewall port 1234 opened between host and management server, but specific port	start -port 1234	-port 1234	10.250.250.10 :1234 OR 172.31.250.10 :1234 OR 192.168.250.10:1234 Communication Port: 1234
Firewall port 4673 opened between host and management server on the 172.31.250.x subnet	start -on 172.31.250.10	-on 172.31.250.10	172.31.250.10 Communication Port: 4673

Table 18-1: Troubleshooting Firewalls (Continued)

Configur-ation	Manual Start Parameters for CIM Extension	If Mentioned in cim.extension.parameters	Step 1 Discovery and RMI Registry Port
Firewall port 1234 opened between host and management server on the 192.168.250.x subnet	start -on 192.168.250.10:1234	-on 172.31.250.10:1234	172.31.250.10 :1234 Communication Port: 1234
With 3 firewall ports opened on different ports respectively 1234, 5678, 9012.	start -on 10.250.250.10:1234 -on 172.31.250.10: 5678 -on 192.168.250.10: 9012	-on 10.250.250.10:1234 -on 172.31.250.10:5678 -on 192.168.250.10: 9012	10.250.250.10 :1234 OR 172.31.250.10 :5678 OR 192.168.250.1 0:9012 Communication Port: 1234, 5678, 9012

Table 18-1: Troubleshooting Firewalls (Continued)

Configur-ation	Manual Start Parameters for CIM Extension	If Mentioned in cim.extension.parameters	Step 1 Discovery and RMI Registry Port
With firewall port 4673 opened between host and management server. NAT environment where 10.250.250.10 subnet is translated to 172.16.10.10 when it reaches other side of the firewall	start		172.16.10.10 Communication Port: 17001

Table 18-1: Troubleshooting Firewalls (Continued)

Configur-ation	Manual Start Parameters for CIM Extension	If Mentioned in cim.extension.parameters	Step 1 Discovery and RMI Registry Port
With firewall port 1234 opened between a host and management server. NAT environment where 10.250.250.10 subnet is translated to 172.16.10.10 when it reaches other side of the firewall	start -port 1234	-port 1234	172.16.10.10 Communication Port: 17001
With 3 firewall ports opened on different ports respectively 1234, 5678, 9012. NAT environment where all 3 NICs are translated to different 172.16.x.x subnets	start -on 10.250.250.10:1234 -on 172.31.250.10:5678 -on 192.168.250.10:9012	-on 10.250.250.10:1234 -on 172.31.250.10:5678 -on 192.168.250.10:9012	172.16.10.10: 1234 OR 172.16.20.20: 5678 OR 172.16.30.30: 9012 Communication Port: 1234, 5678, 9012

Table 18-1: Troubleshooting Firewalls (Continued)

Configur-ation	Manual Start Parameters for CIM Extension	If Mentioned in cim.extension.parameters	Step 1 Discovery and RMI Registry Port
False DNS or IP is slow to resolve		jboss.properties, stop and restart service cimom.Dcxws.agency.firstwait=200000 cimom.Dcxws.agency.timeout=200000	Any IP that is reachable Communication Port: 4673
No DNS, never resolve		jboss.properties, stop and restart service cimom.Dcxws.agency.firstwait=200000 cimom.Dcxws.agency.timeout=200000	Any IP that is reachable Communication Port: 4673

Table 18-1: Troubleshooting Firewalls (Continued)

Configur-ation	Manual Start Parameters for CIM Extension	If Mentioned in cim.extension.parameters	Step 1 Discovery and RMI Registry Port
No firewall. Don't want to use root credentials. Want to discover with a non-existent user.	start -credentials abcuser:passwd	-credentials abcuser:passwd	Specify abcuser and password in the discovery list. Communication Port: 4673
With 3 firewall ports opened on different ports respectively 1234, 5678, 9012. Don't want to use root credentials. Want to discover with a non-existent user.	start -on10.250.250.10:1234 -on172.31.250.10:5678 -on192.168.250.10:9012 -credentials abcuser:passwd	-on10.250.250.10:1234 -on172.31.250.10:5678 -on192.168.250.10:9012 -credentials abcuser:passwd	10.250.250.10 :1234 OR 172.31.250.10 :5678 OR 192.168.250.1 0:9012. Then, specify abcuser and passwd in the discovery list. Communication Port: 1234, 5678, 9012

Volume Names from Ambiguous Automounts Are Not Displayed

Volume names from ambiguous automounts on Solaris hosts are not displayed on the Storage Volumes page and in Capacity Explorer. Some Solaris hosts have autofs and NFS mounted through an automounter. The management server cannot display volume names from ambiguous automounts because it cannot determine if the comma separate strings that are part of the mounted volume name are host names or part of the name of a remote volume.

The following example is a comma separate string that is part of a mounted volume name. The management server cannot tell whether `test` and `three` are host names or part of the name of a remote volume. As a result, the management server does not display the volume name.

```
VolumeName = two:/ntlocal2,two:/comma,test,three,one:/ntlocal
```

Solaris Management Server Suddenly Restarts

When the memory usage for management server Java process grows considerably, users may experience sudden restart of management server on machines with low physical memory. The restart occurs because Java Virtual Machine (JVM) for management server exits when it is not able to expand heap during Garbage Collection. This is a known JVM issue.

Work around:

1. Increase the swap size on solaris server.
2. Set -Xms and -Xmx to the same value and -XX:PermSize and -XX:MaxPermSize to the same value so that no heap expansion takes place during Garbage Collection. These variables can be set using the Advanced option under the Product Health menu.

Installing the Software Security Certificate

To stop receiving a Security Alert message each time you use the HTTPS logon, install the software security certificate, as described in the following steps.

Important: Enter the DNS name of the computer in the URL instead of localhost. If you use `https://localhost` to access the management server, you are shown a “Hostname Mismatch” error.

Installing the Certificate by Using Microsoft Explorer 6.0

1. Access the management server by typing the following:
   `https://machinename`
   where `machinename` is the name of the management server.
2. When the security alert message appears, click **OK**.
   If you do not want the Web browser to warn you about a secure connection at any Web site, select the **In the future, do not show this warning** option.
3. When you are told there is a problem with the site's security certificate, click the **View Certificate** button.
4. When you are shown the certificate information, click the **Install Certificate** button at the bottom of the screen.
5. When you are shown the Certificate Import Wizard, click **Next** to continue the installation process.
6. Select one of the following:
   - **Automatically select the certificate store based on the type of certificate** - This option places the certificate automatically in the appropriate location.
   - **Place all certificates in the following store** - This option lets you pick the store where the certificate will be stored.
7. Click **Finish**.
8. When you are asked if you want to install the certificate, click **Yes**.
   You are shown the following message when the certificate is installed.

Installing the Certificate by Using Netscape Navigator 7

1. Access the management server by typing the following:
   `https://machinename`
   where `machinename` is the name of the management server.
2. When the security alert message appears, click the **Always** button.
3. When you are told you are requesting an encrypted page, click **OK**.
4. Click the **Always** button when you are asked if you want to accept the certificate.
5. When asked if you wanted to trust the signed applet, click the **Always** button.

Changing the Security Certificate to Match the Name of the Server

If your users are shown a Security Alert window with the following message, you might want to modify the security certificate so users feel more comfortable with installing the certificate:

“The name of the security certificate is invalid or does not match the name of the site.”

You can change the security certificate so that users receive the following message instead:

“The security certificate has a valid name matching the name of the page you are trying to view.”

When you change the certificate, you must use the generateAppiqKeystore.bat program to delete the original certificate. Then, use the generateAppiqKeystore.bat program to create a new certificate and to copy the new certificate to the management server.

To change the certificate:

1. (Solaris management servers only) Go to the `[Install_Dir]/Tools` directory and run the following command:
   `eval ‘./usersvars.sh‘`

   Important: The quotes in the example must be entered as left single quotes.

2. Go to the following directory:

- **Solaris** - `[Install_Dir]/Tools`
- **Windows** - `[Install_Dir]\Tools`

where `[Install_Dir]` is the directory into which you installed the management server.

3. To delete the original certificate, enter the following at the command prompt:
   `perl generateAppIQKeyStore.pl del`
   The original certificate is deleted.

Note: If you see an error message when you enter this command, a previous certificate may not have been created. You can ignore the error message.

---

4. To create a new certificate containing the DNS name of the management server, enter the following at the command prompt:
   `perl generateAppIQKeyStore.pl`
5. If the program is unable to detect a DNS name, enter the following at the command prompt:
   `perl generateAppIQKeyStore.pl create mycomputername`
   where `mycomputername` is the DNS name of the computer
6. To copy the new certificate to the management server, enter the following at the command prompt:
   `perl generateAppIQKeyStore.pl copy`
   The new certificate is copied to the correct location.

Troubleshooting After Upgrading

This section provides information on troubleshooting after upgrading. It includes the following topics:

SMI-S Switches Must Be Removed and Rediscovered After Upgrading on page 380

SMI-S Switches Must Be Removed and Rediscovered After Upgrading

You must remove and rediscover Cisco, QLogic, or CNT switches supported through SMI-S after you upgrade the management server.

1. Remove the Cisco, QLogic, or CNT switches supported through SMI-S. See “Deleting Elements from the Product” on page 136.
2. Rediscover the Cisco, QLogic, or CNT switches. See “Step 1 - Discover Switches” on page 78.
3. Perform Get Details. See “Step 4 - Get Details” on page 138.

Troubleshooting Discovery and Get Details

This section describes the following:

- Names are Changed After Running Get Details for Cisco SMI-S Switches on page 381
- Configuring E-mail Notification for Get Details on page 382
- Increasing the Time-out Period and Number of Retries for Switches in Progress on page 383
- “Connection to the Database Server Failed” Error on page 385
- Using the Test Button to Troubleshoot Discovery on page 385
- DCOM Unable to Communicate with Computer on page 387
- Duplicate Listings for Brocade Switches in Same Fabric on page 388
- Element Logs Authentication Errors During Discovery on page 388
- EMC Device Masking Database Does Not Appear in Topology (AIX Only) on page 388
- Management Server Does Not Discover Another Management Server's Database on page 389
- Microsoft Exchange Drive Shown as a Local Drive on page 389
- Unable to Discover Microsoft Exchange Servers on page 389
- Nonexistent Oracle Instance Is Displayed on page 389

- Requirements for Discovering Oracle on page 389
- “Do Not Run Overlapping Discovery Schedules” on page 390
- "This storage system uses unsupported firmware. ManagementClassName: ???" Message on page 390
- Troubleshooting Topology Issues on page 391
- Incorrect Topology Sometimes Displayed for CNT Switches on page 397
- Unable to Find Elements on the Network on page 397
- Device Locking Mechanism for Brocade Element Manager Query/Reconfiguration on page 397
- A Discovered Sun StorEdge A5000 JBOD Does Not Display Its WWN Properly on page 398
- Unable to Monitor McDATA Switches on page 398
- Unable to Detect a Host Bus Adapter on page 398
- Navigation Tab Displays Removed Drives as Disk Drives on page 399
- Unable to Obtain Information from a CLARiiON Storage System on page 399
- Discovery Fails Too Slowly for a Nonexistent IP Address on page 399
- “CIM_ERR_FAILED” Message on page 400
- Communicating with HiCommand Device Manager Over SSL on page 403
- Unable to Discover a UNIX Host Because of DNS or Routing Issues on page 404
- Troubleshooting Hardware on page 407

Names are Changed After Running Get Details for Cisco SMI-S Switches

Cisco switches on the fabric are displayed without their names—each Cisco SMI-S switch name on the fabric is replaced with a generic name such as: Switch_1401 after running Get Details.

To view the correct names for the Cisco SMI-S switches after running Get Details, manually enter the correct name for the Cisco SMI-S switches.

Configuring E-mail Notification for Get Details

The management server lets you send status reports about Get Details to users. The status reports that are sent to users can also be found in the `GAEDSummary.log` file in the `[Install_DIR]\logs` directory on the management server.

To configure the management server to send status reports on Get Details to your e-mail account:

1. Enable e-mail notification for the management server. Refer to the User Guide for more information.
2. Add or edit the e-mail address for the Admin account.
   The status reports for Get Details automatically go the e-mail account provided for the Admin user. To add or edit an e-mail address for the Admin account, log in as Admin and then follow the steps in “Modifying Your User Profile” on page 334.
3. If you want additional users to receive the status reports for Get Details, do the following:
   a. Click **Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree.
   b. Click **Show Default Properties** at the bottom of the page.
   c. Copy the `gaedemail` property. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.
   d. Return to the Advanced page (**Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree).
   e. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
   f. Assign the e-mail accounts you want to receive the report to the `gaedemail` property. For example, if you want user1@appiq.com and user2@appiq.com to receive these status reports, modify the `gaedemail` property in the **Custom Properties** field as follows:
      `gaedemail=user1@appiq.com;user2@appiq.com`
      Note: Make sure the harsh (#) symbol is removed from the gaedmail property.
   g. When you are done, click **Save**.
   h. Restart the service for the management server for your changes to take effect.

Increasing the Time-out Period and Number of Retries for Switches in Progress

If you are having difficulty obtaining information from switches with SNMP connections during Get Details, you may need to increase the time-out period and the number of retries. By default, the management server gives a switches five seconds to respond to its requests for information during Get Details. If the switch does not respond the first time, the management server tries again. The management server says it cannot contact the switch if it does not receive a response from the switch a second time.

To change the time-out period and number of retries for switches, modify the properties specified Table 18-2, “Time-out Properties,” on page 384 and Table 18-3, “Retry Properties,” on page 384 as described in the following steps:

1. Access the management server.
2. Select **Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree.
3. Click **Show Default Properties** at the bottom of the page.
4. Copy the commands specified in Table 18-2, “Time-out Properties,” on page 384. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.
5. Return to the Advanced page (**Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree).
6. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
7. Make sure the property is not commented out by removing the hash (#) symbol in front of the property.To modify the time-out period, set the corresponding property for your switch in the following table to the number of millisecond you want. The default is 5000 ms. For example, to change the time-out period to 30000 ms for a McDATA switch, you would set the `cimom.McData.Snmp.Timeout` property to 30000, as shown in the following example:

```
cimom.McData.Snmp.Timeout=30000
```

Table 18-2: Time-out Properties

Switch	Property
McDATA/Connectrix discovered through SNMP	`cimom.McData.Snmp.Timeout`
Cisco	`cimom.Cisco.Snmp.Timeout`
Other switches discovered through SNMP: ■ Sun StorEdge ■ QLogic	`cimom.snmp.switch.timeout`

8. To modify the number of retries, repeat Steps 4 through 6 by copying and pasting the property specified in Table 18-3, “Retry Properties,” on page 384. Set the corresponding property for your switch in the following table to the number of retries you want. The default is two retries. For example, to change the number of retries to five for a McDATA switch, set the `cimom.McData.Snmp.Retries` properties as shown in the following example:
   `cimom.McData.Snmp.Retries=5`

Table 18-3: Retry Properties

Switch	Property
McDATA/Connectrix discovered through SNMP	`cimom.McData.Snmp.Retries`
Cisco	`cimom.Cisco.Snmp.Retries`
Other switches discovered through SNMP: ■ Sun StorEdge ■ QLogic	`cimom.snmp.switch.retries`

9. When you are done, click **Save**.
10. Restart the service for the management server for your changes to take effect.

While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

“Connection to the Database Server Failed” Error

If you received an error message resembling the following after getting all element details, verify that the database instance is running:

```
The connection to the database server failed. Check that the Oracle
instance 'OIQ3 on host '192.168.1.162:1521 is running correctly and has
the management software for Oracle installed correctly.
```

Assume you received the error message listed above. You would want to verify the following:

- Oracle instance OIQ3 on host 192.168.1.162 port 1521 is running.
- The management software for Oracle is installed on the server running the Oracle instance. One of the installation's tasks is to create an APPIQ_USER user account with enough privileges for the software to view statistics from the database.

Once you have verified the items listed above, run Get Details again. If you continue to see the error message, contact customer support.

Using the Test Button to Troubleshoot Discovery

If you are having problems discovering an element, click the **Test** button on the Discovery setup page (**Discovery** > **Setup**). When you click the **Test** button, the management server attempts to ping the element. Then, it runs a series of device-specific connectivity tests. The output of these tests can be viewed in the discovery log window.

The management server uses a provider to communicate with an element. A provider is software that communicates with the element and the management server. When you click the **Test** button, it checks every available provider against the element to see which one works. When this test is being performed, you may notice messages such as “Test provider not supported,” “Connection Refused” or “Failed to Establish Connection.” This means a provider was tested against the element and the provider was not the correct one.

When the correct provider is found, a message is displayed, such as “ExampleComputer responds to a Wind32 system” or “Connection accepted,” as shown below:

```
Testing provider APPIQ_Win32Provider for: 192.168.1.2
ExampleComputer responds as a Win32 system with CIM Extensions 3.0.0.129
```

The success messages are intertwined with the other messages, so you need to scroll through the log messages. For example, the success message shown previously appeared in the middle of the log messages, as shown in the following example. The success message is underlined in the following example.

To make it easier to view the log messages, copy and paste the log messages from the log window to a text editor.

```
LOG MESSAGES

[2004/01/15 09:10]    Test Discovery Started
[2004/01/15 09:10]    Successfully pinged 192.168.1.2
[2004/01/15 09:10]
Testing provider APPIQ_SolarisProvider for: 192.168.1.2
Connection refused to host: 192.168.1.2; nested exception is:
java.net.ConnectException: Connection refused: connect
Testing provider APPIQ_CimProxyProvider for: 192.168.1.2
Test provider functionality not supported for APPIQ_CimProxyProvider
Testing provider APPIQ_McDataProvider for: 192.168.1.2
Can't connect.
No current SWAPI connection to host 192.168.1.2.  Cannot establish
connection
Testing provider APPIQ_AltixProvider for: 192.168.1.2
Connection refused to host: 192.168.1.2; nested exception is:
java.net.ConnectException: Connection refused: connect
Testing provider APPIQ_IrixProvider for: 192.168.1.2
Connection refused to host: 192.168.1.2; nested exception is:
java.net.ConnectException: Connection refused: connect
Testing provider APPIQ_Win32Provider for: 192.168.1.2
ExampleComputer responds as a Win32 system with CIM Extensions 3.0.0.129
Windows host does not support remote testing
VERITAS Volume Manager not available
HDLM Multipathing Software not available
Powerpath Multipathing Software not available
RDAC Multipathing Software not available
Testing provider APPIQ_EmcProvider for: 192.168.1
Can't connect
```

```
appiqSymInitialize() failed with error code 510
Testing provider APPIQ_AixProvider for: 192.168.1.2
Connection refused to host: 192.168.1.2; nested exception is:
java.net.ConnectException: Connection refused: connect
Testing provider APPIQ_HdsProvider for: 192.168.1.2
Cannot connect to Proxy
Cannot connect to Proxy
Testing provider APPIQ_BrocadeElementManager for: 192.168.1.2
Cannot connect
Cannot connect
Testing provider EngenioSSI_Provider for: 192.168.1.2
Failed to establish connection.
Testing provider APPIQ_ClariionProvider for: 192.168.1.2
NaviCLI not installed
No such file: C:\Program Files\EMC\Navisphere CLI\NaviCLI.exe
[2004/01/15 09:10]    Test Discovery Completed
TEST DISCOVERY COMPLETED in 5 seconds
```

Note: By design the **Test** button is not available when any of the discovery steps are occurring.

DCOM Unable to Communicate with Computer

Sometimes the following error message appears in the event log of the management server when the software is monitoring a Brocade switch:

```
DCOM was unable to communicate with the computer 192.168.10.21 using
any of the configured protocols
```

where 192.168.10.21 is the IP address of the Brocade switch.

Ignore this error message.

Duplicate Listings for Brocade Switches in Same Fabric

If you discover more than one Brocade switch in the same fabric, the **Targets** tab displays duplicate listings for the Brocade switches. Each Brocade switch is listed multiple times with the IP address of the other switches and its own.

For example, assume you discovered Brocade switches QBrocade2 and QBrocade5 in the same fabric, the switches are listed twice on the **Targets** tab. QBrocade2 is listed twice, once with its own IP address, the other time with the IP address of QBrocade5, as shown below:

```
192.168.10.22 Switch QBrocade2, QBrocade5 admin
192.168.10.25 Switch QBrocade2, QBrocade5 admin
```

Element Logs Authentication Errors During Discovery

During discovery, you may see SNMP authentication errors on the element you are trying to discover. The management server is probing the element with an SNMP request. If the element does not know the management server, it logs authentication errors.

EMC Device Masking Database Does Not Appear in Topology (AIX Only)

An EMC device masking database attached to an AIX host does not appear in the Topology tree under the **Application Path - Unmounted** node on the **Topology** tab in System Explorer.

If the EMC device masking database is attached to a host running Microsoft Windows or Sun Solaris, the masking database appears under the **Application Path - Unmounted** node.

Management Server Does Not Discover Another Management Server's Database

In some situations the management server may not discover another management server’s database. Make sure that the Oracle monitoring software (CreateOracleAct.bat for Microsoft Windows or CreateOracleAct.sh for UNIX) is installed on the management server to be discovered and that the Oracle instance is added to the discovery list.

Microsoft Exchange Drive Shown as a Local Drive

Microsoft Exchange Servers have a drive M. The software displays this drive as a local fixed disk, instead of a Microsoft Exchange Server special drive.

Unable to Discover Microsoft Exchange Servers

If DNS records for your Microsoft Exchange servers are outdated or missing, the discovery of Microsoft Exchange may fail because Microsoft Exchange is dependant on Active Directory, which is dependant on DNS. Since Active Directory is dependant on DNS, Active Directory replication and Active Directory lookups may fail or contain errors if DNS records are not accurate.

Nonexistent Oracle Instance Is Displayed

The software uses the Oracle Transparent Name Substrate (TNS) listener port to detect Oracle instances on a server. Sometimes an Oracle instance is removed from the server, but not from the TNS listener port. This results in the software detecting the nonexistent Oracle instance and displaying it in the topology. Refer to Oracle documentation for information on how to remove the deleted Oracle instance from the TNS listener port.

Requirements for Discovering Oracle

To discover Oracle:

- The management software for Oracle must be installed. For information about installing the management software for Oracle, refer to the *Installation Guide*.
- By default, the software sets the TNS Listener Port to 1521. If you use another port, you can change the port number on the Discovery Targets tab.
- Oracle discovery relies on the TNS networking substrate on which Oracle is built (TNS is Oracle's proprietary protocol). The software does not use TNS listener password. If you have set a TNS Listener password, the software is not able to discover the Oracle instances serviced by the listener.

Do Not Run Overlapping Discovery Schedules

If you are creating multiple Discovery schedules, care must be taken to avoid scheduling conflicts—concurrently scheduled Discovery tasks—and that each scheduled task has enough time to start and finish before the next Discovery task is scheduled to start. For example, if a scheduled Discovery is still in progress when another scheduled Discovery attempts to start, the Discovery task that attempts to start will not start because the first Discovery is still running. The Discovery that is unable to start is re-scheduled according to its recurring rule. If the Discovery task is scheduled to run on a daily basis for example, then the Discovery will start again on the next day. To check the status of scheduled Discovery tasks, view the appiq.log file in the following directory:

```
[Install_Dir]\jbossandjetty\server\appiq\logs
```

"This storage system uses unsupported firmware. ManagementClassName: ???" Message

The following message is displayed when an Engenio storage system is discovered, and is running unsupported firmware:

“This storage system uses unsupported firmware. ManagementClassName: ???”

The management class name for the unsupported array is displayed in the message.

New releases of storage system firmware are supported with each new release of this software. See the Support Matrix for the latest information on supported firmware.

Troubleshooting Topology Issues

- About the Topology on page 391
- Undiscovered Hosts Display as Storage Systems on page 395
- Solaris Machines Appear to Have Extra QLogic HBAs on page 396
- No Stitching for Brocade Switches with Firmware 3.2.0 on page 396
- Link Between a Brocade Switch and a Host Disappears from the Topology on page 396
- Incorrect Topology Sometimes Displayed for CNT Switches on page 397
- Unable to Find Elements on the Network on page 397
- Device Locking Mechanism for Brocade Element Manager Query/Reconfiguration on page 397
- A Discovered Sun StorEdge A5000 JBOD Does Not Display Its WWN Properly on page 398
- Unable to Monitor McDATA Switches on page 398
- Unable to Detect a Host Bus Adapter on page 398
- Navigation Tab Displays Removed Drives as Disk Drives on page 399
- Unable to Obtain Information from a CLARiiON Storage System on page 399
- Discovery Fails Too Slowly for a Nonexistent IP Address on page 399
- “CIM_ERR_FAILED” Message on page 400
- Communicating with HiCommand Device Manager Over SSL on page 403
- Unable to Discover a UNIX Host Because of DNS or Routing Issues on page 404

About the Topology

The software determines the topology by looking at the following:

- **Fibre channel switch** The fibre channel switch contains a list of all elements within the fabric. The software obtains a detailed listing of all elements connected to the switch fabric.
- **A host containing a Host Bus Adapter (HBA)** All fibre channel host adapters look for available elements attached to the HBA. This information is gathered by CIM Extensions and sent to the management server.
- **A proxy connected to the SAN** - Include a proxy that has a direct connection or a SAN connection to the management server. An example of a proxy is the EMC Solutions

Enabler or Hitachi HiCommand Device Manager. Engenio storage systems do not require a proxy, as they can be accessed directly. Make sure the proxy service has started. On a computer running Windows, this can be determined by looking in the **Services** window.

Table 18-4: Troubleshooting Discovery and Get Details

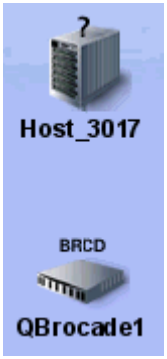
Scenario	Description	What to do
 The host appears discovered and it is connected to the switch.	The software is aware of the host, but it cannot obtain additional information about it.	Verify that a CIM Extension is installed on the host. Try discovering the element again. Then, run Get Details.
 Host appears discovered and it is not connected to the switch.	The switch was previously made aware of the host, but it can no longer contact it. If the steps provided do not work, see “Link Between a Brocade Switch and a Host Disappears from the Topology” on page 396.	Verify that the host is on and the network cables are connected to it. Try discovering the element again. Then, run Get Details.

Table 18-4: Troubleshooting Discovery and Get Details (Continued)

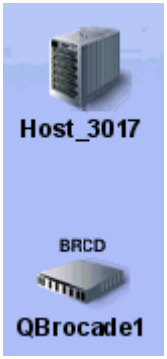
Scenario	Description	What to do
 The host appears managed, but it is not connected to the switch.	There is a problem with Get Details from the host. If the steps provided do not work, see “Link Between a Brocade Switch and a Host Disappears from the Topology” on page 396.	Try getting the topology again. 1. Click the **Discovery** menu. Then, click the **Topology** tab. 2. Verify the element is selected and click the **Get Topology** button.

Table 18-4: Troubleshooting Discovery and Get Details (Continued)

Scenario	Description	What to do
 The element appears discovered, but a connected switch does not appear.	The switch has not been discovered.	Try discovering the switch again. 1. Click the **Discovery** menu. Click the **Setup** tab and the **Add Address** button on the **IP Addresses** tab. 2. Type the IP address or DNS Name of the switch. Then, type its user name and password. Click **OK**. 3. Verify the element is selected. 4. Click the **Start Discovery** button. 5. After discovery has completed, click the **Topology** tab. 6. Verify the element is selected and click the **Get Topology** button.

Table 18-4: Troubleshooting Discovery and Get Details (Continued)

Scenario	Description	What to do
When discovering a Windows-based host, the correct IP address is entered, but the host does not appear in the topology. The following can be seen on the host: ■ *In Windows Event Manager the `WinMgmt.exe` process is not running. This process starts WMI. ■ In the Windows Event Log, DCOM error messages are shown.	An invalid user account was entered	Enter a valid user account that has administrative privileges so it can start WMI.

*The CIM Extension for Microsoft Windows enhances Windows Management Instrumentation (WMI) so that it can gather information from host bus adapters and make the information available to management server.

Important: One way to determine what is happening is to look at the log messages during discovery and getting element details. See “Viewing Log Messages” on page 104 for more information.

Undiscovered Hosts Display as Storage Systems

On rare occasions, undiscovered hosts will display as storage systems in System Explorer. Specifying the host’s WWN in the jboss.properties file will cause the host to display correctly. Follow these steps to modify the jboss.properties file:

1. Determine the host's WWN. This information is available on the IEEE Standards Association web site at http://standards.ieee.org/regauth/oui/oui.txt.
2. Go to the %JBOSS4_DIST%\server\appiq\conf directory on the management server.
3. Open the jboss.properties file in a text editor and locate the `hostPortWWNs` property.
4. Uncomment the property and enter the host's WWN in hex format. Multiple WWNs can be entered as a comma-separated list. For example:
   `hostPortWWNs=00-01-C9,00-01-C8`
5. Restart the service for the management server.

Solaris Machines Appear to Have Extra QLogic HBAs

Solaris machines using fibre channel drives internally will always appear to have extra QLogic HBAs. After discovering a Solaris machine, internal fiber channel drives will show an extra QLogic adapter on the host adapters page.

No Stitching for Brocade Switches with Firmware 3.2.0

Stitching does not appear for hosts attached to Brocade switches running firmware 3.2.0. There is no stitching when the PID format is 0. The port setting must be the same for all Brocade switches in the fabric or the fabric will become segmented. The PID format should be set to 1 for all Brocade switches running firmware later than 2.6.0 and 3.0. The PID=0 setting is a legacy Port ID format that does not support the numbers of ports beyond 16.

Link Between a Brocade Switch and a Host Disappears from the Topology

If a link that used to work between a Brocade switch and a host disappears from the topology, you may need to rediscover the Brocade switch and the host. Also, confirm that both are online and there are no network connection issues. As a last resort, you may need to reboot the switch. In some instances, the API of the Brocade switch has been known to hang. Rebooting the switch clears the switch of the API hang.

Incorrect Topology Sometimes Displayed for CNT Switches

The CNT SMI-S provider for CNT switches does not return the correct topology information when more than one fabric is managed by the same InVSN™ Storage Network Manager. McDATA, which completed its acquisition of CNT in the summer of 2005, has been made aware of this issue.

Unable to Find Elements on the Network

The management server uses ping to find the devices on the network enabled for IP. Ping is a program that lets you verify that a particular IP address exists. Ping is not guaranteed to return a response from all devices. If Discovery is not able to find a device automatically, enter the IP address for the device on the Discovery Targets tab, which can be accessed by clicking the Discovery button at the top of the screen in the management server. Sometimes ping cannot find the device if one of the following conditions occur:

- Network configuration does not support ping, including data center security (firewalls).
- Device has the ping responder turned off.
- Device does not support ping.

Device Locking Mechanism for Brocade Element Manager Query/Reconfiguration

Please keep in mind that the configuration for Brocade switches is locked while getting all details for elements in a zones. The software ensures that each CIM query locks out any reconfiguration. For example, if you are getting details for elements in all zones, you cannot add a new Brocade switch while you are doing it (the discovery or configuration process waits until the collection of details is finished before proceeding). However, simultaneous CIM queries do not lock each other out.

A Discovered Sun StorEdge A5000 JBOD Does Not Display Its WWN Properly

Although full monitoring and management support is available only to those devices for which there is a provider, the software's topology displays other devices found on your storage area network (SAN) to give you a more complete view. However, because these devices do not have a provider, only basic information is returned. In some cases, as with the Sun StorEdge A5000 JBOD (Just a Bunch of Disks), the Worldwide Name (WWN) presented and reported to the management server may be different from the official WWN of the device, as the management server reports the WWN of the port connected to the fabric.

Unable to Monitor McDATA Switches

McDATA switches use the Fibre Channel Switch Application Programming Interface (SWAPI) to communicate with devices on the network. The McDATA switches allow only one SWAPI connection at a time. For example, if the management server discovers the IP address of the McDATA switch, other management servers and third-party software are not able to communicate with the switch using SWAPI.

Use Enterprise Fabric Connectivity (EFC) Manager to communicate with the McDATA switch. EFC Manager versions 7.0 and later can communicate with the management server and the switch. This configuration lets multiple instances of the management server or other clients contact EFC Manager, which in turn provides information about the switch. To communicate with the EFC Manager, discover the McDATA switches as described in Chapter 4, “Discovering NAS Devices, Tape Libraries, Switches and Storage Systems” on page 65.

Important: EFC Manager uses the SWAPI connection, preventing other third-party software from contacting the switch.

Unable to Detect a Host Bus Adapter

The software is unable to detect a host bus adapter if you install its driver before you have completed installing the Solaris operating system for the first time. For example, you installed the

HBA drives too early when you used JumpStart to install Solaris. The best way to install the HBA driver is to install it after Solaris has been installed and is running.

Navigation Tab Displays Removed Drives as Disk Drives

If you remove an internal disk from a Solaris host and do not enter the `cfgadm` command, the Navigation tab displays the empty slot as `DiskDrives_XXXXX` after getting element details. The `cfgadmn` command makes the software realize the drive has been removed. Refer to the documentation that shipped with the Solaris operating system for more information about the `cfgadm` command.

Unable to Obtain Information from a CLARiiON Storage System

If you are having difficulty obtaining topology information or element details from a CLARiiON storage system, the NaviCLI might have timed out as a result of the service processor being under a heavy load. The management server uses the NaviCLI to communicate with the CLARiiON storage system. This situation has been seen in the field when the service processor is running more than 35,000 IOPS (IOs/Sec).

Try obtaining the topology and/or Get Details from a CLARiiON storage system when the service processor is not under such a heavy load.

Discovery Fails Too Slowly for a Nonexistent IP Address

If you enter a nonexistent IP address, the management server times out by default after 20 seconds on Windows and after three minutes and after 45 seconds on Solaris. If you want to shorten the time-out period, modify the `cimom.CimXmlClientHttpConnectTimeout` property as described in this section.

Note: The management server does not accept a period longer than its default setting. If you set `cimom.CimXmlClientHttpConnectTimeout` property to more than 20 seconds on Windows or three minutes and 45 seconds on Solaris, the management server ignores the values of this property and reverts back to the default settings.

To modify the default time-out:

1. Access the management server.
2. Click **Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree.
3. Click **Show Default Properties** at the bottom of the page.
4. Copy the `cimom.CimXmlClientHttpConnectTimeout` property you want to modify. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.
5. Return to the Advanced page (**Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree).
6. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
7. Make your changes in the **Custom Properties** field. Make sure the property is not commented out by removing the hash (#) symbol in front of the property.
8. To modify the time-out period, set the `cimom.CimXmlClientHttpConnectTimeout` property to the number of millisecond you want. For example, to change the time-out period to 200 ms, set the `cimom.CimXmlClientHttpConnectTimeout` property, as shown in the following example:
   `cimom.CimXmlClientHttpConnectTimeout=200`
9. When you are done, click **Save**.
10. Restart the service for the management server for your changes to take effect.
    While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

“CIM_ERR_FAILED” Message

If you are in a McDATA environment where the EFC Manager Service Processor is managing multiple switches, it is possible that the management server will send SWAPI requests faster than the EFC Manager Service Processor can handle them. The management server may detect this as a failed connection and take corrective action. When this happens, you are shown a “CIM_ERR_FAILED” message whenever the management server tried to access the McDATA switches and directors.

The management server then attempts to reconnect to the EFCM by creating a new SWAPI connection. EFCM versions 8.x and later have five SWAPI connections available. EFCM versions 7.1.3 and later but before version 8.x have three SWAPI connections available. If the management server reconnects successfully, a reconnect event is generated and no further action is necessary.

If the management server cannot reconnect to the EFCM, another event is generated with a severity of major. If this happens, any operation the management server is performing (Get Details) involving switches on that EFCM fails.

To prevent the “CIM_ERR_FAILED” messages, increase the delay between the management server’s SWAPI calls to EFCM, as described in the following steps:

1. Click **Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy `cimom.mcData.swapiThrottle=200`. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.
4. Return to the Advanced page (**Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree).
5. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
6. Make your changes in the **Custom Properties** field by changing the value of `cimom.mcData.swapiThrottle`. For example, the default is 200 milliseconds. To change the value to 800 milliseconds, change the xxx value to 800, as shown in the following example:
   `cimom.mcData.swapiThrottle=800`

Note: If you want no delay, change the value to 0 for 0 milliseconds. The maximum delay you can have is 1,000 milliseconds (`cimom.mcData.swapiThrottle=1000`),

7. When you are done, click **Save**.
8. Restart the service for the management server for your changes to take effect. While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.
9. Verify if you can re-establish communication with EFCM by following the steps in “Re-establishing Communication with EFCM” on page 402. You may need to change the value of the `cimom.mcData.swapiThrottle` property if you cannot re-establish communication with EFCM after following the steps in that section.

Re-establishing Communication with EFCM

To re-establish communication with EFCM, perform the following steps:

1. To check the status of the connection, click the **Test** button on the Discovery Setup screen. If the McDATA provider reports that it can connect to EFCM, the connection has been restored. A provider is a component of the management server that is used to gather information about an element. In this case, the McDATA provider gathers information about McDATA switches for the management server. To ensure the management server does not have corrupt data as a result of the loss of communication, perform Get Details to obtain the latest information from the element.
2. If the ping results to EFCM fails, there is a network problem that must be resolved. Once network connectivity is restored, use the **Test** button to verify the McDATA provider can communicate with EFCM, then do a Get Details.
3. If the **Test** button results from the management server indicates that it still cannot communicate with EFCM, wait approximately three minutes for the lost SWAPI connection to time out, then click the **Test** button again. If it works, do a Get Details.
4. If the **Test** button results continue to indicate a lost connection after three minutes, perform the following steps to restore the connection. Please note these steps involve restarting services on the EFCM server. Any other applications using SWAPI to communicate with EFCM are affected by these actions.

a. Open the EFCM client. Make sure that the EFCM is still actively managing at least one switch. If there are no switches under management, you will not be able to connect to this EFCM.
b. On the EFCM server, stop and restart the Bridge Agent service. Repeat Steps 1 through 3. If the connection is still down, proceed to Step c.
c. On the EFCM server, stop and restart the EFCM services. On Windows, use the McDATA EFCM Manager options in the **Start** > **Programs** menu. Repeat Step 1 through 3. If the connection is still down, proceed to Step d.
d. Reboot the EFCM server. Repeat Step 1 through 3. If the connection is still down, proceed to Step e.
e. Stop and restart the service for the management server. Repeat Step 1 through 3. If the connection is still down, proceed to Step f.
f. Reboot the management server. Repeat Step 1 through 3. If the connection is still down, proceed to Step g.
g. If none of the above steps have restored the connection, refer to the support matrix to determine if the EFCM and switch versions are all supported. Contact technical support for further information.

Communicating with HiCommand Device Manager Over SSL

By default the management server communicates with HiCommand Device Manager through a nonsecure connection. You can configure the management server so that it communicates with HiCommand Device Manager over a secure socket layer (SSL) connection by doing one of the following:

- **Use HTTPS in the discovery address** - Prepend https:// to the discovery address to force the connection to HTTPS mode, for example, https://192.168.1.1, where 192.168.1.1 is the IP address of the host running HiCommand Device Manager. Use this option if you have one HiCommand Device Manager you want to communicate through a secure connection (SSL) and another you want to communicate through a nonsecure connection.
- **Modify an internal property** - Change the value of the `cimom.provider.hds.useSecureConnection` to true, as described in the steps in this section. Use this option if you want all connections to HiCommand Device Manager to be secure (SSL).

To set all connections with HiCommand Device Manager to SSL:

1. Click **Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the `cimom.provider.hds.useSecureConnection` property. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.
4. Return to the Advanced page (**Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree).
5. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
6. Make your changes in the **Custom Properties** field. Make sure the property is not commented out by removing the hash (#) symbol in front of the property.
7. Change the value assigned to the `cimom.provider.hds.useSecureConnection` property to true, as shown in the following example:
   `cimom.provider.hds.useSecureConnection=true`
8. When you are done, click **Save**.
   If you want to connect to another instance of HiCommand Device Manager by using a nonsecure connection, prepend http:// to the discovery address to force the connection to nonsecure mode, for example, http://192.168.1.1, where 192.168.1.1 is the IP address of the host running HiCommand Device Manager.
9. Restart the service for the management server for your changes to take effect.
   While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

Important: While the AppStorManager service is stopped, the following occurs:

- Users are not be able to access the management server.
- The management server is unable to monitor elements at this time.

Unable to Discover a UNIX Host Because of DNS or Routing Issues

If the management server is unable to discover a UNIX host because of a DNS or routing issues, you will need increase the amount of time that passes before the management server times out for that CIM Extension. By default, the management server waits 1,000 ms before it times out. It is recommended you increasing the time before the management server times out to 200000 ms (3.33

minutes), as described in the following steps. If you continue to see time out issues, you can still increase the time before the management server times out, but keep in mind that it will lengthen discovery.

To increase the time out period:

1. Select **Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree.
2. Paste the following text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.

   ```
   cimom.cxws.agency.firstwait=200000
   cimom.cxws.agency.timeout=200000
   ```

   where

   - `cimom.cxws.agency.firstwait` - The firstwait property controls the amount of time required for the management server to wait after it first contacts the CIM Extension on the host before the management server attempts to proceed with a username and password. The default value is 1,000 ms. You are modifying it to wait 20,000 ms or 3.33 minutes.
   - `cimom.cxws.agency.timeout` - The timeout property controls the allowable interval of silence before either the CIM Extension or the management server start to question whether its partner is still alive. If an entity (management server or extension) has not received a message from the other during the interval set by the timeout property, it will send an “are you there” message. If that message is not acknowledged during the interval set by the timeout property, the entity will conclude that the connection is no longer functioning. The CIM Extension will stop attempting to make a connection. When this occurs on the side of the management server, the management server will attempt to re-connect (and it will keep re-attempting until the host becomes available). The default value is 1,000 ms. You are modifying it to wait 20,000 ms or 3.33 minutes.
3. Click **Save**.
4. Restart the service for the management server for your changes to take effect. While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

Unable to View System Explorer After Upgrade

System Explorer might not display if the Java applet plug-in for the Web browser is configured to use a proxy. This issue has been seen after the management server has been upgraded and the Web browser has cached Java class files. Clearing the cache does not correct this issue. The only known work around is to disable the proxy.

Troubleshooting Provisioning

This section describes the following:

- Cannot Access a Resource Owned by Another Controller on page 406
- Error -56 on page 406
- “Can't delete this zone” Message on page 406
- Changes in EFC Manager Requiring Get Details on page 406

Cannot Access a Resource Owned by Another Controller

You received the message about not being able to access a resource owned by another controller because you tried to access a controller that has not been discovered. You should discover all controllers on the Engenio storage system.

For example, assume you discovered only one of the controllers on an Engenio storage system with two controllers. If you want to change a volume, such as add or delete a LUN, you will not be able to make the change to the volume associated with the controller that has not been discovered.

See Chapter 4, “Discovering NAS Devices, Tape Libraries, Switches and Storage Systems” on page 65 for more information on how to discover a controller.

Error -56

If you see `error -56`, the switch has network connection failures/problems. To solve the problem, make sure the switch is physically connected to the network. Then, redo the task you were originally trying to complete.

If you now see `-21(OBJECT_NOT_FOUND)` errors, the switch needs to be rediscovered.

“Can't delete this zone” Message

If you are shown the following message when you try to delete a zone, move the zone to an inactive zone set. Then, delete the zone.

```
Can't delete this zone, it is member of an Active Zoneset
```

Changes in EFC Manager Requiring Get Details

If you use EFC Manager to delete zones or zone sets, perform Get Details on the management server afterwards. The changes are not reflected by the management server until Get Details is done.

Troubleshooting Hardware

This section describes the following:

- About Swapping Host Bus Adapters on page 407
- “Fork Function Failed” Message on AIX Hosts on page 407
- Known Driver Issues on page 407
- Known Device Issues on page 408
- “mailbox command 17 failure status FFF7” Message on page 411
- ”Process Has an Exclusive Lock” Message on page 412

About Swapping Host Bus Adapters

Swapping brands of host bus adapters (HBA) on a Microsoft Windows 2000 host may have undesirable side effects. For example, after swapping out one brand of an HBA for another (including driver installation), `WinMgmt.exe` might crash repeatedly and appear to be associated with an error in the Windows Event Log about being unable to retrieve data from the `PerfLib` subkey in the Registry. To solve this problem, reinstall the operating system.

“Fork Function Failed” Message on AIX Hosts

If a CIM Extension running on AIX detects low physical or virtual memory while starting, a “Fork Function Failed” message appears. A CIM Extension on AIX uses additional memory and CPU resources at start time. If the resources on the AIX machine is already low, you may see the “Fork Function Failed” message. Depending on the AIX operating system or hardware, the host may crash after you see this message.

Known Driver Issues

If you are having problems with a driver, keep in mind the following:

- The software requires the driver to have a compliant SNIA HBA API. Emulex driver version 4.21e does not support the SNIA HBA API.
- If the driver has a compliant SNIA HBA API, make sure the driver is installed correctly.

Known Device Issues

The following table provides a description of the known device issues. You can find the latest information about device issues in the release notes.

Table 18-5: Known Device Issues

Device	Software	Description

AIX host	NA	If you are receiving replication errors for an AIX host, the provider may be trying to connect to the host using the 0.0.0.0 IP address instead of the real host IP address. If this situation is occurring, you would see a message containing the following when you start the CIM Extension:
		`CXWS 3.1.0.144 on 0.0.0.0/0.0.0.0 now accepting connections`
		
		To fix this situation, add the following line to the `/opt/APPQcime/tools/start` file on the AIX host:
		
		`export NSORDER=local,bind`

AIX host using an IBM Storage System	NA	If you have an AIX host using an IBM storage system, not all bindings may be displayed on the bindings page on the Navigation tab. For example, assume diskA on host123 has six paths. All six bindings may not be displayed.

Table 18-5: Known Device Issues (Continued)

Device	Software	Description
Hosts running SGI IRIX version 6.5.22 or 6.5.24	NA	If a host running SGI IRIX version 6.5.22 or 6.5.24, the HBA port page on the Navigation tab in System Explorer displays 0 GB/s for HBA ports.
SGI IRIX host	CXFS file systems	The management server can only monitor CXFS file systems from the host generating the input/output. For example, assume the elements are part of a CXFS file system. When you generate input/out into the metadata server into /folder, only the metadata server is able to monitor the file system. For example, assume the metadata server generates 100 KB write, the management server displays 0 KB write for /folder on the metadata client.
Solaris host	Sun SAN Foundation Suite driver (Leadville driver)	The bindings page reports a SCSI number that comes from the HBAAPI. This number cannot be seen by the user. For example SCSI target 267008 does not correlate to anything.
Solaris host	HDLM	If you sync the Solaris host by itself without the switches and storage, the storage volume page reports all drive types as local. Once you discover the host with the switches and storage, it reports its drives as being external. It was the same result with Active-Active and Active-Standby.
Solaris host	HDLM	Solaris HDLM disks cannot be monitored. If you try monitoring them, the management server displays a message saying “data is late or an error occurred.”

Table 18-5: Known Device Issues (Continued)

Device	Software	Description
Solaris host	HDLM	Do a Get Details for the host by itself. In the bindings page, the controller number are displayed as c-1. For example c-1t0d58. Perform Get Details on the host with storage and switches. The controller numbers are displayed correctly.
Solaris host	VxVM	If you discover a host with any typical SAN disk groups off line, the storage volume page shows SAN mount points as local instead of external. These disks, however, are not accessible. When you perform Get Details with all disk groups online, disks on the SAN are shown as external. Hosts connected directly to a storage system are shown as local, except for hosts connected by fibre. Hosts connected directly to a storage system through fibre are shown as external.
Windows host	VxVM	When a Windows host with VxVM is used, the SCSI bus number is always reported to be one in the SCSI bus column of the Disk Drives page.

Table 18-5: Known Device Issues (Continued)

Device	Software	Description
Any host	NA	The Unmounted Volume field under Capacity Summary automatically displays 0 MB if you discovered the host but not the storage system connected to it. This may occur if you did not enter the IP address of the storage system when performing discovery and/or your license does not allow you to discover a particular storage system. See the Supported Elements section in the “List of Features” to determine which storage systems you can discover. The “List of Features” is accessible from the Documentation Center (**Help** > **Documentation Center**.
IBM Storage Systems	Subsystem Device Driver (SDD) or MPIO (Multi Pathing IO)	If you discovery an IBM storage system without SDD, incorrect stitching is displayed in System Explorer for the storage system. You are shown only one path if the storage system is using MPIO instead of SDD.

“mailbox command 17 failure status FFF7” Message

If one or more of your Microsoft Windows hosts are using an Emulex HBA driver, you may see the following message in Windows Event Viewer:

“mailbox command 17 failure status FFF7”

This message can be safely ignored. The HBAAPI is being used to access data in the FLASH memory of the adapter that does not exist and this is causing the event to be logged. This issue has been seen with version 5.2.2 of the driver.

”Process Has an Exclusive Lock” Message

You will receive a message resembling the one shown below if a process has already locked the EMC Symmetrix storage system and you attempt a process that requires a lock on the Symmetrix storage system. The Symmetrix storage system can become locked for many reasons. For example, the storage system becomes locked when it performs LUN mapping, LUN masking or Get Details. The Symmetrix storage system may also remain locked after a provisioning operation has failed.

“SYMAPI routine SymDevMaskSessionStart failed with error code 188: The operation failed because another process has an exclusive lock on the local Symmetrix.”

After the management server has detected the lock on the Symmetrix storage system, it tries to access the storage system for 15 minutes and logs the errors.

If you receive the error message, determine if someone is performing an operation that requires a lock, such as LUN mapping, LUN masking or Get Details. This also applies even if one of the processes is being used by a third-party product, such as for LUN masking. If so, wait until the process is complete. Only manually remove the lock if you are certain that no other processes are occurring on the storage system. To learn how to remove the lock, refer to the documentation for the Symmetrix storage system.

If a provisioning failure has caused the Symmetrix storage system to remain locked, you are alerted to this situation in Event Manager and on the Properties tab. You may receive a message resembling the following:

```
Unable to end device masking session. Symmetrix '000001835005700' may be
locked.
```

Index

Numerics

3PAR storage systems 109

A

about
  AIX CIM Extension 161
  Altix CIM Extension 175
  HP-UX CIM Extension 187
  IRIX CIM Extension 201
  management server 2
  security 322
  Solaris CIM Extension 225, 253
  Windows CIM Extension 267
accessing
  domain controller 293
  help xxx
account
  password 331
accounts
  users 330
Active Directory 389
adding
  domain controller 293, 316
  elements 341, 343
  IP address 73
  IP range 72
  new elements 151
  organizations 341
  roles 338
  switches 145
  TNS Listener Port 315
  user accounts 330
additional documentation xxx
AIX 388
AIX CIM Extension
  installing 161
  prerequisites 161
  removing 161
  starting 161
  stopping 161
Altix CIM Extension
  installing 175
  prerequisites 175
  removing 175

starting 175
stopping 175
APPIQ_OWNER account 293
APPIQ_USER 317
Application Administrator role 322
applications
discovering 293
assigning
MIME types 147
authentication errors
SNMP 388

B

benefits 2
Bridge Agent 91
Brocade Rapid program 133
Brocade switches 133
discovering 81
building
topology 78, 133

C

certificate
installing 34
changing
database 78
domain controller 293, 316
e-mail address 334
full name 334
login name 334
number of retries 106, 383
organizations 343
password 135, 317, 332, 333, 334
phone number 334
roles 339
SNMP trap listener 90
time-out period 106, 383
TNS Listener Port 315
user account 331
user name 135
user preferences 335
user profile 334
child organizations 322
CIM xxix, 2
OpenVMS 240
CIM Extension
installing 187, 225, 253, 267
port 367
Solaris 187, 225, 253
Windows 267
CIM Extensions
about 161, 175, 187, 201, 225, 253, 267
AIX 161
Altix 175
HP-UX 187
IRIX 201
Solaris 225, 253
Windows 267
cimom.CimXmlClientHttpConnectTimeout 399
cimom.emc.skipRefresh 141
cimom.hds.exclude 117
cimom.symmetrix.exclude 112
CIO role 322
Cisco SMI-S switches
troubleshooting 381
clearing
elements 76
CNT
switches 87
controller
removing 293
cookies
JavaScript 2
creating
new password 333
organizations 341
roles 338
topology 65
user accounts 330

D

database
AIX 388
management server 9, 45
updating 78
database connection failed
error 385
DCOM
unable to communicate 387

deleting
domain controller 293
elements 76, 136
organizations 345
roles 340
switches 146
TNS Listener Port 315
user accounts 333
zone sets 407
zones 407
details
obtaining 138
detecting
IP range 72
McDATA switches 145
switches 145
device issues 408
devices
deleting 136
discovered address
modifying 135
discovered elements
deleting elements 136
discovering
applications 293
Brocade switches 81, 133
CNT switches 87
DNS Name 73
EMC Solutions Enabler 110
HDS storage systems 116
HDS systems 117
HP XP storage systems 118, 119
IBM storage systems 122
IP address 73
McDATA switches 91
Microsoft Exchange 293, 310, 389
NetApp filers 130
new elements 151
Oracle 293, 294
Oracle clusters 294
passwords 70
SQL servers 300
storage system 65
storage systems 114, 124
Sun StorEdge storage systems 124, 126
Sun StorEdge switches 89
switches 65, 81
Sybase 293, 306
Symmetrix systems 112
troubleshooting 389, 391, 412, 413
user names 70
discovery
authentication errors 388
quarantine 149, 150
time-out 399
troubleshooting 385
Windows proxy 282
discovery groups 135
discovery requirements
Oracle 389
discovery settings
importing 76
saving 77
disk drive 318, 399
displaying
deleted Oracle instances 389
DNS 389
documentation
additional xxx
Domain Administrator role 322
domain controller
access 316
accessing 293, 316
removing 293
domain controller access 293, 316
drivers
fixing 408
drives
Microsoft Exchange 389
uninitialized 399

E

editing
e-mail address 334
full name 334
login name 334
organizations 343, 345
password 332, 333, 334

phone number 334
roles 339
user account 331
user preferences 335
user profile 334
EFC Manager 91, 407
element details
obtaining 138
elements
adding 341, 343
deleting 76, 136
getting details 78
managing 343
modifying 135
organization 343
removing 345
topology 133
unable to find 391, 397
e-mail address
changing 334
EMC CLARiiON 114
EMC Solutions Enabler 110
error
database connection failed 385
error -56 407
Error 503 365
error message
exclusive lock 412, 413
errors
authentication 388
excluding
HDS systems 117
switches 103
Symmetrix systems 112
exclusive lock
error message 412, 413
Extension
CIM 187, 225, 253

F

features
key 2
file extension
assigning 147
filtering
organizations 346
finding
applications 293
hosts 293
information xxx
IP address 73
IP range 72
new elements 151
storage systems 65
switches 65
fixing
drivers 408
full name
changing 334

G

Get Details
email notification 382
getting
element details 138
getting details 78, 138
applications 293
hosts 293

H

HBAs
swapping 408
HDS storage systems
discovering 116
HdsSkipRefresh 142
help
accessing xxx
Help Desk role 322
hierarchy
organizations 322
host
not in topology 391, 397
host bus adapter
unable to detect 398
hosts
discovering 293
removing 76
hot-swapped
drives 399
HP XP storage systems 118, 119

HP-UX CIM Extension
  installing 187
  prerequisites 187
  removing 187
  starting 187
  stopping 187
HTTP Error 503 365
HTTPS 9, 34, 45

I

IBM storage systems
  discovering 122
importing
  discovery settings 76
inaccessible
  device 406
information
  finding xxx
  obtaining element 138
installation
  OpenVMS CIM 240
installing
  AIX CIM Extension 161
  Altix CIM Extension 175
  CIM Extension 187, 225, 253, 267
  HP-UX CIM Extension 187
  IRIX CIM Extension 201
  Java plug-in 32, 36, 54, 55
  management server 9, 45
  OpenVMS CIM 240
  security certificate 9, 34, 45
  Solaris CIM Extension 225, 253
  Windows CIM Extension 267
intended audience xxix
intended_audience xxix
internal
  drives 399
IP range 72
IRIX CIM Extension
  installing 201
  prerequisites 201
  removing 201
  starting 201
  stopping 201
issues
  devices 408

J

Java 2
Java plug-in
  installing 32, 36, 54, 55

K

key benefits 2
key features 2

L

local drives 389
locating
  storage systems 65
  switches 65
log messages
  viewing 106
login name
  modifying 334

M

management server
  about 2
  database 9, 45
  installing 9, 45
  porting across operating systems 36, 42, 55, 62
  security 322
managing
  elements 341, 343, 345
  switches 145
McDATA switches 398
  adding 145
  discovering 91
messages
  data is late 364
Microsoft Exchange
  discovering 293, 310, 389
  drive M 389
MIME types 147
mixed mode authentication 301
modifying
  database 78
  discovered address 135

discovery IP address 75
DNS name for discovery 75
domain controller 293, 316
elements 135
e-mail address 334
full name 334
login name 334
organizations 343
password 135, 317, 332, 333, 334
phone number 334
roles 339
SNMP trap listener 90
TNS Listener Port 315
user account 331
user name 135
user preferences 335
user profile 334
moving
management server 36, 55

N

naming organizations 322
NetApp filers
discovering 130
netcnfg 110
nethost 110
Networking xxix
new elements
adding 151
new password 333
nonexistent IP addresses 399
nonexistent Oracle instances 389
number of retries
changing 106, 383

O

obtaining
security certificate 34
topology information 133
online help xxx
OpenVMS
CIM
installing 240
OpenVMS CIM installation
prerequisites 240
Oracle
deleted instances 389
discovering 293, 294
discovery requirements 389
Oracle TNS Listener Port 315
organizations
about 322
adding 341
deleting 345
editing 343, 345
elements 341, 343, 345
filtering 346
properties 337
users 337
viewing 343

P

parent organizations 322
password
changing 135, 317, 331, 332, 333, 334
Performance Explorer
Java plug-in 32, 36
phone number
editing 334
planning organizations 322
port
CIM Extension 367
porting
management server 36, 55
Prerequisites
OpenVMS CIM installation 240
prerequisites
AIX CIM Extension 161
Altix CIM Extension 175
HP-UX CIM Extension 187
IRIX CIM Extension 201
Solaris CIM Extension 225, 253
Windows CIM Extension 267
privileges
roles 322
problems
drivers 408
process
exclusive lock 412, 413
profile

user 334
properties
organizations 337
roles 337
provisioning
troubleshooting 406, 407, 412, 413

Q

quarantine
adding elements 149
clearing elements 150

R

Rapid program 133
refreshing
Symmetrix systems 141
remote drives 389
removing
AIX CIM Extension 161
Altix CIM Extension 175
domain controller 293
elements 76, 136, 343, 345
HP-UX CIM Extension 187
IRIX CIM Extension 201
organizations 345
roles 340
Solaris CIM Extension 225, 253
switches 146
TNS Listener Port 315
user accounts 333
Windows CIM Extension 267
zone sets 407
zones 407
replacing
switches 146
replication 78
requirements 2
software 2
roles
about 322
adding 338
Application Administrator 322
CIO 322
deleting 340
Domain Administrator 322
editing 339
Element Control privilege 322
Full Control privilege 322
Help Desk 322
privileges 322
properties 337
Server Administrator 322
Storage Administrator 322
users 337
View privilege 322

S

SAN xxix
saving
discovery settings 77
settings to a file 77
scanning
IP range 72
security
Management server 322
roles 338, 339
security certificate
installing 9, 34, 45
Server Administrator role 322
setting
discovery passwords 70
discovery user name 70
silent installation
Windows 273
SMI-S support
troubleshooting 380
SMI-S switches
see the support matrix 81, 380
SNMP
authentication errors 388
SNMP trap listener
changing 90
software requirements 2
Solaris
porting management server 36, 55
Solaris CIM Extension
installing 225, 253
prerequisites 225, 253
removing 225, 253
starting 225, 253

stopping 225, 253
SQL Server
authentication modes 301
SQL servers
discovering 300
starting
AIX CIM Extension 161
Altix CIM Extension 175
HP-UX CIM Extension 187
Solaris CIM Extension 225, 253
Windows CIM Extension 267
statistics 318
Step 42, 62
stopping
AIX CIM Extension 161
Altix CIM Extension 175
HP-UX CIM Extension 187
IRIX CIM Extension 201
SAN details 140
Solaris CIM Extension 225, 253
Windows CIM Extension 267
Storage Administrator role 322
storage systems 124, 318
discovering 65, 124
removing 76
storage terms 2
Sun StorEdge
SNMP trap listener 90
Sun StorEdge storage systems 124, 126
Sun StorEdge switches 89
swapped
drives 399
swapping
switches 146
swapping HBAs 408
switches
adding 145
discovering 65, 81
excluding 103
managing 145
McDATA 91, 145, 398
number of retries 106, 383
removing 76, 146
replacing 146
time-out period 106, 383
unable to monitor 398
Sybase
discovering 293, 306
System Explorer
can't access 406
deleting elements 136
Java plug-in 32, 36

T

terms
storage 2
time-out period
changing 106
TNS Listener Port
changing 315
topology
AIX 388
building 133
host not appearing 391, 397
topology issues 391
troubleshooting
Cisco SMI-S switches
switch names 381
discovery 385
discovery and getting element details 385, 387, 389, 391, 397, 412, 413
Microsoft Exchange 389
provisioning 406, 407, 412, 413
SMI-S switches 81, 380

U

unable to
discover 385
Unable to access resource 406
unable to detect
host bus adapter 398
unable to find
elements 397
unable to retrieve data 408
uninitialized
drives 399
updating
database 78
user accounts

creating 330
deleting 333
user name
changing 135
user preferences
changing 335
user profile
modifying 334
users
about 322
adding 330
organizations 337
roles 337, 338, 339

V

viewing
log messages 106
organization properties 337
organizations 343
security certificate 34
topology 65

W

Web browsers 2
WEBEM 2
Windows
porting management server 36, 55
silent installation 273
Windows CIM Extension
installing 267
removing 267
starting 267
stopping 267
Windows proxy
discovery 282
WinMgmt.exe 391

X

Xiotech storage systems 127

Z

zone sets
deleting 407
zones
deleting 407