



Sun StorageTek™ Operations Manager 6.0 Installation Guide

Sun Microsystems, Inc.
www.sun.com

Part No. 817-7922-16
January 2008, Revision A

Submit comments about this document at: <http://www.sun.com/hwdocs/feedback>

Copyright 2002-2007 Hewlett-Packard Development Company, L.P., 3000 Hanover Street, Palo Alto, California 94304, U.S.A. All rights reserved.
Copyright 2002-2007 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

This document and the product to which it pertains are distributed under licenses restricting their use, copying, distribution, and decompilation. No part of the product or of this document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any.

Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd. Sun, Sun Microsystems, the Sun logo, AnswerBook2, docs.sun.com, Sun StorageTek, Java, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and in other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and in other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

U.S. Government Rights—Commercial use. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

Microsoft and Windows are registered trademarks of Microsoft Corporation. Oracle is a registered trademark of Oracle Corporation. AIX and IBM are registered trademarks of International Business Machines Corporation in the United States, other countries or both. McDATA is a registered trademark of McDATA Corporation. Engenio is a registered trademark of Engenio Corporation. CLARiiON is a registered trademark of EMC Corporation. SGI and IRIX are registered trademarks of Silicon Graphics, Inc. Netscape is a registered trademark of Netscape Communications Corporation in the United States and other countries. HP, HP-UX, and OpenVMS, Tru64 UNIX are registered trademarks of Hewlett-Packard Development Company. QLogic is a trademark of QLogic Corporation. Emulex is a registered trademark of Emulex Corporation. HBAware is a trademark of Emulex Corporation.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2002-2007 Hewlett-Packard Development Company, L.P., 3000 Hanover Street, Palo Alto, Californie 94304, Etats-Unis. Tous droits réservés.
Copyright 2002-2007 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, Californie 95054, Etats-Unis. Tous droits réservés.

Sun Microsystems, Inc. a les droits de propriété intellectuelle relatants à la technologie qui est décrit dans ce document. En particulier, et sans la limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains énumérés à <http://www.sun.com/patents> et un ou les brevets plus supplémentaires ou les applications de brevet en attente dans les Etats-Unis et dans les autres pays.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a.

Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, AnswerBook2, docs.sun.com, Sun StorageTek, Java, et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciées de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

Microsoft et Windows sont des marques déposées de Microsoft Corporation. Oracle est la marque déposée de Oracle Corporation. AIX et IBM des marques déposées de International Business Machines Corporation aux Etats-Unis et dans d'autres pays. McDATA est la marque déposée de McDATA Corporation. Engenio est la marque déposée de Engenio Corporation. CLARiiON est la marque déposée de EMC Corporation. SGI et IRIX des marques déposées de Silicon Graphics, Inc. Netscape est la marque déposée de Netscape Communications Corporation aux Etats-Unis et dans d'autres pays. HP, HP-UX, et OpenVMS, Tru64 UNIX des marques déposées de Hewlett-Packard Development Company. QLogic est une marque déposée de QLogic Corporation. Emulex est la marque déposée d'Emulex Corporation. HBAware est une marque déposée d'Emulex Corporation.

LA DOCUMENTATION EST FOURNIE "EN L'ÉTAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFAÇON.



Adobe PostScript

Contents

1. Overview	1
Supported Platforms for Installing the Management Server	1
Roadmap for Installation and Initial Configurations	1
About this Product	3
Storage Management Terms	4
Key Benefits	4
Key Features	4
Software Requirements	5
Web Browser Configuration Requirements	5
2. Installing the Management Server on Linux	7
Pre-installation Checklist	8
Pre-requisite RPMs for Oracle on Linux	8
Software Dependencies	9
Verify Network Settings	11
Installing from a Network Drive	12
Step 1 - Install the Oracle Database	12
Before Installing the Oracle Database	13
Prerequisites	13
Installing the Database	14

Oracle Critical Patch Update	21
Accessing the Linux Host	24
Step 2 - Install the Management Server	25
Step 3 - Verify that Processes Can Start	28
Step 4 - Configure Firefox	31
Installing the Java Plug-in on Linux	33
Configurations Required for Discovering EMC CLARiiON Storage Systems	34
Removing the Management Server	34
Upgrading the Linux Management Server from v5.1 to v6.0	37
Considerations Before You Upgrade	37
Upgrade Overview	39
Steps to Upgrade the Management Server	40
Step 1 - Read the Support Matrix and Release Notes	40
Step 2 - Verify that You Are Running Build 5.1 Service Pack 4 or a Later 5.1 Service Pack	41
Verify that you have a working Build 5.1, SP4 management server before upgrading to Build 6.0. Existing installations that are at Build 5.1, SP1, Build 5.1, SP2, or Build 5.1, SP3, must upgrade to Build 5.1, SP4 or later prior to upgrading to Build 6.0. Step 3 - Save Configuration Files for the Global	
Change Management Business Tool	41
Step 4 - Run the upgradeAppStorManager Script	41
Step 5 - Run the uninstallOracle9i Script	41
Step 6 - Install the Oracle 10g Database	42
Step 7 - Upgrade the Management Server	43
Step 8 - Import the Database	43
Step 9 - Start Management Server	43
Step 10 - Customize Database Passwords	43
Step 11 - Enable RMAN Backup if Desired	43
Step 12 - Upgrade Selected CIM Extensions	44
Step 13 - Rediscover All Elements	44

Steps that Can Be Run Anytime after the Upgrade	44
Re - Add Remote Sites in Global Reporters	45
Migrate Your Brocade Switches to SMI-A	45
About Migrating Your Brocade Switches to SMI-A	45
Upgrade Your CLI Clients	48
Upgrading Your CIM Extensions	48
3. Installing the Management Server on Sun Solaris	49
Step 1 - Install the Oracle Database (Solaris)	50
Before Installing the Oracle Database	50
Prerequisites	50
Installing the Database	53
Step 2 - Install the Management Server	59
Step 3 - Verify that Processes Can Start	61
Step 4 - Verify You Can Connect to the Management Server	63
Installing the Java Plug-in on Sun Solaris	64
Configurations Required for Discovering EMC CLARiiON Storage Systems	65
Removing the Management Server	66
Porting the Management Server Across Operating Systems	69
Upgrading the Management Server	70
Considerations Before you Upgrade	72
Step 1 - Read the Support Matrix and the Release Notes	72
Step 2 - Verify your Version	73
Step 3 - Save the Configuration Files	73
Step 4 - Manually Export the Database and Create an Image of the Server	73
Step 5 - Run the upgradeAppStorManager script	73
Step 6 - Upgrade Oracle 9i to Oracle 10gr	75
Step 7 - Upgrade the Management Server	76

Step 8 - Upgrade and Start the Windows Proxy	76
Step 9 - Execute migrateData.sh	76
Step 10 – Customize Database Passwords	78
Step 11 - Enable RMAN Backup if desired	78
Step 12 - Upgrade Select CIM Extensions	78
Step 13 - Rediscover All Elements	78
Steps that can be run anytime after the Upgrade	79
Re-add Remote Sites in Global Reporter	79
Upgrade your CLI Clients	83
Upgrading your CIM Extensions	83
4. Installing the Management Server on Microsoft Windows	85
Pre-installation Checklist	
(Installations and Upgrades)	86
Installation and Upgrade Requirements	
(Cannot Proceed with Install/Upgrade if	
Not Met)	87
About the Verify System Requirements Screen	88
How to turn off Internet Information Services (IIS) and	
Third-Party Web servers	89
How to Verify Networking	89
Be Sure to Install a Supported Browser	90
About the Windows Installer	90
Installing the Management Server for Windows	91
Step 1 – Read the Support Matrix and Release Notes	91
Step 2 – Install the Management Server for Windows	91
Step 3 –	93
Step 4 – Check for Required Service Packs	
and Hot Fix Files	94
Step 5 – Install Your CIM Extensions and Set Up Discovery	94

Upgrading the Windows Management Server	94
Keep in Mind the Following	94
Considerations Before Upgrading	94
About the Windows Upgrade Wizard	96
About Migrating Brocade Fabric Access API-Managed Switches to SMI-S After Upgrading	96
About Resetting Archive Mode After Upgrading If You Use Automatic RMAN Backups	97
About CIM Extensions and Backup Manager Hosts After Upgrading	97
Upgrading the Management Server for Windows	100
Step 1 – Read the Support Matrix and Release Notes	100
Step 2 – Verify that You are Running Build 5.1 Service Pack 4 or a Later Build 5.1 Service Pack	101
Step 3 – Save Configuration Files for the Global Change Management Business Tool	101
Step 4 – Manually Export the Database	101
Step 5 – Start the Upgrade Wizard	101
Step 6 – Customize Database Passwords	104
Step 7 – Enable RMAN Backup if Desired	104
Step 8 – Upgrade Select CIM Extensions	104
Step 9 – Rediscover all Elements	104
Steps That Can be Run Anytime After the Upgrade	105
Re-add Remote Sites in Global Reporter	105
Upgrade your CLI Clients	106
Upgrading your CIM Extensions	107
Migrate Your Brocade Switches to SMI-A	107
Check any McDATA and Connectrix Switches	109
Configurations Required for Discovering EMC CLARiiON Storage Systems	110
Removing the Management Server	110

5. Managing Licenses	113
Modifying the License Summary Page	117
6. Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries	119
Discovery Steps	120
Overall Discovery Tasks	120
Overview of Discovery Features	122
Setting Default User Names and Passwords	122
Adding an IP Range for Scanning	125
Adding a Single IP Address or DNS Name for Discovery	127
Modifying a Single IP Address Entry for Discovery	128
Removing Elements from the Addresses to Discover List	129
Importing Discovery Settings from a File	129
Importing a File	130
Re-discovering the Management Server	130
Saving Discovery Settings to a File	131
Discover Switches	132
Discovering Brocade Switches	133
Migrating Brocade API Switches to SMI-S After Upgrading	133
To Discover Brocade SMI-S Switches	136
Discovering CNT Switches	137
Discovering Cisco Switches	138
Discovering Sun StorEdge, QLogic and HP StorageWorks M-Series for p-Class BladeSystems	140
Discovering McDATA and EMC Connectrix Switches	142
Discovering McDATA and Connectrix switches with SMI-S	143
Discovering McDATA and Connectrix Switches through a Proxy with SWAPI	145

Discovering McDATA and Connectrix Switches through a Proxy with SNMP	147
Discovering McDATA and Connectrix Switches through a Direct Connection and SNMP	149
Changing the Discovery Settings	150
Excluding McDATA and EMC Connectrix Switches from Discovery	151
Managing McDATA and EMC Connectrix Switches	152
Changing the SNMP Trap Listener Port and Community String for Switches Discovered with SNMP	155
Discover Storage Systems, NAS Devices and Tape Libraries	156
Discovering 3PAR Storage Systems	157
Discovering EMC Solutions Enabler	158
Excluding EMC Symmetrix Storage Systems from Discovery	159
Excluding EMC Symmetrix Storage Systems from Force Device Manager Refresh	160
Discovering EMC CLARiiON Storage Systems	161
Discovering LSI Storage Systems	162
Discovering HDS Storage Systems	163
Excluding HDS Storage Systems from Discovery	164
Excluding HDS Storage Systems from Force Device Manager Refresh	166
Discovering HP StorageWorks MSA Arrays	167
Discovering HP StorageWorks EVA Arrays	168
Obtaining SNMP Traps using Command View EVA	169
Discovering HP StorageWorks XP Arrays	171
Discovering HP XP Arrays by Using Command View XP and SMI-S	172
Discovering HP XP Arrays Using Command View XP Advanced Edition	173
Discovering HP XP Arrays by using the built-in XP Provider	174
Discovering IBM Storage Systems	174

Discovering Sun StorEdge 3510 Storage Systems	176
Discovering Sun StorEdge 6920 and 6940 Storage Systems	178
Discovering Sun StorEdge 6130 Storage Systems	179
Discovering Xiotech Storage Systems	179
Discovering HP NAS Devices on Windows	180
Discovering HP NAS Devices on Linux	181
Discovering NetApp NAS Devices	183
Enabling SSL Communication with a NetApp NAS Device	184
Discovering Sun NAS Devices	184
Discovering HP and IBM Tape Libraries	185
Building the Topology	186
Building the Topology View	186
Modifying the Properties of a Discovered Address	187
Get Details	188
About Get Details	188
Running Get Details	189
Stopping the Gathering of Details	190
Using Discovery Groups	191
Creating Custom Discovery Lists	192
Managing Discovery Groups	192
Moving Elements Between Discovery Groups	193
Deleting Elements from the Product	194
Deleting an Element Using System Explorer or Chargeback	195
Deleting Elements Using Discovery Step 2 (Topology)	196
Working with Quarantined Elements	197
Placing an Element in Quarantine	197
Removing an Element from Quarantine	197
Updating the Database with Element Changes	198

Notifying the Software of a New Element	199
Viewing Log Messages	200
Viewing the Status of System Tasks	201
7. Deploying and Managing CIM Extensions	203
Remote CIM Extensions Management	203
About SSH	204
Copying the CIM Extensions to the Management Server	205
Creating Default Logins for Hosts	206
The CIM Extension Management Wizard	206
The CIM Extensions Management Tool	208
Launching the CIM Extensions Management Tool	208
Adding Remote Hosts	209
Host Lists	209
Importing a Host List	209
Exporting a Host List	210
Managing CIM Extensions on Remote Hosts	210
Configuring CIM Extensions	211
Log Files	212
Status Icons	212
About Upgrading Your CIM Extensions	213
8. Installing the CIM Extension for IBM AIX	215
About the CIM Extension for IBM AIX	216
Prerequisites	216
Verifying SNIA HBA API Support	217
Installing the CIM Extension	218
Setting Up Monitoring	219
Starting the CIM Extension Manually	220

How to Determine if the CIM Extension Is Running	220
Configuring CIM Extensions	221
Changing the Port Number	221
Adding a New Port Number to Discovery	221
Configuring the CIM Extension to Listen on a Specific Network Card	222
Additional Parameters	223
Finding the Version of a CIM Extension	223
Stopping the CIM Extension	224
Rolling Over the Log Files	224
Fulfilling the Prerequisites	224
Removing the CIM Extension from AIX	226
9. Installing the CIM Extension for SGI ProPack for Linux	227
About the CIM Extension for SGI ProPack for Linux	228
Prerequisites	228
Verifying SNIA HBA API Support	229
Installing the CIM Extension	230
Starting the CIM Extension Manually	231
How to Determine if the CIM Extension Is Running	233
Configuring CIM Extensions	233
Changing the Port Number	233
Adding a New Port Number to Discovery	234
Configuring the CIM Extension to Listen on a Specific Network Card	234
Additional Parameters	235
Stopping the CIM Extension	236
Rolling Over the Log Files	236
Removing the CIM Extension from SGI ProPack for Linux	237
10. Installing the CIM Extension for SGI IRIX	239

About the CIM Extension for SGI IRIX	239
Prerequisites	240
Verifying SNIA HBA API Support	240
Installing the CIM Extension	241
Starting the CIM Extension Manually	242
How to Determine if the CIM Extension Is Running	243
Configuring CIM Extensions	243
Changing the Port Number	243
Adding a New Port Number to Discovery	244
Configuring the CIM Extension to Listen on a Specific Network Card	244
Additional Parameters	245
Starting the CIM Extension by chkconfig	246
Finding the Version of a CIM Extension	246
Stopping the CIM Extension	247
Rolling Over the Logs	247
Removing the CIM Extension from SGI IRIX	248
11. Installing the CIM Extension for HP-UX	249
About the CIM Extension for HP-UX	249
Prerequisites	250
Verifying SNIA HBA API Support	250
Installing the CIM Extension	251
Starting the CIM Extension Manually	253
How to Determine if the CIM Extension Is Running	253
Configuring CIM Extensions	254
Restricting the Users Who Can Discover the Host	254
Changing the Port Number	255
Adding a New Port Number to Discovery	255
Configuring the CIM Extension to Listen on a Specific Network Card	256

Additional Parameters	256
Finding the Version of a CIM Extension	257
Combining Start Commands	258
Stopping the CIM Extension	258
Rolling Over the Log Files	258
Fulfilling the Prerequisites	259
Removing the CIM Extension from HP-UX	259
12. Installing the CIM Extension for SUSE and Red Hat Linux	261
About the CIM Extension for Red Hat Linux Advanced Server and SUSE Linux	262
Prerequisites	262
Verifying SNIA HBA API Support	262
Driver Information for Verifying Emulex SNIA Adapters	263
Driver Information for Verifying QLogic SNIA Adapters	264
Installing the CIM Extension	264
Starting the CIM Extension Manually	267
How to Determine if the CIM Extension Is Running	267
Configuring CIM Extensions	268
Changing the Port Number	268
Adding a New Port Number to Discovery	268
Configuring the CIM Extension to Listen on a Specific Network Card	269
Additional Parameters	270
Finding the Version of a CIM Extension	270
Stopping the CIM Extension	271
Rolling Over the Log Files	271
Removing the CIM Extension from Red Hat or SUSE Linux	272
13. Installing the CIM Extension for NonStop	273
About the CIM Extension for NonStop	273

Prerequisites	274
NonStop G06.27 or later Software Requirements	274
Network Port	274
Installing the CIM Extension	275
Verifying SNIA HBA API Support	277
Starting the CIM Extension Manually	277
Restricting the Users Who Can Discover the Host	279
Changing the Port Number	279
Specifying the CIM Extension to Listen on a Specific Network Card	280
Finding the Version of a CIM Extension	282
Combining Start Commands	282
Finding the Status of the CIM Extension	282
Stopping the CIM Extension	283
Rolling Over the Logs	283
Increasing the native logging level	284
Fulfilling the Prerequisites	284
Removing the CIM Extension from NonStop	284
Handling Daylight Savings Time Changes for the NonStop CIM Extension	285
14. Installing the CIM Extension for OpenVMS	287
About the CIM Extension for OpenVMS	287
Prerequisites	288
Installing the CIM Extension	289
Installing the CIM Extension on a Standalone Host	289
Installing the CIM Extension on a Cluster	291
Starting the CIM Extension Manually	291
How to Determine if the CIM Extension is Running	292
Configuring CIM Extensions	292
Restricting the Users Who Can Discover the Host	293

Changing the Port Number	294
Adding a Port Number to Discovery	294
Configuring the CIM Extension to Listen on a Specific Network Card	295
Additional Parameters	296
Finding the Version of a CIM Extension	296
Combining Start Commands	297
Modifying the Boot Time Start Script (Optional)	297
Stopping the CIM Extension	298
Rolling Over the Log Files	298
Increasing the Native Logging Level	299
Removing the CIM Extension from OpenVMS	299
Uninstalling the OpenVMS CIM Extension on a Standalone Host	299
Uninstalling the OpenVMS CIM Extension on a Cluster Host	300
15. Installing the CIM Extension for Sun Solaris	301
About the CIM Extension for Solaris	301
Prerequisites	302
Verifying SNIA HBA API Support	303
Installing the CIM Extension	304
Starting the CIM Extension Manually	305
How to Determine if the CIM Extension Is Running	306
Configuring CIM Extensions	306
Restricting the Users Who Can Discover the Host	307
Changing the Port Number	307
Adding a New Port Number to Discovery	308
Configuring the CIM Extension to Listen on a Specific Network Card	308
Additional Parameters	309
Finding the Version of a CIM Extension	310
Combining Start Commands	310

Stopping the CIM Extension	311
Rolling Over the Log Files	311
Removing the CIM Extension from Solaris	312
16. Installing the CIM Extension for HP Tru64 UNIX	313
About the CIM Extension for Tru64 UNIX	314
Prerequisites	314
Installing the CIM Extension	315
Installing the CIM Extension on a Standalone Host	315
Installing the CIM Extension on a Cluster	316
Verifying SNIA HBA API Support	317
Starting the CIM Extension Manually	318
How to Determine if the CIM Extension Is Running	318
Configuring CIM Extensions	319
Restricting the Users Who Can Discover the Host	319
Changing the Port Number	320
Adding a New Port Number to Discovery	320
Configuring the CIM Extension to Listen on a Specific Network Card	321
Additional Parameters	321
Finding the Version of a CIM Extension	322
Stopping the CIM Extension	323
Rolling Over the Logs	323
Increasing the Native Logging Level	324
Fulfilling the Prerequisites	324
Removing the CIM Extension from Tru64	324
Removing the CIM Extension from a Standalone Host	324
Removing the CIM Extension from a Cluster	325
17. Installing the CIM Extension for Microsoft Windows	327

About the CIM Extension for Windows	328
Verifying SNIA HBA API Support	329
Installing the CIM Extension	330
Installing the CIM Extension Using the Silent Installation	331
Upgrading a Host with the Latest CIM Extension	331
Configuring CIM Extensions	332
Changing the Port Number	333
Adding a New Port Number to Discovery	333
Configuring the CIM Extension to Listen on a Specific Network Card	334
Defining UNC Volumes	335
Additional Parameters	336
Rolling Over the Log Files	336
Removing the CIM Extension from Windows	337
18. Installing and Discovering the Windows Proxy	339
Installing the Windows Proxy	340
Discovering the Windows Proxy	341
Configuring Windows Proxy Authentication	342
Decreasing the Maximum Java Heap Size	343
Removing the Windows Proxy	344
19. Discovering Applications, Backup Hosts and Hosts	345
Step 1 — Discovering Your Hosts and Backup Manager Hosts	345
Step A — Set Up Discovery for Hosts	347
Step B — Build the Topology	350
(Optional) Step C — View the Topology	351
Step D — Get Details	351
Step 2 — Setting Up Discovery for Applications	353
Creating Custom Passwords on Managed Database Instances	354

Monitoring Oracle	355
Step A — Create the APPIQ_USER Account for Oracle	355
Removing the APPIQ_USER Account for Oracle	357
Step B — Provide the TNS Listener Port	359
Step C — Set up Discovery for Oracle 10g	359
Discovering Oracle Real Application Clusters (RAC)	360
Deleting Oracle Application Information	363
Monitoring Microsoft SQL Server	363
Switching to Mixed Mode Authentication	364
Step A — Create the appiq_user Account for the Microsoft SQL Server	365
Step B — Provide the Microsoft SQL Server Name and Port Number	368
Removing the appiq_user Account for Microsoft SQL Server	370
Deleting Microsoft SQL Server Information	371
Monitoring Microsoft SQL Server Clusters	372
Monitoring Sybase Adaptive Server Enterprise	374
Step A — Create the APPIQ_USER account for Sybase	375
Removing the APPIQ_USER Account for Sybase	376
Step B — Provide the Sybase Server Name and Port Number	377
Deleting Sybase Information	378
Monitoring Microsoft Exchange	378
Adding Microsoft Exchange Domain Controller Access	378
Editing a Microsoft Exchange Domain Controller	380
Deleting a Microsoft Exchange Domain Controller	380
Monitoring Microsoft Exchange Failover Clusters	380
Monitoring Caché	381
Step A — Import the Wrapper Class Definitions into the Caché Instance	381
Step B — Create APPIQ_USER Account on the Caché Instance	386

Removing the APPIQ_USER Account from the Caché Instance	389
Step C — Provide the Caché Instance Name and Port Number	391
Deleting Caché Information	392
Step 3 — Discovering Applications	392
Step A — Detect Your Applications	393
Step B — Obtain the Topology	393
Step C — Run Get Details	394
Changing the Oracle TNS Listener Port	396
Changing the Password for the Managed Database Account	396
20. Host and Application Clustering	399
About Clustering	399
Discovering Clusters	399
Automatic Discovery of Host Clusters	400
Manual Discovery of Host Clusters	401
Filtering Hosts	402
File Servers and Clusters	403
Clustering in System Explorer	403
Clustering in Topology	405
Clustering in Capacity Manager	407
21. Managing Security	409
About Security for the Management Server	409
About Roles	410
About Organizations	413
Planning Your Hierarchy	415
Naming Organizations	416
Managing User Accounts	416
Adding Users	416

Editing a User Account	418
Changing the Password for a User Account	419
Changing Your Password	420
Deleting Users	420
Modifying Your User Profile	420
Modifying Your User Preferences	421
System, Capacity and Performance Manager Preferences	421
System Explorer and Element Topology Preferences	422
Warnings for Slow Systems Operations	422
Viewing the Properties of a Role	422
Viewing the Properties of an Organization	423
Managing Roles	423
Adding Roles	424
Editing Roles	424
Deleting Roles	425
Managing Organizations	426
Adding an Organization	426
Adding Storage Volumes to an Organization	428
Viewing Organizations	428
Editing an Organization	429
Removing an Organization	430
Removing Members from an Organization	430
Filtering Organizations	431
Changing the Password of System Accounts	432
Using Active Directory/LDAP for Authentication	434
Step 1 — Configure the Management Server to Use AD or LDAP	434
Configuring the Management Server to Use Active Directory	435
Configuring the Management Server to Use LDAP	439

Step 2 — Restart the AppStorManager Service and Login as the Designated Admin Account	443
Step 3 — Add Users to the Management Server	444
Step 4 — Provide Login Information to Your Users	444
22. Troubleshooting	447
Troubleshooting Installation/Upgrade	447
If Your Installation or Upgrade Failed, Capture the Logs	448
Checking Installation Log Files	449
“The environment variable ‘perl5lib’ is set.” Message	449
“SEVERE: OUI-10029...” Message	450
Brocade API Switches Displaying Stale Data	450
Troubleshooting the Oracle Database (Windows)	450
Use Only the Installation Wizard (or Unix Scripts) to Install/Upgrade Oracle	450
Cancelling an Installation or Upgrade Before Completion	451
Uninstalling Oracle Using the Oracle Scripts	451
Re-installing the Management Server	452
Existing Oracle Database Is Detected	452
Configuring the Java Console	452
“Data is late or an error occurred” Message	453
appstorm.<timestamp>.log Filled with Connection Exceptions	453
Receiving HTTP ERROR: 503 When Accessing the Management Server	454
Windows	455
Unix systems	455
Errors in the Logs	456
Permanently Changing the Port a CIM Extension Uses (UNIX Only)	457
Configuring UNIX CIM Extensions to Run Behind Firewalls	458
Volume Names from Ambiguous Automounts Are Not Displayed	461
Solaris Management Server Suddenly Restarts	462

Installing the Software Security Certificate	462
Installing the Certificate by Using Microsoft Internet Explorer 6.0	463
Changing the Security Certificate to Match the Name of the Server	464
Windows	464
Sun Solaris and Linux	465
Troubleshooting Discovery and Get Details	466
Troubleshooting Mode	467
Unable to discover Emulex host bus adapters	467
CIMOM Service Not Starting After Trying to Discover Sybase or SQL Server Applications	468
Configuring E-mail Notification for Get Details	468
Increasing the Time-out Period and Number of Retries for Switches in Progress	469
“Connection to the Database Server Failed” Error	471
Using the Test Button to Troubleshoot Discovery	471
DCOM Unable to Communicate with Computer	474
Duplicate Listings/Logs for Brocade Switches in Same Fabric	474
Duplicate listings: Targets tab	474
Duplicate Logs	474
Duplicate entries for the same element on the Get Details page	475
Element Logs Authentication Errors During Discovery	475
EMC Device Masking Database Does Not Appear in Topology (AIX Only)	476
Management Server Does Not Discover Another Management Server's Database	476
Microsoft Exchange Drive Shown as a Local Drive	476
Unable to Discover Microsoft Exchange Servers	476
Nonexistent Oracle Instance Is Displayed	476
Requirements for Discovering Oracle	477
Do Not Run Overlapping Discovery Schedules	477

"This storage system uses unsupported firmware. ManagementClassName: class_name" Message	477
Troubleshooting Topology Issues	478
About the Topology	478
Undiscovered Hosts Display as Storage Systems	481
Solaris Machines Appear to Have Extra QLogic HBAs	482
No Stitching for Brocade Switches with Firmware 3.2.0	482
Link Between a Brocade Switch and a Host Disappears from the Topology	482
Incorrect Topology Sometimes Displayed for CNT Switches	482
Unable to Find Elements on the Network	483
Device Locking Mechanism for Brocade Element Manager Query/Reconfiguration	483
A Discovered Sun StorEdge A5000 JBOD Does Not Display Its WWN Properly	483
Sun 6920 Storage Systems: "ReplicatorSQLException: Database create error" During Get Details	484
Mirrored Volumes Cannot Be Provisioned on Sun 6920 Storage Systems	484
Unable to Monitor McDATA Switches	484
Unable to Detect a Host Bus Adapter	485
Navigation Tab Displays Removed Drives as Disk Drives	485
Unable to Obtain Information from a CLARiiON Storage System	485
Discovery Fails Too Slowly for a Nonexistent IP Address	486
"CIM_ERR_FAILED" Message	487
Re-establishing Communication with EFCM	488
CIM_ERR_FAILED When Trying to Activate a Zone Set Using McDATA SWAPI	489
Communicating with HiCommand Device Manager Over SSL	489
Unable to Discover a UNIX Host Because of DNS or Routing Issues	490
ERROR replicating APPIQ_EVAStorageVolume during Get Details for an EVA array	491

Recalculating the Topology	492
Unable to View System Explorer After Upgrade	492
Troubleshooting Provisioning	492
Cannot Access a Resource Owned by Another Controller	492
Error -56	493
“Can't delete this zone” Message	493
Changes in EFC Manager Requiring Get Details	493
Troubleshooting Hardware	493
About Swapping Host Bus Adapters	494
“Fork Function Failed” Message on AIX Hosts	494
Known Driver Issues	494
Known Device Issues	494
“mailbox command 17 failure status FFF7” Message	498
“Process Has an Exclusive Lock” Message	498

Figures

FIGURE 2-1	Missing Xvfb Package Message	10
FIGURE 2-2	Setting Kernel Parameters	16
FIGURE 2-3	Oracle User Account Not Enabled Error	16
FIGURE 5-1	An Example of Direct Attached Storage	116
FIGURE 6-1	Setting Default User Names and Passwords	124
FIGURE 6-2	Adding an IP Range for Scanning	126
FIGURE 6-3	Deleting Elements from the Management Server	196
FIGURE 19-1	Selecting Import from Disk	382
FIGURE 19-2	Enabling Compile Class	383
FIGURE 19-3	Selecting appiq.cls	384
FIGURE 19-4	Importing Wrapper Class Definitions	386
FIGURE 20-1	System Explorer Cluster Representation	404
FIGURE 20-2	Cluster Element Topology Representation	406
FIGURE 20-3	Capacity Manager Cluster Representation	408
FIGURE 21-1	Parent-Child Hierarchy for Organizations	413
FIGURE 21-2	Children in Multiple Organizations	414
FIGURE 21-3	Clicking the Name of Your User Account	421
FIGURE 21-4	Clicking the Organization Link	431
FIGURE 21-5	Filtering Organizations	432
FIGURE 21-6	Active Organization	432

Tables

TABLE 1-1	Roadmap for Installation and Initial Configurations	2
TABLE 4-1	Pre-installation Requirements to Install or Upgrade	87
TABLE 5-1	License Restrictions	113
TABLE 5-2	Determining Managed Access Points	115
TABLE 6-1	Discovery Requirements for Switches	132
TABLE 6-2	Discovery Settings for McDATA and Connectrix Switches	142
TABLE 6-3	Discovery Requirements for Storage Systems, Tape Libraries & NAS Devices	156
TABLE 6-4	Discovery Group Ports	191
TABLE 6-5	Task Status Descriptions	201
TABLE 7-1	Status Icons	212
TABLE 8-1	Parameters for CIM Extensions	223
TABLE 9-1	Parameters for CIM Extensions	235
TABLE 10-1	Parameters for CIM Extensions	245
TABLE 11-1	Parameters for CIM Extensions	257
TABLE 12-1	Parameters for CIM Extensions	270
TABLE 13-1	TCP/IP Process Display Commands	281
TABLE 13-2	Port Arguments	281
TABLE 14-1	Parameters for CIM Extensions	296
TABLE 15-1	Parameters for CIM Extensions	309
TABLE 16-1	Parameters for CIM Extensions	322

TABLE 17-1	Parameters for CIM Extensions	336
TABLE 19-1	Script Names for Managed Databases	354
TABLE 21-1	Default Role Privileges	410
TABLE 21-2	Default Role Privileges by Elements	412
TABLE 22-1	Troubleshooting Firewalls	459
TABLE 22-2	Time-out Properties	470
TABLE 22-3	Retry Properties	471
TABLE 22-4	Troubleshooting Discovery and Get Details	479
TABLE 22-5	Known Device Issues	495

Revision History

Short Name	Part Number	Dash	Date	Comments
INSTALLATION GUIDE	817-7922-16	-05	January 2008	

Preface

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

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

Using UNIX Commands

This document might not contain information on basic UNIX® commands and procedures such as shutting down the system, booting the system, and configuring devices. See the following for this information:

- Software documentation that you received with your system
- Solaris™ operating environment documentation, which is at
`http://docs.sun.com`

Table with descriptions and examples of the typographic conventions that are used in this book.

Related Documentation

Application	Title	Part Number
Installation	Release Notes	-----
Operations Manager	<i>Sun StorageTek™ Operations Manager 6.0 User Guide</i>	817-7923-16
Resource Manager	<i>Sun StorageTek™ Resource Manager 6.0 Guide</i>	817-7925-16
CLI	<i>Sun StorageTek™ Operations Manager 6.0 CLI Guide</i>	817-7924-16
Application Module	<i>Sun StorageTek™ Application Module 6.0 Guide</i>	817-7926-16

Accessing Sun Documentation

You can view, print, or purchase a broad selection of Sun documentation, including localized versions, at:

<http://www.sun.com/documentation>

Contacting Sun Technical Support

If you have technical questions about this product that are not answered in this document, go to:

<http://www.sun.com/service/contacting>

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can submit your comments by going to:

<http://www.sun.com/hwdocs/feedback>

Please include the title and part number of your document with your feedback:

Sun StorageTek™ Operations Manager 6.0 Installation Guide, part number 817-7922-16

Overview

This chapter contains the following topics:

- “Supported Platforms for Installing the Management Server” on page 1
- “Roadmap for Installation and Initial Configurations” on page 1
- “About this Product” on page 3

Supported Platforms for Installing the Management Server

This chapter provides a general overview of the installation steps for the various operating systems on which the management server is supported:

- Linux
- Microsoft Windows
- Sun Solaris

Roadmap for Installation and Initial Configurations

See the following table for an outline of the installation steps and be sure to see the support matrix . The support matrix can be found on the top level of the management server CD-ROM.

TABLE 1-1 Roadmap for Installation and Initial Configurations

Step	Description	Where to Find
1	Install the management server.	<ul style="list-style-type: none"> • Sun Solaris - See “Installing the Management Server on Sun Solaris” on page 49. • Microsoft Windows - See “Installing the Management Server on Microsoft Windows” on page 85. • Linux - See “Installing the Management Server on Linux” on page 7.
2	Perform discovery for switches, NAS devices, and storage systems. This step requires the management server to be connected to the network containing the switches, NAS devices, and storage systems you want to manage.	See “Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries” on page 119.
3	<p>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.</p> <p>It is possible to install, upgrade, and manage CIM Extensions remotely across any number of hosts. See “Deploying and Managing CIM Extensions” on page 203.</p> <hr/> <p>Caution – Do not install CIM extensions on the management server.¹</p> <hr/>	<ul style="list-style-type: none"> • IBM AIX - See “Installing the CIM Extension for IBM AIX” on page 215. • SGI ProPack for Linux - See “Installing the CIM Extension for SGI ProPack for Linux” on page 227. • HP-UX - See “Installing the CIM Extension for HP-UX” on page 249. • SGI IRIX - See “Installing the CIM Extension for SGI IRIX” on page 239. • SUSE and Red Hat Linux - See “Installing the CIM Extension for SUSE and Red Hat Linux” on page 261. • HP OpenVMS (Alpha) - See “Installing the CIM Extension for OpenVMS” on page 287. • HP Tru64 UNIX - See “Installing the CIM Extension for HP Tru64 UNIX” on page 313. • Sun Solaris - See “Installing the CIM Extension for Sun Solaris” on page 301. • Microsoft Windows - See “Installing the CIM Extension for Microsoft Windows” on page 327. • NonStop - See “Installing the CIM Extension for NonStop” on page 273

TABLE 1-1 Roadmap for Installation and Initial Configurations (*Continued*)

Step	Description	Where to Find
4	The Windows Proxy is required when the management server is on Sun Solaris or Linux and you want to obtain information from Microsoft Windows hosts that do not have a CIM extension installed.	See “Installing and Discovering the Windows Proxy” on page 339.
5	Configure the applications and hosts for monitoring. This step includes discovering applications, master backup servers, and hosts.	See “Discovering Applications, Backup Hosts and Hosts” on page 345.
6	Change the password of the admin account for the management server and system accounts.	See “Changing Your Password” on page 420 and “Changing the Password of System Accounts” on page 432.
7	Add users.	See “Adding Users” on page 416.

¹If you install CIM extensions on the management server, the Database Admin Utility returns the following error and does not run correctly:
`[isAppIQCIMOMAlive] - false`

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 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.

Web Browser Configuration Requirements

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

- cookies
- JavaScript
- Java

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

Installing the Management Server on Linux

See the following topics if you are installing the management server on another supported operating system:

- “Installing the Management Server on Microsoft Windows” on page 85
- “Installing the Management Server on Sun Solaris” on page 49

This part of the chapter describes installing the management server on Linux. If you are upgrading your management server software, please refer to the upgrade information and steps described later in this chapter, beginning with “Upgrading the Linux Management Server from v5.1 to v6.0” on page 37.

Keep in mind the following:

- **All steps must be completed for the management server to work properly.**
- Linux management server is supported only on the following versions:
 - Redhat 4 (U3 or higher)
 - SUSE 9 (SP3)
 - SUSE 10 or SUSE 10 SP1
- Refer to the product Support Matrix regarding other related software and version requirements.
- For optimal performance, install the management server on a dedicated computer. See the support matrix for hardware requirements.
- Installation through Virtual Network Computing (VNC) software is not supported.
- During management server installation, double-byte characters are not allowed in the installation path. InstallScript.iap_xml has been modified to display the following message if double-byte characters are entered:
`The installation path for $PRODUCT_NAME$ may NOT contain double-byte characters.`
`The installation path must be basic ASCII alphanumeric characters, no spaces, no international characters, and no double-byte characters.`
`Please choose a different installation directory.`

This chapter describes the following installation topics and steps:

- “Pre-installation Checklist” on page 8
- “Installing from a Network Drive” on page 12
- “Step 1 - Install the Oracle Database” on page 12
- “Step 2 - Install the Management Server” on page 25
- “Step 3 - Verify that Processes Can Start” on page 28
- “Step 4 - Configure Firefox” on page 31
- “Installing the Java Plug-in on Linux” on page 32
- “Configurations Required for Discovering EMC CLARiiON Storage Systems” on page 34
- “Removing the Management Server” on page 34
- “Upgrading the Linux Management Server from v5.1 to v6.0” on page 37

Pre-installation Checklist

Pre-requisite RPMs for Oracle on Linux

Verify that your system includes the required packages by using the following command:

```
# rpm -q <package-name>
```

Required RPMs for Oracle 10g on RHEL systems:

- binutils-2.15.92.0.2-10.EL4
- compat-db-4.1.25-9
- control-center-2.8.0-12
- gcc-3.4.3-9.EL4
- gcc-c++-3.4.3-9.EL4
- glibc-2.3.4-2
- glibc-common-2.3.4-2
- gnome-libs-1.4.1.2.90-44.1
- libstdc++-3.4.3-9.EL4
- libstdc++-devel-3.4.3-9.EL4
- make-3.80-5
- xscreensaver-4.18-5.rhel4.2

Required RPMs for Oracle 10g on SUSE 9 systems:

- binutils-2.15.90.0.1.1-32.5
- gcc-3.3.3-43.24
- gcc-c++-3.3.3-43.24
- glibc-2.3.3-98.28
- gnome-libs-1.4.1.7-671.1

- libstdc++-3.3.3-43.24
- libstdc++-devel-3.3.3-43.24
- make-3.80-184.1
- xscreensaver-4.16-2.6
- orarun-1.8-109.15
- sysstat-5.0.1

Required RPMs for Oracle 10g on SUSE 10

- binutils
- glibc-2.4
- gcc-4.1.0
- gcc-c++-4.1.0
- libaio
- libaio-devel
- libstdc++
- make-3.80
- openmotif-libs
- sysstat-6.0.2
- orarun-1.9-21

The preceding information is taken from

http://www.novell.com/products/server/oracle/oracle10g_install.html. RPMs for SLES 9 can be found at

<http://www.novell.com/products/server/oracle/software.html> and RPMs for SLES 10 can be found in the SLES 10 product CD.

Note – The **orarun-1.9** package is available from <http://ftp.novell.com/partners/oracle/sles-10/orarun-1.9-21.15.i586.rpm>.

The list of packages described above for RHEL and SUSE includes all the packages needed for Oracle installation. Some of these packages might be selectively installed depending on the mode of installation followed during OS installation.

Software Dependencies

Note – The database configuration and creation script is different for Oracle 10g than it was for Oracle 9i. As a result, the management server software Build 6.0 is not supported by Oracle 9i. Management server software builds earlier than 6.0 are not supported on the Oracle 10g platform.

Verify that the following required software is available on your system, and install any that are missing:

- Perl 5.8.3 or above. By default, the OS installs Perl 5.8.3 on SUSE 9 and Perl 5.8.5 on RHEL 4.
- 'Xvfb' is required for Application Explorer and Reporter. The Application Explorer and Reporter pages show a 'java.lang.NoClassDefFoundError' if 'Xvfb' is not installed. This package comes with the OS distribution (for both RHEL & SLES) and is installed if Full OS Install is selected.
 - For RHEL, the package name is "xorg-x11-Xvfb"
 - For SLES 9, the package name is "XFree86-Xvfb"
 - For SLES 10, the package name is "xorg-x11-Xvfb"

For RHEL 4 or SUSE 10, if the "xorg-X11-Xvfb" package is not installed, the management server installer displays a message that the "Xvfb" package is not installed, and stops the install process. User needs to install the package named "xorg-X11-Xvfb" and then must re-run the management server installation. This package is available on RHEL 4 OS CD's and SUSE 10 CDs.

For SUSE 9, if the "XFree86-Xvfb" package is not installed, the management server installer displays a message that the "Xvfb" package not installed, and stops the install process. User needs to install the package named "XFree86-Xvfb" and then must re-run the management server installation. This package is available on the SUSE 9 CD's.

The following shows a representative example of the error message that would display.



FIGURE 2-1 Missing Xvfb Package Message

Verify Network Settings

Verify the network configuration for the management server:

1. Verify that the appropriate DNS server entries are present in `/etc/resolv.conf`. Verify that the correct DNS suffixes are mentioned in the order of preference in which they need to be appended to hostnames.

For example:

```
nameserver 172.168.10.1
nameserver 172.168.10.2
search "yourenvironment".com
```

2. From a console window on the management server, enter the following command:

```
ping <hostname>
```

where <hostname> is the hostname (without domain name) of the Linux CMS.

The 'ping' command must ping the IP address of the management server. It must not ping the loopback address (127.0.0.1). If it pings the loopback address, edit the `/etc/hosts` file to make appropriate corrections.

The `/etc/hosts` file should have entries similar to:

```
127.0.0.1      localhost.localdomain localhost
192.168.0.100 myservername.mydomain.com myservername
```

Note – If the ping command fails to ping the IP address and instead pings the loopback address, the oracle listener process will fail to start and therefore, the CIMOM process will also fail.

3. Enter the following command:

```
nslookup <hostname>
```

where <hostname> is the hostname (without domain name) of the management server.

4. Enter the following command:

```
nslookup <IP address>
```

where <IP address> is the IP address of the server.

5. Verify that both results from nslookup have the same fully qualified computer name and IP address.

Installing from a Network Drive

Support for installing (or upgrading) from a network drive is limited to NFS mounted network drives only. After the network drive is mounted to the local server, there are no separate network drive-related steps required for the installation (or upgrade).

- Create a directory on which the NFS drive will be mounted:

```
#mkdir /InstallSE
```

- Mount the NFS shared network drive from NFS server (example: "pillbox") with shared drive "InstallSE", with strong recommendation to set it as read only.

```
#mount pillbox:/InstallSE /InstallSE
```

- Any database ISO files must be loop-mounted and it is strongly recommended to set them to read only mode. Management CD ISO files can be mounted in the same way as shown in the following representative example for the Oracle database. (Names such as Disk1 or Vol1 can be user-configurable, created by user with "mkdir".) The steps need to be repeated for any other ISO user trying to mount from NFS mount (Database, management server, CIM extension)

Example:

```
#mkdir /Disk1
```

```
#mount -o loop,ro /InstallSE/database/linux/<oracle10g.iso>  
/Disk1
```

In this example, to install the Oracle database:

```
#/Disk1/InstallDatabase
```

Step 1 - Install the Oracle Database

The management server uses a database to store the data it collects from the hardware it monitors. The management server ships with a DVD that includes Oracle 10g Release 2, 10.2.0.1, upgrade to Oracle 10g Release 2, 10.2.0.3, and the October 2007 Critical Patch Update for Oracle 10g Release 2.

The install for Oracle 10g Release 2, 10.2.0.1, will also install the upgrade to Oracle 10g Release 2, 10.2.0.3, and apply the October 2007 Critical Patch Update.

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 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 management server will not run correctly.
- Install the database on the computer on which you plan to install the management server.
- Before you install Oracle, ensure the Linux server has the packages installed that are required by Oracle.
- For both Linux SUSE and RHEL, Oracle 10.2.0.1.0 (32 bit) Standard Edition software is used.
 - For the management server Build 6.0 software, the Oracle install runs in silent mode. (Oracle installs silently showing progress indication in the console through text messages.) This process does not require X-server and DISPLAY settings.
- When you install the database on Linux, files with group-writeable permissions are installed in the ORA_HOME directory.

Prerequisites

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

- Verify that the server is running sh, ksh or bash shell.
- Verify the following directories have write permissions:

/

/tmp

Parent directory of ORA_HOME

- If you are running Red Hat Enterprise Linux AS 4 or Red Hat Enterprise Linux ES 4, delete the existing Oracle user if present, before proceeding with the installation. The installation will fail if there is an existing Oracle user.
- On SUSE Linux systems, on installing the 'oracrun' rpm, the Oracle user account gets created automatically. However the oracle user account needs to be enabled by changing the shell entry from '/bin/false' to '/bin/bash' for oracle user in the /etc/passwd file.
- Setting of the kernel parameters for Oracle on both Red Hat and SUSE systems is handled by the Oracle installer script and the user need not set the kernel parameters.
- At least 400 MB of free space is required in the /tmp directory.
- ORA_HOME should have a minimum of 50 GB of free space.

Note – If the Oracle installation fails, a re-install will not run successfully because of existing files or existing Oracle user. In such a case, uninstall Oracle using the Oracle uninstall script. Refer to step 6 of “Removing the Management Server” on page 34.

Installing the Database

To install the database:

1. Login to the Linux host as root user.
2. Insert the first Oracle Database DVD and mount it using the following commands:

```
# mkdir -p /mnt/oradisk
# mount /dev/cdrom /mnt/oradisk
    where /dev/cdrom is the device.
```

3. Verify that you are in the top level directory:

```
# cd /
```

4. Start the installation of the database by entering the following:

```
# /mnt/oradisk/InstallDatabase
```

Note – All commands and filenames are case-sensitive.

5. The script will ask if you wish to continue. Enter “y.”
6. The oracle installer script checks for required RPMs and terminates if any required RPM is missing. In such case, install the missing RPMs and restart the installation.

```
INFO: Checking for required packages...
```

```
ERROR: sysstat is not installed.
```

```
ERROR: Please install missing pre-requisite packages
        before proceeding with installation.
```

```
Terminating installation.
```

If the installer finds a different version of a pre-requisite RPM, it will prompt the user to confirm continuing the installation.

```
INFO: Checking for required packages...
```

```
WARN: Looking for package gcc-4.1.0. Found gcc-4.1.2_20070115-0.11.
```

```
WARN: Looking for package gcc-c++-4.1.0. Found gcc-c++-4.1.2_20070115-0.11.
```

```
WARN: Version mismatch in pre-requisite packages.
```

```
Oracle may not work with these versions.
```

```
Do you want to continue? [y/n]:
```

```
y
```

```
INFO: Verified pre-requisite packages.
```

```
INFO: Proceeding with installation...
```

7. If there is insufficient swap space, the script displays a message saying that the swap space is insufficient and a message similar to the following displays:

```
INFO: Checking swap space...
```

```
INFO: Available RAM: 4082752
```

```
INFO: Recommended Swap size: 4082752
```

```
INFO: Current Swap: 2097144
```

```
INFO: Insufficient swap size.
```

```
INFO: Creating additional swap space: 1985608
```

```
1985608+0 records in
```

```
1985608+0 records out
```

```
mke2fs 1.38 (30-Jun-2005)
```

```
/tmp/swapForOracle1.tmp is not a block special device.
```

```
Proceed anyway? (y,n)
```

Enter 'y' at the prompt.

You may be prompted to create multiple swap files. Enter 'y' each time you encounter the prompt described above.

8. The temporary disk space in /tmp is checked. If the disk space in /tmp is less than 400 MB, the installation will abort with the below message.

ERROR: You need at least 400MB in the /tmp directory.
You only have 100 MB.

Terminating installation.

9. Appropriate kernel parameters are automatically set by the installation script.

```
Setting kernel parameters for Oracle, see file
/etc/sysconfig/oracle for explanations.
Shared memory:      SHMMAX=3294967296 SHMMNI=4096 SHMALL=2097152
Semaphore values:   SEMMSL=1250 SEMMNS=32000 SEMOPM=100 SEMMNI=256
Other values:       FILE_MAX_KERNEL=131072 IP_LOCAL_PORT_RANGE=1024 65000
                   RMEM_DEFAULT=262144 WMEM_DEFAULT=262144 RMEM_MAX=262144 WMEM_MAX=262144
Huge Pages:         SHM_GROUP=dba NR_HUGE_PAGES=0
ULIMIT values:      MAX_CORE_FILE_SIZE_SHELL=unlimited
                   FILE_MAX_SHELL=65536 PROCESSES_MAX_SHELL=16384

Kernel parameters set for Oracle: ..done
```

FIGURE 2-2 Setting Kernel Parameters

10. On SUSE systems, the oracle user account should be enabled prior to starting the installation. If the oracle user is not enabled, an error message is shown as below.

```
ERROR: The oracle user account is not enabled.
Please edit the /etc/passwd file and change the shell entry from
'/bin/false' to '/bin/bash' for the oracle user.
Terminating installation.
```

FIGURE 2-3 Oracle User Account Not Enabled Error

On Red Hat systems, if an oracle user is already existing, an error message is shown indicating that this oracle user needs to be deleted. The following shows the error message.

ERROR: This script has detected an existing Oracle user account on this
system.

This script requires that no Oracle user account be present prior to the installation.

Please contact your System Administrator to resolve this conflict.

11. When prompted, enter the Oracle home directory. The default location for SUSE 9 and SUSE 10 is /opt/oracle, and for RHEL 4 is /home/oracle.
12. When prompted, enter the Oracle installation directory. The default location is opt/oracle.

```
Please enter the Oracle user's home directory. [Default:
/home/oracle]
```

```
Please enter Oracle installation directory [Default: /opt/oracle]
```

```
INFO: Created Oracle users home directory.
```

13. If you are running Red Hat Enterprise Linux AS 4 or RHEL 4.0, you will be asked to enter the password for oracle user. Enter the password when prompted.
14. Enter “y” when asked to start the Oracle Universal Installer. For RHEL 4.0, text similar to the following console output may display. (Representative console output for SUSE 10 and SUSE 10 SP1 is also included at the end of this example following the “Note” information.)

```
Starting Oracle Installer...
```

```
Starting Oracle Universal Installer...
```

```
Checking installer requirements...
```

```
Checking operating system version: must be redhat-3, SuSE-9, redhat-
4, UnitedLinux-1.0, asianux-1 or asianux-2
```

```
Passed
```

```
All installer requirements met.
```

```
Preparing to launch Oracle Universal Installer from
/tmp/OraInstall2007-10-24_05-33-55PM. Please wait ...Oracle
Universal Installer, Version 10.2.0.1.0 Production
```

```
Copyright (C) 1999, 2005, Oracle. All rights reserved.
```

```
Font specified in font.properties not found
```

```
[--symbol-medium-r-normal---%d-*-*p-*-*adobe-fontspecific]
```

```
Font specified in font.properties not found
```

```
[--symbol-medium-r-normal---%d-*-*p-*-*adobe-fontspecific]
```

```
Font specified in font.properties not found
[--symbol-medium-r-normal--*-%d-*-*p-*-*adobe-fontspecific]
```

```
Warning: Cannot convert string "<Key>Escape,_Key_Cancel" to type
VirtualBinding
```

```
Warning: Cannot convert string "<Key>Home,_Key_Begin" to type
VirtualBinding
```

```
Warning: Cannot convert string "<Key>Help,_Key_F1" to type
VirtualBinding
```

Note – The warning messages in the above console output can safely be ignored.

Note – The Oracle Installer that comes with the Oracle Database Server Patch 10.2.0.1 does not officially support SUSE 10; however, the Oracle database is supported on SUSE 10. The resulting error messages can be safely ignored. Also, “Failed” and “Not Executed” check complete messages in the pre-requisites result can be safely ignored.

For SUSE 10 and SUSE 10 SP1, text similar to the following displays:

```
INFO: The next step is to start the Oracle Universal Installer.
```

```
Start the Oracle Universal Installer ? [y/n]:
```

```
y
```

```
Starting Oracle Installer...
```

```
Starting Oracle Universal Installer...
```

```
Checking installer requirements...
```

```
Checking operating system version: must be redhat-3, SuSE-9, redhat-
4, UnitedLinux-1.0, asianux-1 or asianux-2
```

```
Failed <<<<
```

```
>>> Ignoring required pre-requisite failures. Continuing...
```

Preparing to launch Oracle Universal Installer from
/tmp/OraInstall2007-09-29_07-40-00PM. Please wait ...Oracle
Universal Installer, Version 10.2.0.1.0 Production Copyright (C)
1999, 2005, Oracle. All rights reserved.

You can find a log of this install session at:

/opt/oracle/oraInventory/logs/installActions2007-09-29_07-40-
00PM.log

Starting execution of Prerequisites...

Total No of checks: 11

Performing check for CertifiedVersions

Checking operating system requirements ...

Expected result: One of redhat-3,redhat-4,SuSE-9,asianux-1,asianux-2

Actual Result: SuSE-SUSE Linux Enterprise Server 10 (i586)

Check complete. The overall result of this check is: Failed <<<<

Check complete: Failed <<<<

Problem: Oracle Database 10g is not certified on the current operating
system.

Recommendation: Make sure you are installing the software on the
correct platform.

=====
=====

Performing check for Packages

Checking operating system package requirements ...

Check complete. The overall result of this check is: Not executed <<<<

Check complete: Not executed <<<<

OUI-18001: The operating system 'Linux Version SuSE-SUSE Linux
Enterprise Server 10 (i586)' is not supported.

Recommendation: Install the required packages before continuing with
the installation.

.....
..... 100% Done.

15. Once the installer begins installing Oracle 10g, it cannot be paused or cancelled. The only way to re-install Oracle is to uninstall it and start all over again.
16. Once Oracle 10g is installed successfully, the script automatically executes root.sh from \$ORACLE_HOME where \$ORACLE_HOME is usually /opt/oracle/product/10.2.0.1.

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

```
Oracle Database 10g Installation : OK
-----
---
INFO: Running root.sh...
-----
---Running Oracle10 root.sh script...

The following environment variables are set as:
    ORACLE_OWNER= oracle
    ORACLE_HOME=  /opt/oracle/product/10.2.0.1

Enter the full pathname of the local bin directory: [/usr/local/bin]:
Copying dbhome to /usr/local/bin ...
Copying oraenv to /usr/local/bin ...
Copying coraenv to /usr/local/bin ...

Creating /etc/oratab file...
Entries will be added to the /etc/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.
-----
---OK.

The upgrade to Oracle 10g 10.2.0.3 starts after Oracle 10g 10.2.0.1
completes installation.
-----
-----
```



```

This script installs Oracle Database 10g Release Patch Set 2
-----
-----
INFO : Checking the OS Release...

After upgrading to Oracle 10.2.0.3, the installer will execute root.sh from
$ORACLE_HOME. The user does not have to open a new terminal window and run
the script as mentioned in the following representative example.

The following configuration scripts need to be executed as the "root"
user.
/opt/oracle/product/10.2.0.1/root.sh
To execute the configuration scripts:
    1. Open a terminal window
    2. Log in as "root"
    3. Run the scripts

The installation of Oracle Database 10g Release 2 Patch Set 2 was
successful.

Please check '/opt/oracle/oraInventory/logs/silentInstall2007-10-
24_05-41-14PM.log' for more details.

Running Oracle10 root.sh script...

The following environment variables are set as:
    ORACLE_OWNER= oracle
    ORACLE_HOME=  /opt/oracle/product/10.2.0.1

Enter the full pathname of the local bin directory: [/usr/local/bin]:
The file "dbhome" already exists in /usr/local/bin.  Overwrite it?
(y/n)

```

Note – There is no need to overwrite these files as they would not have changed.

Oracle Critical Patch Update

The critical patch update is applied automatically after the installer completes upgrading to Oracle 10.2.0.3. If Oracle 10.2.0.3 upgrade fails, then the critical patch update will exit with a failure.

The installation is done in silent mode and output similar to the following displays when the installation begins:

```
INFO : Checking the OS Release...
Found SUSE LINUX Enterprise Server 9.
Installing Oracle 10g Release 2 Critical Patch Update, October 2007...
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121183
      Patch 6121183 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121242
      Patch 6121242 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121243
      Patch 6121243 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121244
      Patch 6121244 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121245
      Patch 6121245 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121246
      Patch 6121246 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121247
      Patch 6121247 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121248
      Patch 6121248 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121249
      Patch 6121249 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121250
      Patch 6121250 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121257
      Patch 6121257 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121258
      Patch 6121258 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121260
      Patch 6121260 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121261
      Patch 6121261 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121263
      Patch 6121263 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121264
```

Patch 6121264 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121266
Patch 6121266 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121268
Patch 6121268 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6394981
Patch 6394981 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397928
Patch 6397928 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397929
Patch 6397929 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397937
Patch 6397937 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397938
Patch 6397938 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397939
Patch 6397939 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397940
Patch 6397940 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397941
Patch 6397941 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397942
Patch 6397942 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397943
Patch 6397943 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397944
Patch 6397944 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397945
Patch 6397945 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397946
Patch 6397946 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397947
Patch 6397947 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397948
Patch 6397948 installed successfully.

Oracle 10g Release 2, Critical Patch Update, October 2007 is installed.

--

All logs created while applying October 2007 CPU are located under /tmp/6394981, names being 7-digit patch numbers.

Note – InstallDatabase script will not allow Oracle 10g to re-install if the previous installation was terminated before completing. If Oracle 10g has to be re-installed, clear all LOG files under /tmp/6394981 and re-install. Failing to do so may prevent the script from creating new LOG files at the same location.

Accessing the Linux Host

Access the Linux host by doing one of the following:

- **Using the graphics console on the localhost** - Run the following command at the command prompt:

```
# /usr/X11R6/bin/xhost +
```

- **Accessing the Linux host from a remote Linux client**

1. Ensure that the X server on the remote client can accept TCP connections:

a. Open /etc/X11/xdm/Xservers

b. Verify that the line for the screen number 0 (the line containing :0 local) does not contain the -nolisten tcp option. Remove the -nolisten tcp option if present. The line should look like:

```
:0 local /usr/X11R6/bin/X
```

c. Enable TCP connections on the X server of the remote client:

SUSE - Edit /etc/sysconfig/displaymanager and set the following options to yes: DISPLAYMANAGER_REMOTE_ACCESS and DISPLAYMANAGER_XSERVER_TCP_PORT_6000_OPEN.

For example: DISPLAYMANAGER_REMOTE_ACCESS="yes"

```
DISPLAYMANAGER_XSERVER_TCP_PORT_6000_OPEN="yes"
```

RHEL (for gnome) - Edit /etc/X11/gdm/gdm.conf and set the DisallowTCP option to false (uncomment if commented)

For example: DisallowTCP=false

- d. If you made any changes in the configuration files during the previous steps, reboot the system for the changes to take effect.
2. Run the following command at the command prompt:
- ```
/usr/X11R6/bin/xhost +
```
- Then, set the display to your client. Refer to the documentation for your shell for more information.
- **Accessing the Linux host from a remote Windows client** - Start up a local X server, connect through xterm to the remote system and set your DISPLAY environment variable appropriately by using the following commands:
- ```
# DISPLAY=<ip-address>:displaynumber.screennumber
```
- where <ip-address> is the address of the client from which the Installer script is launched.
- ```
export DISPLAY
```
- For Example:
- ```
# DISPLAY=172.168.10.15:0.0
```
- ```
export DISPLAY
```
- 

## Step 2 - Install the Management Server

If you are installing the management server from a network drive, follow the instructions as described in “Installing from a Network Drive” on page 12.

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.
- In this release, no RPM entry is created for management server on Linux.
- When you install the management server on Linux, 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 Linux, the following files from InstallAnywhere are left with writable permissions, and they should not be modified. Modifying them may impact other installations that use InstallAnywhere:
  - `$mgr_dist/Uninstall_<product_name>/com.zerog.registry.xml`
    - where `$mgr_dist` is the location where the management server is installed
  - `/var/com.zerog.registry.xml`
- Verify that the required software is available on your system as described in “Software Dependencies” on page 9.

Management server installation on Linux requires a non-loopback IP address to start the Management Server (appstormmanager service). Linux requires the Fully Qualified Domain Name and the IP address on separate lines on `/etc/hosts` for the management server to start. This is the OS default.)

The following is an example of the acceptable format:

```
cat /etc/hosts
127.0.0.1 localhost.localdomain localhost
15.115.235.13 meet.lab.usa.co.com meet
```

The following format is unacceptable:

```
cat /etc/hosts
meet.lab.usa.co.com.meet
localhost.localdomain.localhost
```

SLES10 may have an entry for 127.0.0.2 in `/etc/hosts` against the host name for that system. Comment out or remove the line that maps the IP address 127.0.0.2 to the systems fully qualified hostname. Retain only that line that contains the actual IP address mapped to the fully qualified host name.

Example:

```
cat /etc/hosts
#
127.0.0.1 localhost
127.0.0.2 demo.novell.com demo
192.168.1.5 demo.novell.com demo
```

In the example shown above, remove or comment the line in bold as shown in the middle line.

To install the management server:

1. Access the Linux host as described in “Accessing the Linux Host” on page 24.

**2. If installing from CD-ROM:**

Insert the CD-ROM for installing the management server in the CD-ROM drive of the server and mount it by using the following commands:

```
mkdir -p /mnt/installer
mount /dev/cdrom /mnt/installer
where /dev/cdrom is the CD device.
```

If installing from network NFS mount:

Create /mnt/installer directory on the server where the NFS drive (for example, /installSE) is mounted and where management server will be installed:

Then, create a directory on which the NFS drive will be mounted:

```
#mkdir /InstallSE
```

Mount the NFS shared network drive from NFS server (example: "pillbox") with shared drive "InstallSE", with strong recommendation to set it as read only.

```
#mount pillbox:/InstallSE /InstallSE
#mkdir /mnt/installer
```

Loop mount the ManagerCDLinux.iso to the /mnt/installer directory.

```
#mount -o loop,ro /InstallSE/ManagerCDLinux.iso
/mnt/installer
```

For more information about installing from a network drive, see "Installing from a Network Drive" on page 12 in this chapter.

3. Enter the following at the command prompt (if you mounted the CD device at the /mnt/installer location)

```
/mnt/installer/InstallManager.bin
```

4. When you see the introduction screen, Select **Next**.
5. When you are asked for an installation directory, you can select the default or choose your own. To choose your own directory, select the **Choose** button. You can always display the default directory by selecting the **Restore Default Folder** button. When you are done, select **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:
  - Select **Install** if you agree with the pre-installation summary.
  - Select **Previous** if you want to modify your selections.

The management server is installed.

---

**Caution** – Do not select 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. Enter the following at the command prompt:

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

---

**Caution** – You will have to set the new Oracle 10g database to ARCHIVE MODE in order to enable automatic RMAN backups. See the User Guide in the Documentation Center (Help > Documentation Center) for steps.

---

## 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 Oracle and the management server have started.

1. To verify the Oracle processes have started, enter the following at the command prompt:

```
/etc/init.d/dbora status
```

Output resembling the following is displayed:

```
#####
#####
Begin of O R A C L E status section
#####
#####
```

Kernel Parameters

```
Shared memory: SHMMAX= 3294967296 SHMMNI= 4096 SHMALL= 2097152
```



Semaphore values: SEMMSL, SEMMNS, SEMOPM, SEMMNI: 1250 32000 100 256

Database-Instances

Instance \* is down \ (autostart: N\)

Instance APPIQ is up \ (autostart: Y\)

TNS-Listener: up

Process list for user oracle:

| PID   | TTY | STAT | TIME | COMMAND                                                       |
|-------|-----|------|------|---------------------------------------------------------------|
| 17158 | ?   | Ss   | 0:00 | ora_pmon_APPIQ                                                |
| 17176 | ?   | Ss   | 0:00 | ora_psp0_APPIQ                                                |
| 17187 | ?   | Ss   | 0:00 | ora_mman_APPIQ                                                |
| 17200 | ?   | Ss   | 0:00 | ora_dbw0_APPIQ                                                |
| 17209 | ?   | Ss   | 0:00 | ora_dbwl_APPIQ                                                |
| 17212 | ?   | Ss   | 0:02 | ora_lgwr_APPIQ                                                |
| 17214 | ?   | Ss   | 0:00 | ora_ckpt_APPIQ                                                |
| 17216 | ?   | Ss   | 0:00 | ora_smon_APPIQ                                                |
| 17218 | ?   | Ss   | 0:00 | ora_reco_APPIQ                                                |
| 17220 | ?   | Ss   | 0:00 | ora_cjq0_APPIQ                                                |
| 17222 | ?   | Ss   | 0:00 | ora_mmon_APPIQ                                                |
| 17224 | ?   | Ss   | 0:00 | ora_mmln_APPIQ                                                |
| 17230 | ?   | Ss   | 0:00 | ora_qmnc_APPIQ                                                |
| 17281 | ?   | Ss   | 0:00 | ora_q000_APPIQ                                                |
| 17584 | ?   | Ss   | 0:00 | ora_q001_APPIQ                                                |
| 4655  | ?   | Sel  | 0:00 | /opt/oracle/product/10.2.0.1/bin/tnslsnr<br>listener -inherit |

#####  
#####  
# End of O R A C L E section #  
#####  
#####

2. If you find your processes for Oracle have not started, you can start 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
```

---

**Caution** – If you are starting the processes manually, start the Oracle process before the process for the management server.

---

3. To verify that the required processes for the management server have started, enter the following at the command prompt:

```
/etc/init.d/appstormanager status
```

The following is displayed if the processes have started:

```
Checking for Cimom Service...
```

```
Cimom Service - RUNNING.
```

```
Checking for appstormanager service...
```

```
appstormanager service - RUNNING.
```

4. If you find your processes for the management server have 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
```

5. The appstormanager service is available with the following options:

```
/etc/init.d/appstormanager
```

```
Usage: /etc/init.d/appstormanager { start | stop | restart |
status | force-reload }
```

6. If the status indicates that the CIMOM service is not running, then one of the following is true:

- The CIMOM service has not yet started. It usually takes some time for the CIMOM process to start.
- The TNS listener process is not running. This happens when the hostname is wrongly mapped to the loopback address (127.0.0.1) in the `/etc/hosts` file. Verify that `ping <hostname>` pings the IP address for the host and not the loopback address. If it pings the loopback address, edit the `/etc/hosts` file and make the appropriate corrections. After verifying that the correct IP address is being pinged, follow steps mentioned in the following bullet to remove the management server and the Oracle database.

- The APPIQ database was not created successfully, and the management server needs to be re-installed. If this is the case, uninstall the management server as described in steps 1 through 5 of “Removing the Management Server” on page 34. Then remove the APPIQ database by doing the following:
    1. As root user, stop the Oracle services by executing the following  
`/etc/init.d/dbora stop`
    2. Login as oracle user  
`su - oracle`
    3. As oracle user, execute the following command to delete the APPIQ database-  
`dbca -silent -deleteDatabase -sourceDB APPIQ`
    4. Check to see if the file `/etc/oratab` has an entry that looks like  
`APPIQ:/opt/oracle/product/10.2.0.1:Y`  
If it does, then as the root user, delete the line and save the file.
    5. If they exist, as root user, delete the APPIQ directories under  
`/opt/oracle/product/`  
`10.2.0.1/oradata` and `/opt/oracle/product/10.2.0.1/admin`:  
`rm -rf /opt/oracle/product/10.2.0.1/oradata/APPIQ`  
`rm -rf /opt/oracle/product/10.2.0.1/admin/APPIQ`
- Do not remove the Oracle Software. Install the management server as described in “Step 2 - Install the Management Server” on page 25.

---

## Step 4 - Configure Firefox

Firefox should be properly configured before accessing the management server from a Linux client.

The RHEL 4 OS distribution comes with Firefox. RHEL 4 (U3) includes Firefox version v1.0.7 which is not supported. RHEL 4 (U4) includes the supported Firefox version v1.5.0.3.

The SUSE OS distribution does not come with Firefox.

To install and configure Firefox v1.5.0.1 or later on Linux:

1. Download Firefox from <http://www.mozilla.com/firefox/all.html>
2. Extract the depot in a suitable location such as `/usr/sbin`
3. Run the following commands:  
`# cd <USER_HOME_DIR>/.mozilla/plugins`

```
ln -s /opt/<product_name>/jre/plugin/i386/ns7
/libjavaplugin_oji.so .
```

---

**Note** – Remember the dot at the end of the command.

---

4. Go to the `/usr/sbin/firefox` directory. Set the `DISPLAY` appropriately and open an X-server on your client.
5. Launch Firefox by entering the following command:  

```
/usr/sbin/firefox/firefox
```
6. Open Firefox Preferences by selecting **Edit > Preferences**.
7. Select **Connection Settings** and set the **Manual proxy configuration** appropriately. Select the **Use this proxy server for all protocols** checkbox.
8. Select the **Content** tab and disable the pop-up blocker.
9. Click **Security > Licenses** in the upper-right corner.
10. Select the tools and enter the number of MAPs, MALs, instances, and terabytes you are licensed to use.

---

**Caution** – Contact customer support if you are uncertain of which products you purchased and for how many MAPs, instances, and terabytes.

---

11. Click the **Save Changes** button to certify that you are authorized to use the components selected.
12. When you are shown the license agreement, accept the license if you agree with its terms.  
Your changes take effect.

---

# Installing the Java Plug-in on Linux

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 Linux, 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>/servlet.html?page=JavaPluginLinux
```

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/i386/ns7/libjavaplugin_oji.so
```

where \$JRE\_HOME is the directory containing the JRE installation.

3. Set the executable permission of the downloaded file:

```
chmod +x downloaded_file_name
```

4. In a terminal window, go to the \$HOME/.mozilla/plugins directory. Create a plugins directory if it does not exist.

5. Remove any existing links to the Java plug-in that are in this directory. You may use the

```
rm libjavaplugin_oji.so
```

command in a terminal window to remove an existing symbolic link to the Java plug-in.

6. Create a symbolic link to the Java plug-in by using the following command:

```
ln -s $JRE_HOME/plugin/i386/ns7/libjavaplugin_oji.so .
```

---

**Note** – Remember the dot at the end of the command.

---

---

**Note** – If you create this symbolic link in any directory other than \$HOME/.mozilla/plugins, your browser will not be able to use this new Java plug-in.

---

7. 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 to the Java plug-in that is in the `plugins` directory under the browser's installation directory.

---

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

---

8. 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.

In Navisphere add the following to the privilege user section:

```
root@name_of_my_management_server
```

```
root@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

The management server service needs to be restarted after installing EMC Navisphere CLI.

---

## Removing the Management Server

To remove the management server from Linux:

1. Access the Linux host and login as user “root” as described in “Accessing the Linux Host” on page 24.
2. To uninstall the management server, enter the following at the command prompt:  

```
<install_loc/productname>/Uninstall_<productname>
/Uninstall_<productname>
```

where <install\_loc/productname> is the directory containing the software, the default value being /opt/<product\_name>
3. 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 <install_loc>
```

where <install\_loc> is the directory containing the software, the default value being /opt/<product\_name>
4. 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/
```

Remove the file /var/.com.zerog.registry.xml
5. If you are going to reinstall a new build of the management server, make sure you keep the file /var/opt/oracle/orahome. This file lets you install a new build of the management server by assuming you kept the same Oracle installation.
6. To remove the Oracle instance containing the data for the management server, mount the Oracle DVD as described in the steps for installing Oracle.
  - a. Execute /mnt/oradisk/UninstallDatabase to delete the management database and uninstall Oracle 10g completely. After the database is deleted, the Oracle 10g instance is removed. Console output similar to the following displays and you will see a message similar to that shown: “Removing <management server> database...”.

```
INFO : Checking the OS Release...
Found SUSE LINUX Enterprise Server 9.
INFO: Checking System architecture...
OK.
This script uninstalls Oracle 10.2.0.1
#####
Begin of O R A C L E shutdown section
#####
Shutting down Oracle services (only those running)
```

```

#####
End of O R A C L E section
#####

Removing the database...

Uninstalling Oracle ...

Starting Oracle Universal Installer...

Checking installer requirements...

Checking operating system version: must be redhat-3, SuSE-9, redhat-
4, UnitedLinux-1.0, asianux-1 or asianux-2

 Passed

All installer requirements met.

Checking Temp space: must be greater than 80 MB. Actual 42712 MB
Passed

Checking swap space: must be greater than 150 MB. Actual 8195 MB
Passed

Preparing to launch Oracle Universal Installer from
/tmp/OraInstall2007-10-25_05-23-36PM. Please wait ...Oracle
Universal Installer, Version 10.2.0.1.0 Production

Copyright (C) 1999, 2005, Oracle. All rights reserved.

Starting deinstall

Deinstall in progress (Thu Oct 25 17:23:43 IST 2007)

Configuration assistant "Oracle Database Configuration Assistant"
succeeded

Configuration assistant "Oracle Net Configuration Assistant -
Deinstall Script" failed

..... 35% Done.
..... 70% Done.
..... 100% Done.

Deinstall successful

End of install phases.(Thu Oct 25 17:24:41 IST 2007)

End of deinstallations

Please check '/opt/oracle/oraInventory/logs/silentInstall2007-10-
25_05-23-36PM.log' for more details.

Oracle Database 10g Uninstallation : OK

Clearing up the Oracle installation

-----INFO: Removing database startup script...

```



```
warning: /etc/profile.d/oracle.sh saved as
/etc/profile.d/oracle.sh.rpmsave
no crontab for oracle
Done.
```

7. Verify that the directory `/opt/oracle` AND the account “oracle” do not exist.

---

**Note** – Files created during Oracle install are removed along with the oracle user account. Since SLES systems require an oracle user account to be present before installing, make sure the correct version orarun RPM is installed before installing Oracle 10g again. For SLES9, orarun RPM can be found at: <http://ftp.novell.com/partners/oracle/sles-9/>  
For SLES10, orarun RPM can be found in the product CD.

---

8. Reboot the server.

---

## Upgrading the Linux Management Server from v5.1 to v6.0

---

**Note** – Prior to beginning the upgrade, ensure your system and software environment meets the version requirements for the upgrade, as stated in the Support Matrix and related documents.

---

---

**Caution** – As part of upgrading the management server, related passwords are set to their defaults. See the User Guide in the Document Center (**Help > Documentation Center**) for more information on default passwords. It is recommended that you customize your passwords following the upgrade process.

---

## Considerations Before You Upgrade

Before you begin, consider the following:

- Refer to the Release Notes for late breaking information about upgrading the management server.
- The latest build of the software requires you to migrate your Brocade switches to the Brocade SMI-Agent Provider (SMI-A). Until you migrate your Brocade switches to SMI-A, data such as topology and zoning from the Brocade switch

will be stale and you will be unable to use the Brocade switch to perform provisioning or gather port performance statistics through the Brocade switch. Any Brocade switches that are managed with the Brocade Fabric Access API provider will be quarantined after upgrading the management server. The management server retains the data for the API switches after upgrading, but you cannot Get Details until you migrate Brocade switches to the Brocade SMI Agent provider.

- The latest build of the software requires you to upgrade some of your CIM Extensions. Please refer to “About Upgrading Your CIM Extensions” (in the Deploying and Managing CIM Extensions chapter) for details.
- The installation will fail if there is insufficient temporary space. You must have at least 2 GB in the /tmp directory.
- After you upgrade the software, you are required to run Discovery Step 1 and Get Details on all new and existing managed elements. This allows the software to gather any new data that is associated with the new features available in the latest release.
- Windows hosts using SecurePath – SecurePath information is not retrieved from legacy CIM extensions.
- After you upgrade, you need to rediscover backup details. Make note of your Backup Manager hosts. Refer to Protection Explorer for a list of Backup Manager hosts.
- The following elements are not supported even though they were supported in Service Pack 4, Build 5.1 of the management server:
  - Cisco switches with firmware versions earlier than 3.1.x for switches discovered through SMI-S. You need to upgrade to version 3.2.(2c) if you want to discover the Cisco switches through SMI-S.
  - Brocade SMI-A versions prior to 120.6.0a. You need to upgrade to at least version 120.6.0a.
- You should try to complete the upgrade and its subsequent steps in one session, which may take several hours, depending on your network configuration.
- It is necessary to perform Get Details after you upgrade to repopulate the database.
- Upgrade and start the Windows proxy service first and then the management server.
- Some upgrade-related steps are required after the upgrade, as indicated later in this section.
- Any customizations to your CIMOMConfig.xml will not be preserved, because the file format has changed. The old file will be saved for reference. The customizations in the old CIMOMConfig.xml file must be manually merged into the file shipped with 6.0 and you must restart the CMS before the customizations are applied to the updated CMS. Depending upon the customizations, starting the CMS using the default CIMOMConfig.xml file can have varying impacts.
  - If end-users change the port number of some of the discovery groups and then start the CMS using the default config file, the discovery groups may not start up since the default ports may be in use.

- If end-users modify the repository location and start the CMS using the default config file, the system fails to locate the discovered elements in the new repository created in the default location. If this happens, reapply the customizations to the new CMS or end-users will have problems running discovery or collecting data.
- Users who wish to continue gathering backup data from their backup manager hosts must update the CIM extensions on those hosts. The procedure for upgrading the CIM extension on a backup managing host is the same as for any host.
- The Brocade switch manufacturer no longer supports the Brocade Fabric Access API provider and as a result, this release of the management server does not support the Brocade Fabric Access API after updating.
- If you are installing from a network drive, see the section at the beginning of this chapter, “Installing from a Network Drive” on page 12

## Upgrade Overview

The following table summarizes the steps to upgrade the management server, and the steps following the table provide additional information about the upgrade process. Make sure you have a functional management server before starting the upgrade. Also, be sure you have completed any necessary pre-upgrade steps prior to starting the upgrade.

**Table 1:**

| Upgrade                  | New Install     | Description                                                                                                                                                                                     |
|--------------------------|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| upgradeAppStorManager.sh | Not Applicable  | Initiates the upgrade process<br>Checks for prerequisite conditions and exits if any condition is not satisfied.<br>Stops running services and exports current database to a temporary location |
| uninstallOracle9i.sh     | Not Applicable  | Removes the existing Oracle 9i installation, clears remaining files and removes the Oracle user account                                                                                         |
| InstallDatabase          | InstallDatabase | Installs Oracle 10g                                                                                                                                                                             |

**Table 1:**

| <b>Upgrade</b>            | <b>New Install</b>        | <b>Description</b>                                                                                                                    |
|---------------------------|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Install Management Server | Install Management Server | Installs Management Server. Upgrades code base and database schema files, if an existing Management Server installation is discovered |
| migrateData.sh            | Not Applicable            | Verifies if the database is created properly and imports database exported by upgradeAppStorManager.sh                                |

---

## Steps to Upgrade the Management Server

### Step 1 - Read the Support Matrix and Release Notes

Read the support matrix and release notes. Read the support matrix to make sure the servers on which you are upgrading the management server meet or exceed the requirements. Management server requirements are listed on the Manager Platform (Mgr Platform) tab of the support matrix. Also, read the release notes for late breaking issues not covered in the Installation Guide. The release notes and support matrix can be found on the top-level of the management server CD and the CIM extension CDs.

## Step 2 - Verify that You Are Running Build 5.1 Service Pack 4 or a Later 5.1 Service Pack

Verify that you have a working Build 5.1, SP4 management server before upgrading to Build 6.0. Existing installations that are at Build 5.1, SP1, Build 5.1, SP2, or Build 5.1, SP3, must upgrade to Build 5.1, SP4 or later prior to upgrading to Build 6.0.

## Step 3 - Save Configuration Files for the Global Change Management Business Tool

Make a copy of the configuration files saved through the Global Change Management Business Tool. The configuration files are not retained after you upgrade the product. These files are located in the “advisors/saved-configuration” area on the management server. Place these files back after the upgrade or reinstall. If you do not use Global Change Management or do not wish to keep the old configurations, you may ignore this step.

## Step 4 - Run the upgradeAppStorManager Script

Run the upgradeAppStorManager.sh script from the Oracle disk to begin the upgrade process.

- The script upgradeAppStorManager.sh initiates the upgrade process. It checks for prerequisite conditions and exits if any condition is not satisfied. It stops running services and exports the current database to a temporary location. All output will be logged to a time stamped file named  
upgradeAppStorManager\_<timestamp>.log in  
/var/tmp/.appstor.
- The upgradeAppStorManager.sh script stops the management server before proceeding with Oracle9i uninstall.

## Step 5 - Run the uninstallOracle9i Script

---

**Note** – Before running uninstallOracle9i.sh, make sure that AppStorManager service is not running.

---

Run the uninstall script to uninstall the Oracle 9i installation.

- Run the uninstall script “uninstallOracle9i.sh” from the Oracle disk to uninstall the Oracle 9i installation. This removes the existing Oracle 9i installation, clears remaining files, and removes the Oracle user account. All output will be logged to a timestamped file named `uninstallOracle9i_<timestamp>.log` in `/var/tmp/.appstor`.

---

**Note** – After Oracle9i is uninstalled, ensure that the oracle listener and other oracle processes are NOT running. Execute the following command and verify that the command does not show any active processes:

```
ps -ef | grep oracle | grep -v grep
```

If any oracle processes are still running, stop them by executing the kill command as shown in the following:

```
kill -9 <process-id> (where <process-id> is the id of each process returned by the previous command)
```

- 
- If you are running SuSE Linux on the machine, for SLES 9, you must install the `orarun-1.8-109.15` RPM to create an Oracle user account. This user account was removed by `uninstallOracle9i.sh` in the previous script. (The RPM for SLES 9 is at <http://www.novell.com/products/server/oracle/software.html>.)
  - After installing the RPM, enable the oracle user account by editing the file `/etc/passwd` and setting the path to the shell for this account.

---

**Note** – For more information about uninstalling Oracle using the scripts, see the Troubleshooting section in this Installation guide “Troubleshooting Installation/Upgrade” on page 447.

---

## Step 6 - Install the Oracle 10g Database

Install the database.

- Run the script “InstallDatabase” from the Oracle disk to install the database. All output will be logged to a time stamped file named `InstallDatabase_<timestamp>.log` to `ORACLE_HOME`.
- An Oracle account is created automatically for Red Hat Linux machines. If the Oracle account is not enabled for SUSE Linux machines, then the `InstallDatabase` script will exit with an error. To enable the account on SUSE Linux machines, edit `/etc/passwd` and set the path to the shell.
- Once Oracle 10g is installed, source the orahome created after the Oracle 10g installation by running `. /var/opt/oracle/orahome` and note there is a space between the period (.) and `/var`.

## Step 7 - Upgrade the Management Server

Install the Management Server from the Management Server disk to perform the upgrade.

- Install the management server as described in this chapter, “Step 2 - Install the Management Server” on page 25. The installation process will determine that the previous management server build has been found and will ask if you want to upgrade the management server. Select **Next** to continue the upgrade process.

## Step 8 - Import the Database

Import the database that was exported by `upgradeAppStorManager.sh` previously, using the `migrateData` script that is present in the Oracle disk.

- Run `migrateData.sh` to import data exported by `upgradeAppStorManager.sh`.
- All output will be logged to a time stamped file named `migrateData_<timestamp>.log` to `/var/tmp/.appstor`.

## Step 9 - Start Management Server

Execute the following command to start the management server (`appstormanager` service):

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

## Step 10 - Customize Database Passwords

During the upgrade, all Oracle passwords are reset to their defaults, including the TNS listener password, and the passwords for the SYS, SYSTEM, DB\_SYSTEM\_USER, RMAN\_USER accounts. Please change these passwords using the `dbAdmin` tool after upgrade completes successfully. This is stated in the console output that is displayed during the upgrade process.

## Step 11 - Enable RMAN Backup if Desired

RMAN Backup is disabled by default as part of the upgrade process. When you log into the management server after upgrade, you will see a message informing you that RMAN Backup is disabled. You should re-enable RMAN Backup as soon as possible so you do not stop backing up your data.

## Step 12 - Upgrade Selected CIM Extensions

Upgrade CIM extensions on servers with the following functionality:

- Backup Manager Hosts - Backup information is not gathered from legacy CIM extensions. In order for backup information to be gathered by the management server, the CIM extensions on the Backup Manager Host must be at the same software version as the management server. When you upgrade your management server, upgrade the CIM extensions on your Backup Manager Host in order to continue to see backup data.
- Windows hosts using SecurePath – SecurePath information is not retrieved from legacy CIM extensions.
- Host for which you want to retrieve cluster information (i.e., Veritas Cluster Server on Solaris cluster and Microsoft Cluster Server). (This is new functionality that requires version 6.0 of the CIM extension.)
- Linux hosts that support QLogic failover. (This is new functionality that requires version 6.0 of the CIM extension.)

## Step 13 - Rediscover All Elements

You should rediscover all elements after you do an upgrade by doing Discovery Step 1 and Get Details. Doing Discovery Step 1 and Get Details is important because:

- Better scalability is provided after discovery.
- Cluster functionality. To use the new functionality, upgrade CIM Extensions to version 6.0. Rediscovery is required.
- You will see the following issues until you do Discovery Step 1 and Get Details:
  - Reports and Capacity Manager/Capacity Explorer show incorrect raw capacity data for storage systems.
  - There is no trunked status indication on Brocade fabrics.
  - No NPIV status indication.
  - No provisioning for 3PAR storage systems and HP StorageWorks EVA arrays using Command View EVA 5.03, 6.0.1, 6.0.2, or 7.x.
  - New hosts modes on storage systems are not available.
  - Backdata collection would be suspended until CIM extensions on Backup Manager Hosts are upgraded to version 6.0 and they are rediscovered.

---

## Steps that Can Be Run Anytime after the Upgrade

The following steps can be completed anytime after the upgrade; however, you will have reduced functionality with the product until you complete these steps.



## Re - Add Remote Sites in Global Reporters

After the upgrade, add remote sites in Global Reporters. This topic is covered in more detail in this guide, in the chapter, *Installing the Management Server on Microsoft Windows*.

---

**Caution** – After upgrade, all remote sites in the Global Reporters are removed. This is done so you can have a chance to upgrade the remote sites to the same build before Global Reporter attempts to gather data. Before you re-add the remote sites, be sure to upgrade them to the same build as the management server.

---

## Migrate Your Brocade Switches to SMI-A

The latest build of the software requires you to migrate your Brocade switches to SMI-A. Until you migrate your Brocade switches to SMI-A, data such as topology and zoning from the Brocade switch will be stale and you will be unable to use the Brocade switch to perform provisioning or gather port performance statistics through the Brocade switch.

Any Brocade switches that are managed with the Brocade Fabric Access API provider will be quarantined after upgrading the management server. The management server retains the data for the API switches after upgrading, but you cannot Get Details until you migrate Brocade switches to the Brocade SMI Agent provider.

The latest build of the software requires you to upgrade some of your CIM Extensions. See “About Upgrading Your CIM Extensions” on page 213.

You will need a new proxy server for Brocade. See the support matrix for requirements.

## About Migrating Your Brocade Switches to SMI-A

After successfully upgrading the management server, any Brocade switches that use the Brocade Fabric Access API provider must be migrated to the Brocade SMI-A provider. The management server will prompt you to migrate your Brocade switches the first time you log on to the management server after the upgrade and will display the Brocade API switches that need to be migrated.

Until you migrate your Brocade switches to SMI-A, data such as topology and zoning from the Brocade switch will be stale and you will be unable to use the Brocade switch to perform provisioning or gather port performance statistics through the Brocade switch. The Brocade Fabric

Access API switches are quarantined and you will have the option to migrate to the Brocade SMI-A provider at your discretion in case your SAN policy requires that you validate the new Brocade SMI Agent provider before migrating your Brocade switches.

The quarantined API-managed Brocade switches retain their historical data and that data remains intact during the migration to the SMI-A provider.

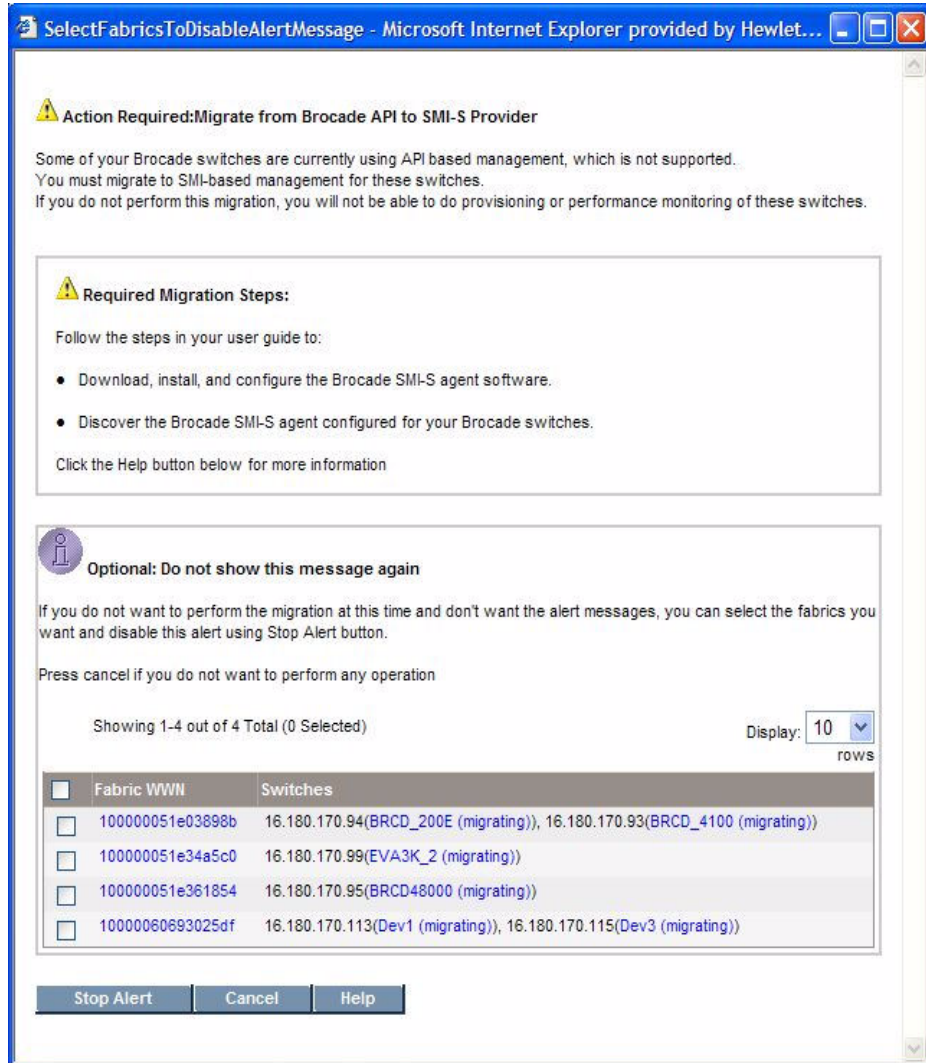
However, new data will not be collected for the quarantined Brocade switches until you migrate the switches to the SMI-A provider.

After migrating the Brocade switches to SMI-A, the Brocade SMI-A proxy server is placed in its own discovery group. This new discovery group is not part of any Get Details schedule. If the Brocade switches were part of a Get Details schedule prior to migration, you must manually adjust those schedules to run Get Details for the migrated Brocade switches. If the schedules are not adjusted manually, Get Details will not run for the migrated switches as per pre-migration schedules.

Follow these steps to migrate your Brocade switches to the Brocade SMI-A provider:

1. Download the Brocade SMI Agent v120.6.0a provider software and its Installation Guide from the Brocade website:  
<http://www.brocade.com/support/SMIAGENT.jsp>  
See the support matrix for your edition for details on the latest supported version for the management server.
2. Install the Brocade SMI Agent with a minimum version of 120.6.0a and configure the proxy servers on the server with which you will manage your Brocade access points following the installation and configuration instructions included in the Brocade v120.6.0a Installation Guide. Refer to the Brocade document for SMI-A requirements.

3. Log on to the management server. The management server alerts you to migrate your Brocade Fabric Access API switches when you first log on.




Your Brocade switches are quarantined until you migrate to the SMI-A provider. The migration message is displayed each time you log on to the management server until each Brocade switch is migrated to the new Brocade SMI-A provider or you choose to disable the message.

4. Run Discovery Step 1 for the Brocade proxy server. See the chapter, "Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries."

5. Run Get Details. See the chapter, “Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries.”

The Brocade switches are migrated to the SMI-A provider.

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

6. If you were using discovery schedules to collect details for Brocade switches prior to migrating them to SMI-A, add the new discovery group for the Brocade proxy server to your pre-existing Get Details schedules as described in the following steps:
  - a. Access the Discovery page by selecting **Configuration > Discovery**.
  - b. Click the **Edit** () button corresponding to the discovery schedule you want to modify.
  - c. Click the **Discovery Groups** tab.
  - d. Select the Brocade proxy under the list of discovery groups.
  - e. Click **Add Selected Groups To Schedule**.
  - f. Click **Finish**.

## Upgrade Your CLI Clients

CLI Clients earlier than Build 6.0 do not work with Build 6.0 of the management server. Refer to the CLI Guide for more information about upgrading your CLI clients.

## Upgrading Your CIM Extensions

It is preferable to upgrade all CIM extensions to the same version as the management server, as some functionality may be unavailable when earlier CIM Extensions are used. See “About Upgrading Your CIM Extensions” on page 213 in the Deploying and Managing CIM Extensions chapter.

## Installing the Management Server on Sun Solaris

---

Follow the steps in this topic to install the management server on Sun Solaris.

See the following topics if you are installing the management server on another supported operating system:

- “Installing the Management Server on Microsoft Windows” on page 85
- “Installing the Management Server on Linux” on page 7

---

**Note** – These steps are for installing the management server on Sun Solaris. See “Upgrading the Management Server” on page 70 later in this topic 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 50
- “Step 2 - Install the Management Server” on page 59
- “Step 3 - Verify that Processes Can Start” on page 61
- “Step 4 - Verify You Can Connect to the Management Server” on page 63
- “Configurations Required for Discovering EMC CLARiiON Storage Systems” on page 65
- “Installing the Java Plug-in on Sun Solaris” on page 64
- “Removing the Management Server” on page 66
- “Porting the Management Server Across Operating Systems” on page 69
- “Upgrading the Management Server” on page 70

# 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 DVD for the management server database.

---

**Caution** – 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 DVD 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.
- Install the database on Solaris. If you are upgrading the management server, see “Upgrading the Management Server” on page 70 for more information.
- When you install the database on Solaris, files with group writeable permissions are installed in the `/opt/oracle` directory.

## 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.

```
forceload: sys/semsys
forceload: sys/shmsys

set shmsys:shminfo_shmmax = 4294967295
set shmsys:shminfo_shmmni = 100
set semsys:seminfo_semmni = 100
set semsys:seminfo_semmsl = 256
set semsys:seminfo_semmns = 1024
set semsys:seminfo_semopm = 100
set semsys:seminfo_sevmx = 32767
```

- The following packages are required for Solaris 9:
  - SUNWspox
  - SUNWarc
  - SUNWbtool
  - SUNWhea
  - SUNWlibm
  - SUNWlibms
  - SUNWmfrun
  - SUNWsprot
  - SUNWtoo
  - SUNWxfnt
  - SUNWi1of
  - SUNWxcu4
  - SUNWuiu8
  - SUNWulcf
  - SUNWi1cs
  - SUNWi15cs

If any of these Solaris 9 packages are not present during install, the installer halts and prompts you to include the missing packages.

- The following minimum patches are required for Solaris 9.
  - 112233-11
  - 111722-04
  - 115675-01

- 113471-08
- 115675-01
- 112963-25

Install the patches with the same or later revision. If the patches are not present, the installer stops and prompts for the missing patch.

- If the management server is being installed on Sun Solaris 10, ensure that the attributes in the user.root project are set with the following values:
  - The `project.max-shm-ids` attribute has a value of 100
  - The `project.max-sem-ids` attribute has a value of 256

Enter the following command to list the current project settings for root:

```
prctl -P -t privileged -i project user.root
```

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)
```

- The following packages are required for Solaris 10:
  - SUNWarc
  - SUNWbtool
  - SUNWhea
  - SUNWlibm
  - SUNWlibms
  - SUNWmfrun
  - SUNWsprot
  - SUNWtoo
  - SUNWxwfnt
  - SUNWi1of
  - SUNWxcu4
  - SUNWuiu8
  - SUNWulcf
  - SUNWi1cs
  - SUNWi15cs

If any of these Solaris 10 packages are not present during install, the installer halts and prompts you to include the missing packages.



# Installing the Database

To install the database:

1. Make sure there are no existing Oracle user accounts on the computer.
2. Choose from one of the following installation options:
  - From the network:
    - a. Insert the DVD into the system to be used to export the install media.
    - b. Share the DVD mount point by updating the `/etc/dfs/dfstab` settings appropriately.
    - c. Mount the exported DVD on the server where the installation is being performed. For example:

```
mkdir /mnt/appdb60
```

```
mount <IP of DVD export server>:<DVD mount point>/mnt/appdb60
```

- d. Run `/mnt/oracleDVD/InstallDatabase`

3. Start the installation of the database by entering the following:

---

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

---

```
/cdrom0/appdb60/InstallDatabase
```

Output similar to the following is displayed. Enter y when prompted and press return to accept the default directories.

```
bash-3.00# /Disk1/InstallDatabase
```

```
This script installs Oracle ##### (Script version: 1.1)
```

```
Logging to /tmp/InstallDatabase_200710180919.log
```

```
Do you wish to continue ? [y/n]: y
```

```
INFO: Oracle Media OK.
```

```
INFO: System architecture OK.
```

```
INFO: System Memory OK. (Minimum is 2048 Megabytes, you have 4096
Megabytes).
```

```
INFO: Swap Space OK. (You have 7361 Mb).
```

```
INFO: Checking KERNEL parameters...
```

```
INFO: KERNEL parameters OK.
```

WARNING: noexec\_user\_stack is not set in /etc/system.  
WARNING: This security setting disables execution of user programs on the stack.  
WARNING: Please consult the install guide for more information.

INFO: Checking for required PACKAGES...  
INFO: PACKAGES OK.  
INFO: PATCHES OK.

Are you ready to start the Oracle installation ? [y/n]: **y**  
Please enter the Oracle user's home directory. [Default: /export/home/oracle]  
Using /export/home/oracle as oracle users home directory

Please enter Oracle installation directory [Default: /opt/oracle]  
Installing Oracle to : /opt/oracle

INFO: Created Oracle users home directory.

WARNING: It is recommended that you have at least 50000 MB (50 GB) of disk space  
in the Oracle installation directory. You only have 34972 MB.  
Do you wish to continue ? [y/n]: **y**

INFO: Creating dba group if not present.

INFO: Creating oracle user

INFO: Created Oracle users home directory.

INFO: The next step is to start the Oracle Universal Installer.

Start the Oracle Universal Installer ? [y/n]: **y**

After the silent install completes, the following script output is displayed. Your output may differ slightly based on the file paths you entered.

The installation of Oracle Database 10g was successful.

Please check '/var/opt/oracle/oraInventory/logs/silentInstall2007-07-16\_04-07-23PM.log' for more details.

Installer Finished: The installation of Oracle Database 10g was successful.

The database installer completed successfully

running /opt/oracle/product/10.2.0/root.sh

Running Oracle10 root.sh script...

The following environment variables are set as:

ORACLE\_OWNER= oracle

ORACLE\_HOME= /opt/oracle/product/10.2.0

Enter the full pathname of the local bin directory: [/usr/local/bin]:

Copying dbhome to /usr/local/bin ...

Copying oraenv to /usr/local/bin ...

Copying coraenv to /usr/local/bin ...

Creating /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.

Oracle Home is /opt/oracle/product/10.2.0

The 10.2.0.3 upgrade proceeds immediately after the 10.2.0 install and requires no interaction.

Starting Patch Installer....

Deinstall in progress (Thu Oct 18 09:35:02 EDT 2007)

..... 0%  
Done.

..... 16%  
Done.

..... 33%  
Done.

..... 50%  
Done.

```

..... 67%
Done.

..... 100%
Done.

Deinstall successful
Installation in progress (Thu Oct 18 09:35:02 EDT 2007)
..... 16%
Done.

..... 33%
Done.

..... 50%
Done.

..... 67%
Done.

..... 84%
Done.

..... 87% Done.

Install successful
Linking in progress (Thu Oct 18 09:39:26 EDT 2007)
.. 87% Done.

Link successful

Setup in progress (Thu Oct 18 09:40:52 EDT 2007)
..... 100% Done.

Setup successful

End of install phases.(Thu Oct 18 09:41:00 EDT 2007)
Starting to execute configuration assistants
Configuration assistant "Oneoff Patch Application" succeeded
The installation of Oracle Database 10g Release 2 Patch Set 2 was
successful.

Please check '/var/opt/oracle/oraInventory/logs/silentInstall2007-
09-24_05-00-13PM.log' for more details.

Patch Installer Finished: The installation of Oracle Database 10g
Release 2 Patch Set 2 was successful.

The database installer completed successfully
INFO: Upgrade Patch installed successfully.

```

```
Starting CPU patch installer
INFO: Installing October Patch: 6121183
INFO: Patch 6121183 installed successfully.
INFO: Installing October Patch: 6121242
INFO: Patch 6121242 installed successfully.
INFO: Installing October Patch: 6121243
INFO: Patch 6121243 installed successfully.
INFO: Installing October Patch: 6121244
INFO: Patch 6121244 installed successfully.
INFO: Installing October Patch: 6121245
INFO: Patch 6121245 installed successfully.
INFO: Installing October Patch: 6121246
INFO: Patch 6121246 installed successfully.
INFO: Installing October Patch: 6121247
INFO: Patch 6121247 installed successfully.
INFO: Installing October Patch: 6121248
INFO: Patch 6121248 installed successfully.
INFO: Installing October Patch: 6121249
INFO: Patch 6121249 installed successfully.
INFO: Installing October Patch: 6121250
INFO: Patch 6121250 installed successfully.
INFO: Installing October Patch: 6121257
INFO: Patch 6121257 installed successfully.
INFO: Installing October Patch: 6121258
INFO: Patch 6121258 installed successfully.
INFO: Installing October Patch: 6121260
INFO: Patch 6121260 installed successfully.
INFO: Installing October Patch: 6121261
INFO: Patch 6121261 installed successfully.
INFO: Installing October Patch: 6121263
INFO: Patch 6121263 installed successfully.
INFO: Installing October Patch: 6121264
INFO: Patch 6121264 installed successfully.
INFO: Installing October Patch: 6121266
INFO: Patch 6121266 installed successfully.
INFO: Installing October Patch: 6121268
```

INFO: Patch 6121268 installed successfully.  
INFO: Installing October Patch: 6394981  
INFO: Patch 6394981 installed successfully.  
INFO: Installing October Patch: 6397928  
INFO: Patch 6397928 installed successfully.  
INFO: Installing October Patch: 6397929  
INFO: Patch 6397929 installed successfully.  
INFO: Installing October Patch: 6397937  
INFO: Patch 6397937 installed successfully.  
INFO: Installing October Patch: 6397938  
INFO: Patch 6397938 installed successfully.  
INFO: Installing October Patch: 6397939  
INFO: Patch 6397939 installed successfully.  
INFO: Installing October Patch: 6397940  
INFO: Patch 6397940 installed successfully.  
INFO: Installing October Patch: 6397941  
INFO: Patch 6397941 installed successfully.  
INFO: Installing October Patch: 6397942  
INFO: Patch 6397942 installed successfully.  
INFO: Installing October Patch: 6397943  
INFO: Patch 6397943 installed successfully.  
INFO: Installing October Patch: 6397944  
INFO: Patch 6397944 installed successfully.  
INFO: Installing October Patch: 6397945  
INFO: Patch 6397945 installed successfully.  
INFO: Installing October Patch: 6397946  
INFO: Patch 6397946 installed successfully.  
INFO: Installing October Patch: 6397947  
INFO: Patch 6397947 installed successfully.  
INFO: Installing October Patch: 6397948  
INFO: Patch 6397948 installed successfully.  
INFO: CPU Patches installed.  
INFO: CPU Patch installed successfully.  
INFO: updating oracle files  
INFO: Oracle install complete.  
[]

Oracle is now installed.

---

**Caution** – In order to enable automatic RMAN backups on Oracle 10g, you must change the archive mode. See the User Guide in the Documentation Center (**Help > Documentation Center**) for the steps to enable automatic RMAN backups.

---

## 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 50.

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_Sun_StorageTek_Operations_Manager_StorageAuthority/.com.zerog.registry.xml`
  - `/var/.com.zerog.registry.xml`
- During the management server installation, double-byte characters are not allowed in the installation path. InstallScript.iap\_xml has been modified to display the following message if double-byte characters are entered:

The installation path for \$PRODUCT\_NAME\$ may NOT contain double byte characters.

The installation path must be basic ASCII alphanumeric characters, no spaces, no international characters, and no double-byte characters.

Please choose a different installation directory.

To install the management server:

---

**Caution** – You must use the Oracle scripts included on the DVD for the management server if you cancel the installation before completion. The Oracle database is automatically installed by the UNIX installation scripts. See “Uninstalling Oracle Using the Oracle Scripts” on page 451 for the steps to cancel the installation before completion.

---

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. 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
```

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. 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. 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
```

---

**Caution** – 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 the management server and Oracle process have started, enter the following at the command prompt:

```
ps -ef | grep ora
```

Output resembling the following is displayed:

```
oracle 19647 1 0 19:12:58 ? 0:00 ora_q000_APPIQ
oracle 19613 1 0 19:12:39 ? 0:05 ora_smon_APPIQ
oracle 19599 1 0 19:12:39 ? 0:00 ora_pmon_APPIQ
oracle 19601 1 0 19:12:39 ? 0:00 ora_psp0_APPIQ
oracle 19627 1 0 19:12:48 ? 0:00 ora_qmnc_APPIQ
root 20820 20819 28 13:01:00 ? 0:21
/opt/<product_name>/Tools/storApplicationServer -Dappiq.mgr.dist=
/opt/SUN
root 20819 1 0 13:00:59 ? 0:00 ./appstormservice
/opt/<product_name>/ManagerData/conf/solaris-wrapper.c
oracle 19651 1 0 19:13:03 ? 0:00 ora_q001_APPIQ
oracle 19611 1 0 19:12:39 ? 0:18 ora_ckpt_APPIQ
oracle 19607 1 0 19:12:39 ? 0:02 ora_dbw1_APPIQ
oracle 19603 1 0 19:12:39 ? 0:01 ora_mman_APPIQ
oracle 19609 1 0 19:12:39 ? 0:05 ora_lgwr_APPIQ
oracle 19605 1 0 19:12:39 ? 0:02 ora_dbw0_APPIQ
oracle 19615 1 0 19:12:40 ? 0:00 ora_reco_APPIQ
oracle 19617 1 0 19:12:40 ? 0:01 ora_cjq0_APPIQ
oracle 19619 1 0 19:12:40 ? 0:01 ora_mmon_APPIQ
oracle 19621 1 0 19:12:40 ? 0:00 ora_mmn1_APPIQ
oracle 19711 1 0 19:20:00 ? 0:00
/opt/oracle/product/10.2.0/ bin/tnslsnr listener -inherit
```

where /opt/<product\_name> is the directory where you installed the management server

2. 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
```

---

**Caution** – If you are starting the processes manually, start the Oracle process before the process for the management server.

---

3. 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:

- 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 64 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 462. Install the security certificate after you have completed the steps in this chapter.

---

**Caution** – 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 appstromanager 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 454:  
Receiving HTTP ERROR: 503 javax.ejb.EJBException: null;  
CausedByException is: Unexpected Error; nested exception is:  
java.lang.NoClassDefFoundError

---

3. Click **Security > Licenses** in the upper-right corner.
4. Select the tools and enter the number of MAPs, MALs, instances, and terabytes you are licensed to use.

---

**Caution** – Contact customer support if you are uncertain of which products you purchased and for how many MAPs, instances, and terabytes.

---

5. Click the **Save Changes** button to certify that you are authorized to use the components selected.
6. When you are shown the license agreement, accept the license if you agree with its terms.

Your changes take effect.

---

## 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 in this directory.
4. Remove any existing links in this directory to the Java plug-in.
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

---

**Note** – The management server service needs to be restarted after installing EMC Navisphere CLI.

---

## 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:

```
oracle 19647 1 0 19:12:58 ? 0:00 ora_q000_APPIQ
oracle 19613 1 0 19:12:39 ? 0:05 ora_smon_APPIQ
oracle 19599 1 0 19:12:39 ? 0:00 ora_pmon_APPIQ
```

```

oracle 19601 1 0 19:12:39 ? 0:00 ora_psp0_APPIQ
oracle 19627 1 0 19:12:48 ? 0:00 ora_qmnc_APPIQ
oracle 19651 1 0 19:13:03 ? 0:00 ora_q001_APPIQ
oracle 19611 1 0 19:12:39 ? 0:21 ora_ckpt_APPIQ
oracle 19607 1 0 19:12:39 ? 0:02 ora_dbw1_APPIQ
oracle 19603 1 0 19:12:39 ? 0:01 ora_mman_APPIQ
oracle 19609 1 0 19:12:39 ? 0:07 ora_lgwr_APPIQ
oracle 19605 1 0 19:12:39 ? 0:03 ora_dbw0_APPIQ
 root 22464 778 0 15:30:17 pts/2 0:00 grep ora
oracle 19615 1 0 19:12:40 ? 0:00 ora_reco_APPIQ
oracle 19617 1 0 19:12:40 ? 0:01 ora_cjq0_APPIQ
oracle 19619 1 0 19:12:40 ? 0:01 ora_mmon_APPIQ
oracle 19621 1 0 19:12:40 ? 0:00 ora_mmln_APPIQ
oracle 20839 1 0 13:01:59 ? 0:00
/opt/oracle/product/10.2.0/ bin/tnslsnr listener -inherit

```

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/10.2.0/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/10.2.0:Y
14. If you are going to reinstall a new build of the management server, make sure you keep the file /var/sadm/appiq/orahome. This file lets you install a new build of the management server by assuming you kept the same Oracle installation.
15. To remove the Oracle software:

- a. Insert the Oracle Database DVD.

- b. Enter the following at the command prompt:

```
uninstallOracle10g.sh
```

- c. If you are asked if you want to continue, click **Y**. Output similar to the following is displayed:

```
This script removes Oracle 10g if present
Continue? [y/n]:
 Oracle 10g found. Removing...
Shutting down Oracle 10g for removal
 Stopping Oracle....
 Oracle stopped.
Removing Oracle 10g
Removing oracle accounts
Oracle 10g has been removed
```

16. Reboot the server.



---

# Porting the Management Server Across Operating Systems

Use the dbAdmin tool to move data from the management server to a management server running a different operating system. The earliest build of the management server supported for porting is 3.0.

Keep in mind the following:

- When you move the management server from Windows to a UNIX system, 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 one operating system to another:

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 the new operating system.
3. Move the \*.zip file you exported in the first step to the computer running the management server, 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 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:

---

**Caution –** Oracle passwords will be reset to their default values. See the User Guide in the Documentation Center (**Help > Documentation Center**) for more information on default passwords.

---

- 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.
- The installation will fail if there is insufficient temporary space. You must have at least 2 GB in the /tmp directory.
- Versions of the software with service packs will report the base build. For example, if you install Service Pack 3, build 5.1.3.51 over the base build 5.1.0.206, and then install a later build such as 6.0.0.x, your previous build is displayed as 5.1.0.206.
- 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.
- 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.
- Any customizations to your CIMOMConfig.xml will not be preserved, because the file format has changed. The old file will be saved for reference. The customizations in the old CIMOMConfig.xml file must be manually merged into

the file shipped with 6.0 and you must restart the CMS before the customizations are applied to the updated CMS. CIMOMConfig.xml is saved in <installation directory>\SavedData.

- The Brocade switch manufacturer no longer supports the Brocade Fabric Access API provider and as a result, this release of the management server does not support the Brocade Fabric Access API after upgrading. See “Migrate Your Brocade Switches to SMI-A” on page 80 for migration information.

**The following files are 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/customTreeNode  
s
- \*All files and subdirectories in \$MGR\_DIST/JBossandJetty/server/appiq/reports/custom
- \*All files and subdirectories in \$MGR\_DIST/JBossandJetty/server/appiq/reports/definitions/cu  
stom

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

**The following files are 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/automato  
rs - 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

## Considerations Before you Upgrade

Before you upgrade, consider the following:

- The latest build of the software requires you to migrate your Brocade switches to SMI-A. Until you migrate your Brocade switches to SMI-A, data such as topology and zoning from the Brocade switch will be stale and you will be unable to use the Brocade switch to perform provisioning or gather port performance statistics through the Brocade switch. Any Brocade switches that are managed with the Brocade Fabric Access API provider will be quarantined after upgrading the management server. The management server retains the data for the API switches after upgrading, but you cannot Get Details until you migrate Brocade switches to the Brocade SMI Agent provider.
- The latest build of the software requires you to upgrade some of your CIM Extensions. See “About Upgrading Your CIM Extensions” on page 213.
- After you upgrade the software, you are required to run Discovery Step 1 and Get Details on all new and existing managed elements. This allows the software to gather any new data that is associated with the new features available in the latest release.
- After you upgrade, you need to rediscover backup details. Make note of your Backup Manager hosts. Refer to Protection Explorer for a list of Backup Manager hosts.
- The following elements are not supported even though they were supported in Service Pack 4, Build 5.1 of the management server:
  - Cisco switches with firmware versions earlier than 3.1.x for switches discovered through SMI-S. You need to upgrade to version 3.2.(2c) if you want to discover the Cisco switches through SMI-S.
  - Brocade SMI-A versions prior to 120.6.0a. You need to upgrade to at least version 120.6.0a.

## Step 1 - Read the Support Matrix and the Release Notes

Read the support matrix to make sure that the servers on which you are upgrading the management server meets or exceeds the requirements. The management server requirements are listed on the **MGR platform** tab of the support matrix. Also, read the release notes for late breaking issues not covered in the installation guide. The release notes and support matrix can be found at the top-level of the management server CD and the CIM Extension CDs.

## Step 2 - Verify your Version

Verify that you have a working management server build 5.1 SP4 before upgrading to build 6.0 Existing installations that are at build 5.1, SP1, build 5.1 SP2 or build 5.1 SP3 must be upgraded to 5.1 SP4 or later prior to upgrading to build 6.0.

## Step 3 - Save the Configuration Files

Make a copy of the configuration files saved through the Global Change Management Business Tool. The configuration files are not retained after you upgrade the product. These files are located in the advisors/saved-configuration area on the management server. Place these files back after the upgrade or reinstall. Ignore this step if you do not use Global Change Management or do not want to keep the old configurations.

## Step 4 - Manually Export the Database and Create an Image of the Server

1. Manually export the database by running the Database Admin Utility (dbAdmin). Refer to the User guide in the Documentation Center (**Help > Documentation Center**) for the steps.

---

**Caution** – Make sure that you save the backup in a directory structure that is not part of the management installation directory.

---

2. Exit all external utilities that use Oracle.

## Step 5 - Run the upgradeAppStorManager script

To run the upgradeAppStorManager script, enter the following at the command prompt as user 'root':

```
$ /mnt/<DBDisk>/upgradeAppStorManager.sh
```

The upgradeAppStorManager script performs all the steps required to back up the current AppStorManager database. It will shut down the AppStorManager process and not restart it.

You are prompted for a backup location with at least 10-Gb of space. The default location is a backup directory in the \$MGR\_DIST install location.

Output similar to the following is displayed. Enter y when prompted and press return to accept the default directories.

```
This script installs AppStorManager Oracle 10g, migrating from
9i
```

```
 Logging to
/opt/Sun_StorageTek_Operations_Manager/logs/upgradeAppStorManager_2
00707191142.log
```

```
INFO: All Oracle passwords will be reset to their defaults,
 including the TNS listener password, and the passwords
 for the SYS, SYSTEM, DB_SYSTEM_USER, RMAN_USER, and
 REPORT_USER accounts. Please change these passwords using
 the dbAdmin tool after upgrade completes successfully.
```

```
Continue? [y/n]: y
```

```
INFO: Check if oracle is installed
```

```
INFO: Oracle found
```

```
INFO: Check for AppStorManager
```

```
INFO: AppStorManager is running
```

```
INFO: Stopping AppStorManager
```

```
stopping appstormanager....
```

```
INFO: Backup AppStorManager
```

```
Please enter a location for the backup: [Default:
/opt/Sun_StorageTek_Operations_Manager/backup]
```

```
INFO: Using /opt/Sun_StorageTek_Operations_Manager/backup as the
backup location
```

```
INFO: the specified directory
/opt/Sun_StorageTek_Operations_Manager/backup only has 7356 MB free
```

```
INFO: need at least 10Gb of space for backup
```

```
Please enter a location for the backup: [Default:
/opt/Sun_StorageTek_Operations_Manager/backup]
```

```
INFO: Using /opt/Sun_StorageTek_Operations_Manager as the backup
location
```

```
INFO: Exporting AppStorManager database to
/opt/Sun_StorageTek_Operations_Manager ***** Started export on: Thu
Jul 19 11:58:04 2007 ****
```

```
***** Started truncateMview on: Thu Jul 19 11:58:04 2007 ****
```

```
Connected.
```

```

*** Finished truncateMview on Thu Jul 19 11:59:52 2007 ***
. exporting job queues
. exporting refresh groups and children
. exporting dimensions
. exporting post-schema procedural objects and actions
. exporting statistics
Export terminated successfully without warnings.
Creating the dump file...
INFO: Backup completed successfully.
INFO: Database migration complete.
*** Restarting the database ***

```

## Step 6 - Upgrade Oracle 9i to Oracle 10g<sub>r</sub>

---

**Note** – The database configuration and creation script is different for Oracle 10g than it was for Oracle 9i. As a result, the management server software build 6.0 is not supported by Oracle 9i. Management server software builds earlier than 6.0 are not supported on the Oracle 10g platform.

---

1. After running the `upgradeAppStorManager.sh` script, remove Oracle 9i with the following command:

```
uninstallOracle9i.sh
```

Output similar to the following is displayed. Enter `y` when prompted and press return to accept the default directories.:

```
This script removes Oracle 9i if present
```

Enter `y` to continue.

```
Continue? [y/n]
```

**y**

```
Oracle 9i found. Removing...
```

```
Shutting down Oracle 9i for removal
```

```
 Stopping Oracle...
```

```
 Oracle stopped.
```

```
Removing Oracle 9i
```

```
Removing oracle accounts
```

```
Oracle 9i has been removed
```

2. Run the InstallDatabase script to install Oracle 10g. See “Installing the Database” on page 52 for the steps to run the InstallDatabase script.

## Step 7 - Upgrade the Management Server

The following steps are required for all users:

1. Install the management server, as described in the topic, “Step 2 - Install the Management Server” on page 59.

The management server automatically installs to its previous location.

2. Upgrade to the latest Sun Solaris CIM Extension on any hosts that are used for backup. See the following chapters for installation information:
  - “Installing the CIM Extension for HP-UX” on page 249
  - Chapter 9, “Installing the CIM Extension for SUSE and Red Hat Linux” on page 187
  - “Installing the CIM Extension for Sun Solaris” on page 301
  - “Installing the CIM Extension for Microsoft Windows” on page 327

## Step 8 - 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 340. After you upgrade the Windows proxy, start its service AppStorWinProxy from the Services window on the Windows host.

## Step 9 - Execute migrateData.sh

Execute `migrateData.sh` from the Oracle DVD. The following output and instructions are displayed:

```
This script finishes the data migration for AppStorManager.
The old backup will be imported into the new AppStorManager product.
Logging to
/opt/Sun_StorageTek_Operations_Manager/logs/migrateData_20070719163
8.log
Continue? [y/n]:
INFO: Check for AppStorManager
INFO: AppStorManager not running
INFO: Restoring AppStorManager
```



```

INFO: A backup file was found:
/opt/Sun_StorageTek_Operations_Manager/backup/dbBackup_200707191142
.zip
Use this backup? [y/n]:
INFO: Importing AppStorManager database to from
/opt/Sun_StorageTek_Operations_Manager/backup/dbBackup_200707191142
.zip
***** Started import on: Thu Jul 19 16:38:58 2007 *****
*** extracting zip file ***
Archive:
/opt/Sun_StorageTek_Operations_Manager/backup/dbBackup_200707191142
.zip
inflating:
/opt/Sun_StorageTek_Operations_Manager/install/database/Oracle/AppI
Q_Oracle_Database.dmp
extracting:
/opt/Sun_StorageTek_Operations_Manager/install/database/Oracle/AppI
Q_CIM_Database.zip
inflating:
/opt/Sun_StorageTek_Operations_Manager/install/database/Oracle/appi
q_tnsnames.ora
inflating:
/opt/Sun_StorageTek_Operations_Manager/install/database/Oracle/appi
q_listener.ora
*** checking AppIQ_Oracle_Database.dmp file ***

```

---

**Note** – The oracle information was removed from the script. Only a partial script is displayed.

---

```

*** Import completed on Fri Jul 20 09:08:19 2007 ***

```

```

INFO: Restore completed successfully.
INFO: Oracle running
INFO: Starting AppStorManager
starting appstormanager

```

```

INFO: AppStorManager is running
INFO: Database migration complete.

```

The management server and Oracle are now upgraded to the latest version. Both Oracle and AppStorManager have been started.

## Step 10 – Customize Database Passwords

All Oracle passwords are reset to their defaults after the upgrade, including the TNS listener password, and the passwords for the SYS, SYSTEM, DB\_SYSTEM\_USER, RMAN\_USER accounts. Please change these passwords using the dbAdmin tool after upgrade completes successfully.

## Step 11 - Enable RMAN Backup if desired

RMAN Backup is disabled by default as part of the upgrade process. When you log into the management server after upgrade, you'll see a message informing you that RMAN Backup is disabled

You should re-enable RMAN backup as soon as possible so you don't stop backing up your data.

## Step 12 - Upgrade Select CIM Extensions

Upgrade CIM extensions on servers with the following functionality:

- Backup Manager Hosts - Backup information is not gathered from legacy CIM extensions. In order for backup information to be gathered by the management server, the CIM extensions on the Backup Manager Hosts must be at the same software build as the management server. When you upgrade your management server, upgrade the CIM extensions on your Backup Manager Hosts in order to continue to see backup data.
- <sup>1</sup> Veritas Cluster Server to retrieve cluster information.

<sup>1</sup>This is new functionality that requires build 6.0 of the CIM extension.

## Step 13 - Rediscover All Elements

You must upgrade the following

You should rediscover all elements after you do an upgrade by doing Discover Step 1 and Get Details.

Performing Discovery Step 1 and Get Details is important because:

- Better scalability is provided after discovery.
- Cluster functionality. To use the new functionality, upgrade CIM Extensions to Version 6.0 and rediscovery is required.

You will see the following issues until you do Discover Step 1 and Get Details:

- Reports and Capacity Explorer show incorrect raw capacity data for storage systems.
- There is no trunked status indication on Brocade fabrics.
- No NPIV status indication.
- No provisioning for 3PAR storage systems and HP StorageWorks EVA arrays using Command View EVA.
- New host modes on storage systems are not available.
- Backup data collection would be suspended until CIM Extensions on Backup Manager Hosts are upgraded to build 6.0 and they are rediscovered.

## Steps that can be run anytime after the Upgrade

The following tasks can be completed anytime after the upgrade. However, you will have reduced functionality with the product until you complete these steps.

### Re-add Remote Sites in Global Reporter

---

**Caution** – After upgrading, all remote sites in the Global Reporters are removed. This is done so you can have a chance to upgrade the remote sites to the same build before Global Report attempts to gather data. Before you re-add the remote sites, be sure to upgrade them to the same build as the management server.

---

All sites that provide global reports must be upgraded to this build of the management server. Install this build 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.


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.

To upgrade the database with data from the added sites, click the **Refresh Now** button at the bottom of the page.

Migrate Your Brocade Switches to SMI-A

After successfully upgrading the management server, any Brocade switches that use the Brocade Fabric Access API provider must be migrated to the Brocade SMI-A provider. The management server will prompt you to migrate your Brocade switches the first time you log on to the management server after the upgrade and will display the Brocade API switches that need to be migrated.

Until you migrate your Brocade switches to SMI-A, data such as topology and zoning from the Brocade switch will be stale and you will be unable to use the Brocade switch to perform

provisioning or gather port performance statistics through the Brocade switch. The Brocade Fabric Access API switches are quarantined and you will have the option to migrate to the Brocade SMI-A provider at your discretion in case your SAN policy requires that you validate the new Brocade SMI Agent provider before migrating your Brocade switches.

The quarantined API-managed Brocade switches retain their historical data and that data remains intact during the migration to the SMI-A provider.

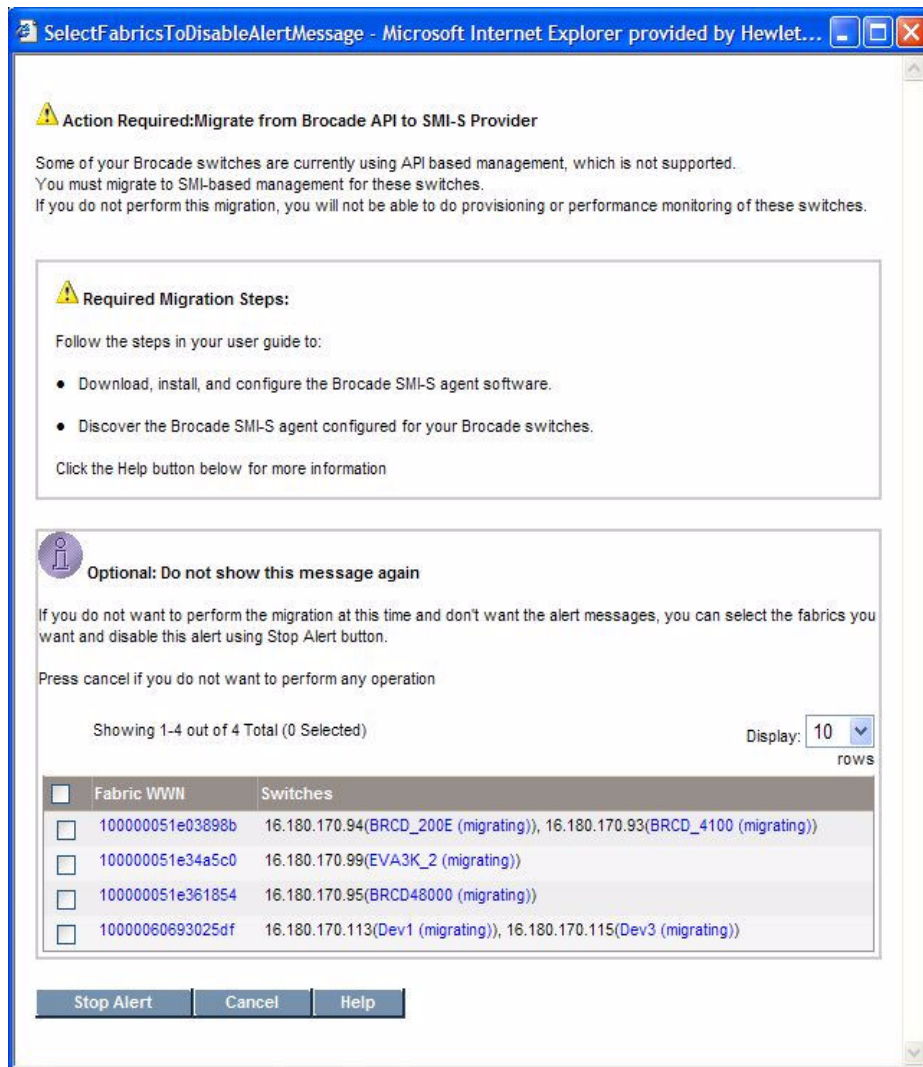
However, new data will not be collected for the quarantined Brocade switches until you migrate the switches to the SMI-A provider.

After migrating the Brocade switches to SMI-A, the Brocade SMI-A proxy server is placed in its own discovery group. This new discovery group is not part of any Get Details schedule. If the Brocade switches were part of a Get Details schedule prior to migration, you must manually adjust those schedules to run Get Details for the migrated Brocade switches. If the schedules are not adjusted manually, Get Details will not run for the migrated switches as per pre-migration schedules.

Follow these steps to migrate your Brocade switches to the Brocade SMI-A provider:

1. Download the Brocade SMI Agent v120.6.0a provider software and its Installation Guide from the Brocade website:  
<http://www.brocade.com/support/SMIAGENT.jsp>  
See the support matrix for your edition for details on the latest supported version for the management server.
2. Install the Brocade SMI Agent with a minimum version of 120.6.0a and configure the proxy servers on the server with which you will manage your Brocade access points following the installation and configuration instructions included in the Brocade v120.6.0a Installation Guide. Refer to the Brocade document for SMI-A requirements.

- Log on to the management server. The management server alerts you to migrate your Brocade Fabric Access API switches when you first log on.




Your Brocade switches are quarantined until you migrate to the SMI-A provider. The migration message is displayed each time you log on to the management server until each Brocade switch is migrated to the new Brocade SMI-A provider or you choose to disable the message.

- Run Discovery Step 1 for the Brocade proxy server. See the chapter, "Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries."

5. Run Get Details. See the chapter, “Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries.”

The Brocade switches are migrated to the SMI-A provider.

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

6. If you were using discovery schedules to collect details for Brocade switches prior to migrating them to SMI-A, add the new discovery group for the Brocade proxy server to your pre-existing Get Details schedules as described in the following steps:
  - a. Access the Discovery page by selecting **Configuration > Discovery**.
  - b. Click the **Edit** () button corresponding to the discovery schedule you want to modify.
  - c. Click the **Discovery Groups** tab.
  - d. Select the Brocade proxy under the list of discovery groups.
  - e. Click **Add Selected Groups To Schedule**.
  - f. Click **Finish**.

## Upgrade your CLI Clients

CLI Clients earlier than build 6.0 do not work with build 6.0 of the management server. Refer to the CLI Guide for more information about upgrading your CLI clients.

## Upgrading your CIM Extensions

See “About Upgrading Your CIM Extensions” on page 213.





## Installing the Management Server on Microsoft Windows

---

Follow the steps in this section to install the management server on the Windows operating system. See “Upgrading the Windows Management Server” on page 94 for information about how to upgrade the management server on Windows.

Be sure to read the requirements in the “Pre-installation Checklist (Installations and Upgrades)” on page 86 for important installation and upgrade information.

See the following topics if you are installing the management server on another supported operating system:

- “Installing the Management Server on Linux” on page 7
- “Installing the Management Server on Sun Solaris” on page 49

This chapter contains the following topics:

- “Pre-installation Checklist (Installations and Upgrades)” on page 86
- “Installation and Upgrade Requirements (Cannot Proceed with Install/Upgrade if Not Met)” on page 87
- “About the Windows Installer” on page 90
- “Installing the Management Server for Windows” on page 91
- “About the Windows Upgrade Wizard” on page 96
- “Upgrading the Windows Management Server” on page 94
- “About Migrating Brocade Fabric Access API-Managed Switches to SMI-S After Upgrading” on page 96
- “About Changes to McDATA and Connectrix Switches After Upgrading” on page 35
- “Configurations Required for Discovering EMC CLARiiON Storage Systems” on page 110
- 

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. The support matrix can be found on the top level of the management server CD-ROM.
- During the management server for Windows installation, double-byte characters are not allowed in the installation path. The installer displays the following error message if the path does not meet the requirements:

The installation path for \$PRODUCT\_NAME\$ may NOT contain embedded spaces, non-English characters, or punctuation. The path is limited to basic ASCII alphanumeric characters.

- Install the management server on a dedicated computer.
- Installation using Virtual Network Computing (VNC) software is not supported.
- If the installation software is accessed over a network, the software must be accessed using a mapped network drive (drive letter). Installation using a UNC path (\\host\sharename) will not work.
- All communication with regard to managed elements is out-of-band via IP, and no SAN connectivity is required or recommended for the management server.

---

## Pre-installation Checklist (Installations and Upgrades)

The following basic requirements must be met before beginning an installation or upgrade. If the management server installation wizard detects missing requirements during system verification you will need to make changes to your system. The basic system requirements are explained in this section along with additional information on how to meet these requirements:

- “Installation and Upgrade Requirements (Cannot Proceed with Install/Upgrade if Not Met)” on page 87
- How to Verify Networking on page 8
- “Be Sure to Install a Supported Browser” on page 90

## Installation and Upgrade Requirements (Cannot Proceed with Install/Upgrade if Not Met)

The requirements listed in Table 4-1 on page 87 must be met or the installation or upgrade will stop. See “About the Verify System Requirements Screen” on page 88 for additional information about the requirements listed on the Verify System Requirements screen (one of the screens displayed during an installation or an upgrade by the installation/upgrade wizard).

**TABLE 4-1** Pre-installation Requirements to Install or Upgrade

| Requirement:                                                                                                                                                                                                                                       | Must Meet or Exceed or the Installation or Upgrade Will Stop:                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NTFS File System:                                                                                                                                                                                                                                  | <p><b>Installations:</b> The NTFS file system is required to install the product. Contact customer support for help with converting the volume to NTFS.</p> <p><b>Upgrades:</b> If Oracle 9i is installed on a volume using the FAT32 file system, you must convert the volume to NTFS before you can upgrade. Contact customer support for information about converting the volume to NTFS.</p>           |
| Screen Resolution:                                                                                                                                                                                                                                 | Minimum resolution is 800x600.                                                                                                                                                                                                                                                                                                                                                                             |
| Windows Account:                                                                                                                                                                                                                                   | You must be logged in as an Administrator.                                                                                                                                                                                                                                                                                                                                                                 |
| Operating System:                                                                                                                                                                                                                                  | Microsoft Windows Server 2003 SP1 or higher. Windows 2000 is no longer supported. See the support matrix for more information.                                                                                                                                                                                                                                                                             |
| MS Internet Explorer:                                                                                                                                                                                                                              | Internet Explorer 6 SP 1 or higher.                                                                                                                                                                                                                                                                                                                                                                        |
| TCP/IP                                                                                                                                                                                                                                             | TCP/IP must be enabled.                                                                                                                                                                                                                                                                                                                                                                                    |
| Minimum disk space for temp and installation files.                                                                                                                                                                                                | The drive that the TEMP environment variable points to must have at least 2 GB of free space. If your TEMP directory is not on your system drive, make sure your system drive has at least 65 MB free as well.                                                                                                                                                                                             |
| %perl5lib% environment variable:                                                                                                                                                                                                                   | The %perl5lib% environment variable cannot be set to any value. See “Troubleshooting Installation/Upgrade” on page 447 for more information.                                                                                                                                                                                                                                                               |
| Installation Locations specified in the Installation Options screen for the following share these requirements: <ul style="list-style-type: none"> <li>• Management Server</li> <li>• Oracle Database</li> <li>• Oracle Database Backup</li> </ul> | <ul style="list-style-type: none"> <li>• Valid locations must be entered on the Installation Options screen.</li> <li>• Path information can only contain the following characters: A-z, 0-9, hyphen, underscore, period, back slash.</li> <li>• The management server, Oracle database, and Oracle database backup paths cannot contain spaces.</li> <li>• Drive letter must be a fixed drive.</li> </ul> |

## About the Verify System Requirements Screen

The Verify System Requirements screen displays the current status for the following based on the results of the system scan performed by the installation wizard after starting the installation or upgrade. Requirements that must be met to proceed with the installation/upgrade and requirements that do not stop the installation/upgrade are described here:

- **Current User Account** — The account you use to install/upgrade must have Windows Administrator privileges or the installation or upgrade will stop.
- **Memory** — The minimum RAM requirement is 4 GB with 6 GB recommended. If the minimum amount of RAM is close to the requirement, the installer continues.
- **Physical Address Extension (PAE)** — PAE is a Windows requirement to utilize amounts of RAM greater than 4 GB on certain versions of Windows. See your Windows documentation for more information about PAE settings. The installation or upgrade continues regardless of PAE.
- **Disk Storage (typical installation)** — Depends on the following:
  - With ARCHIVING and RMAN backup off: minimum disk space: 100 GB, recommended disk space: 200 GB.
  - With ARCHIVING and RMAN backup on: minimum disk space: 200 GB, recommended disk space: 350 GB.

The installation or upgrade will not continue if the disk space requirements are not met.

**Operating System** — Windows 2003 Server SP1, SP2, R2, R2 SP2. The installation or upgrade will not continue if the operating system requirement is not met.

- **Processor** — A dual Intel XEON (or AMD equivalent) 3.4 GHz or higher CPU is required. If the CPU is close to the requirement, the installer continues.
- **DNS Resolution** — The installer verifies the IP address and DNS name of the server using nslookup. If nslookup is not successful, the installation will continue.
- **Port Availability** — The management server requires the following ports to be available:
  - 80
  - 162
  - 443
  - 1098–1120
  - 4444
  - 4445
  - 4763
  - 5962–5988
  - 8009
  - 8083
  - 8093

If you see a warning in the Ports Availability requirement you need to check to be sure that the ports listed are not currently in use and make any changes that are necessary. Be aware that the installation will continue even if a required port is not available.

---

**Note** – The Port Availability requirement line may show a warning during an upgrade that can be ignored, as it indicates that the existing management server service has reserved the ports.

---

## How to turn off Internet Information Services (IIS) and Third-Party Web servers

To turn off Internet Information Services (IIS) and third-party Web servers, verify that Internet Information Services (IIS) is either not installed or the service is set to manual and stopped.

Other third-party Web servers also conflict with the management server, which uses port: 80 and/or port: 443 for its services. If IIS is running, port: 80 and/or port: 443 is already used and management server pages will not be displayed. If IIS is running, you will not be able to access the management server and you will see the following error in the log located at <management serverInstallation Directory>\logs\appiq.log:

```
java.net.BindException: Address already in use: JVM_Bind:
```

## How to Verify Networking

The management server must have static or dynamic host name resolution. To verify that the server's name can be resolved through DNS:

1. Right click **My Computer** in the Start menu.
2. Select **Properties**.
3. Click on the **Computer Name** tab to see the fully qualified name of the computer under the label Full Computer Name. The server must be in the domain in which it is going to be used.
4. From a command prompt, type `nslookup <FQDN>`.  
FQDN (fully qualified domain name) is the fully qualified computer name obtained in the previous step.
5. In the command prompt, type `nslookup <IP address>`.  
IP address is the IP address of the server.

Both results from nslookup should have the same fully qualified computer name and IP address.

6. In the command prompt, type `nslookup <Short name of computer>`. Results should resolve to the computer's fully qualified computer name and IP address.

The management server uses nslookup to resolve managed systems' names and IP addresses. If the DNS suffix `com` is listed in the TCP/IP properties as one to append, problems such as inaccurate system status and incorrect IPs for systems the management server manages may occur. To correct this, remove `com` from the TCP/IP DNS suffix list:

1. Open **Control Panel > Network Connections > Local Area Connection > Properties**. Choose the **Internet Protocol > Properties > Advanced > DNS** tab.
2. If `com` is in the **Append these suffixes (in order)** box, remove it.

---

**Note** – If you will be browsing to the management server from a server in a different domain, assure that the DNS suffix of the management server is added to the suffix list of the web client.

---

## Be Sure to Install a Supported Browser

Install a supported browser on any machine from which you intend to view management server pages. See the support matrix for a list of supported browsers.

---

## About the Windows Installer

The management server installation (wizard) checks your system to verify that it meets the basic system requirements, and it installs the required Oracle database instance and the management server software.

---

**Caution** – Do not install the Oracle database separately. With this release of the product, you must first install the management server for Windows CD-ROM. The installation wizard automatically installs the Oracle database and prompts you for

the Oracle CD-ROM during the installation at the appropriate time. Installing the Oracle database used by the management server manually is no longer recommended.

---

## Installing the Management Server for Windows

Complete the following steps to install the management server for Windows.

---

**Caution** – The drive on which you install the management server must be NTFS format or the install wizard will fail.

---

### Step 1 – Read the Support Matrix and Release Notes

Read the support matrix and the release notes to make sure the server on which you are installing the management server meets or exceeds the requirements. The installer provides a link to these documents accessible on each screen (**Documentation > Support Matrix**). Additionally, see “Installation and Upgrade Requirements (Cannot Proceed with Install/Upgrade if Not Met)” on page 87.

### Step 2 – Install the Management Server for Windows

Do not install the Oracle database separately. See “About the Windows Installer” on page 90 for important information about installing the Oracle database.

1. Start the installation wizard using one of the following options:
  - Put the CD-ROM in the CD-ROM drive of the designated server. The installation wizard program should start automatically. If it does not start, double-click **setup.exe** found in the `root` directory on the management server CD.
  - Optionally, you can copy the contents of the CDs to a network drive or the local hard drive of the designated server and double-click `setup.exe` in the `root` directory. The installer will prompt you to browse to each directory as each component is installed unless you use the following subdirectory structure, in which case the installation wizard automatically locates and installs each installation component. You must create the directory structure below when copying files to a network or local drive.

```
\<ManagementServerCDs>\oracle (Oracle 10 G)
```

```
\<ManagementServerCDs>\srm (management server for
Windows)
```

```
\<ManagementServerCDs>\cimext1 (CIM Extensions CD 1)
\<ManagementServerCDs>\cimext2 (CIM Extensions CD 2, not
required as part of installation)
```

---

**Caution** – 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.

---

2. Read the information on the Welcome screen. Click the hypertext links on the screen to learn about service packs and other important requirements and click **Next** when you are ready to continue.

The System Inspection screen is displayed briefly while the installer checks the system and the Getting Started screen is displayed giving you an overview of the installation process.

3. Click **Next** to continue. The Installation Location screen is displayed.
4. Choose the installation location. You can change the installation location of the management server and the Oracle database if you prefer.

Choose the installation directory where you want to install the Oracle database for the management server. Choose a drive with enough dedicated disk space for the Oracle database and its backup files. The disk space requirements are dependent on the size of the SAN you are managing.

5. Click **Next**.

The installer scans the system to verify that it meets the requirements specified in the support matrix and the Verify System Requirements screen is displayed showing the current status of the system.

If the system does not meet the disk space requirements for the Oracle database used to store the management server data, the installation stops and prompts you to allocate the required disk space.

6. Scroll through the list of system requirements to see if you need to make any changes to your system and click **Next**. Once you click Next, the Summary screen is displayed.

---

**Note** – See “Pre-installation Checklist (Installations and Upgrades)” on page 86 if you need help making changes to meet basic system requirements. See “Troubleshooting Installation/Upgrade” on page 447 for additional information.

---



7. Click **Install**. Click **Previous** if you need to make any changes before installing the management server files. Once you click the Install button, the Oracle installation for the management server begins and the Command Prompt window is displayed showing the status of the Oracle installation. The management server installer Status screen is displayed in the background.

If you click **Cancel** during the installation, the installer completes the installation of the current component before stopping. Once the component installation is complete, the installer prompts you to confirm that you want to cancel. Click **Yes** to cancel or **No** to continue with the installation. If you choose to cancel the installation after the Oracle database has been installed, you must remove the Oracle database using the Oracle scripts or future installation of the management server will fail. See “Uninstalling Oracle Using the Oracle Scripts” on page 451.

---

**Caution** – The CIM extension files are copied to the management server so that you can install the extensions on the hosts in your network at a later time. The CIM extensions are not installed, only copied to the management server during this installation.

---

If you are installing the management server from the CD set, you are prompted to insert the CDs in the required order of installation indicated by the installer screens.

8. Click **Next** when all components are installed. The Installation Complete screen is displayed.
9. If you see a Unique Client ID number on the Installation Complete screen, copy the number and complete “Step 3 –” on page 93.

If your product allows honorary licensing, you will not see the Unique Client ID in which case, you must select the restart the management server option and click **Done**.

## Step 3 –

See your product invoice for important information about licensing. If you are required to import a license, copy your Unique Client ID number and follow the instructions in your product invoice documentation to obtain and apply your license key. If your product provides honorary licensing you do not see a Unique client ID, skip this step and continue to “Step 4 – Check for Required Service Packs and Hot Fix Files” on page 94.

## Step 4 – Check for Required Service Packs and Hot Fix Files

Check with your Sales Engineer to obtain and install the latest required service packs and hot fix files.

## Step 5 – Install Your CIM Extensions and Set Up Discovery

Before you can discover elements (systems) on your network, you must install the CIM extensions that were copied to the management server during the installation. See the following chapters:

See “Deploying and Managing CIM Extensions” on page 203.

See “Discovery Steps” on page 120.

---

# Upgrading the Windows Management Server

This section provides details about upgrading the management server.

## Keep in Mind the Following

- Before upgrading, verify that the server meets the requirements listed in the “Pre-installation Checklist (Installations and Upgrades)” on page 86.
- Refer to the release notes for upgrade path and late breaking information about upgrading the management server. See the Upgrade section in the release notes.
- 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.

## Considerations Before Upgrading

Before you upgrade, consider the following:

- **Brocade SMI-S Switches**

The Brocade switch manufacturer no longer supports the Brocade Fabric Access API provider and with this release of the management server, the Brocade Fabric Access API provider is no longer supported. After upgrading, any Brocade

switches that are managed by the Brocade API provider will be quarantined. Historical data will be retained by the API-managed Brocade switches, but you will not be able to run Get Details on these switches until they are migrated to the Brocade SMI-S provider (called the SMI-Agent in the Brocade documentation). Data such as topology and zoning from the Brocade switch will be stale and you will be unable to use the Brocade switch to perform provisioning or to gather port performance statistics through the Brocade switch.

Before the Brocade API-managed switches can be migrated to SMI-S, you must first download, install, and configure the Brocade SMI-S provider on the management server. For details on downloading, installing, and configuring the Brocade SMI-A agent provider, see “Migrate Your Brocade Switches to SMI-A” on page 107.

- **CIM Extensions**

The latest build of the management server requires you to upgrade some of your CIM extensions. Please refer to “About Upgrading Your CIM Extensions” on page 213 for details.

- After you upgrade the management server, you are required to run Get Details on all new and existing managed elements. This allows the software to gather any new data that is associated with the new features available in the latest release.

- **Windows hosts using SecurePath**

SecurePath information is not retrieved from legacy CIM extensions.

- **Backup Manager Hosts**

After you upgrade, you need to rediscover backup details. Make note of your Backup Manager hosts. Refer to Managing Backups in the user guide for help with viewing a list of Backup hosts.

- The following elements are not supported even though they were supported in Service Pack 4, Build 5.1 of the management server:
  - Cisco switches with firmware versions earlier than 3.1.x for switches discovered through SMI-S. You need to upgrade to version 3.2.(2c) if you want to discover the Cisco switches through SMI-S.
  - Brocade SMI-A versions prior to 120.6.0a. You need to upgrade to at least version 120.6.0a.

- **Oracle Upgrade**

This release of the management server is only compatible with Oracle 10g Standard Edition. During the upgrade process, Oracle 9i is automatically removed from the management server and Oracle 10g is automatically installed. Because Oracle 9i is removed during the upgrade to Oracle 10g, any customized Oracle passwords must be reset to the defaults. After the upgrade is successful it is strongly recommended that you change the Oracle passwords from the defaults using the Database Admin utility. See Database Passwords in the user guide for more information.

---

**Caution** – Oracle passwords will be reset to their default values.

---

- Windows 2000 is no longer supported. See the support matrix for complete information on supported Windows versions.
- After upgrading, hosts are managed directly from the application server, and will no longer be managed by our internal CIMOMs. Each host will be treated as its own discovery group; hosts will no longer be members of the built-in discovery groups (default, discovery group 1, etc). See “Upgrades only: Migrating a Schedule” on page 169 for more information.
- CLI clients earlier than the current revision are not supported.
- Any customizations to your CIMOMConfig.xml will not be preserved, because the file format has changed. The old file will be saved to <installation directory>\SavedData for reference. The customizations in the old CIMOMConfig.xml file must be manually merged into the file shipped with 6.0 and you must restart the management server before the customizations are applied to the updated management server.

■ **Files backed up to %MGR\_DIST%\SavedData**

The upgrade will save data to %MGR\_DIST%\SavedData. Do not delete this directory.

## About the Windows Upgrade Wizard

---

**Caution** – Do not install the oracle database separately.

---

You must use the installation wizard developed for installing the management server to install/upgrade the Oracle database. Installing the Oracle database separately is not recommended with this release of the management server.

## About Migrating Brocade Fabric Access API-Managed Switches to SMI-S After Upgrading

As noted earlier, The Brocade switch manufacturer no longer supports the Brocade Fabric Access API provider and the Fabric Access API provider is no longer supported with this release of the management server. Any Brocade switches that are managed with the Brocade Fabric Access API provider will be quarantined after upgrading the management server. The management server retains the data for the API switches after upgrading, but you cannot complete Get Details until you

migrate these Brocade switches to the Brocade SMI Agent provider. See “Migrate Your Brocade Switches to SMI-A” on page 107 for instructions on downloading and installing the Brocade SMI-A provider.

## About Resetting Archive Mode After Upgrading If You Use Automatic RMAN Backups

After upgrading to Oracle 10g, your Archive mode setting in the Database Admin Utility is reset to the default setting (No Archive Mode). If ARCHIVE MODE was enabled before upgrading, you must access the Database Admin Utility and re-enable Archive Mode in order to continue automatic RMAN backups. See the User Guide in the Documentation Center (**Help > Documentation Center**) for the steps.

## About CIM Extensions and Backup Manager Hosts After Upgrading

Upgrade CIM extensions on servers with the following functionality:

- **Backup Manager Hosts** – Backup information is not gathered from legacy CIM extensions. In order for backup information to be gathered by the management server, the CIM extensions on the Backup Manager Host must be at the same build number as the management server.

When you upgrade your management server, upgrade the CIM extensions on your Backup Manager Host in order to continue to see backup data.

- **Windows hosts using SecurePath** – SecurePath information is not retrieved from legacy CIM extensions.

After successfully upgrading the management server, any Brocade switches that use the Brocade Fabric Access API provider must be migrated to the Brocade SMI-A provider. The management server will prompt you to migrate your Brocade switches the first time you log on to the management server after the upgrade and will display the Brocade API switches that need to be migrated.

Until you migrate your Brocade switches to SMI-A, data such as topology and zoning from the Brocade switch will be stale and you will be unable to use the Brocade switch to perform provisioning or gather port performance statistics through the Brocade switch. The Brocade Fabric Access API switches are quarantined and you will have the option to migrate to the Brocade SMI-A provider at your discretion in case your SAN policy requires that you validate the new Brocade SMI Agent provider before migrating your Brocade switches.

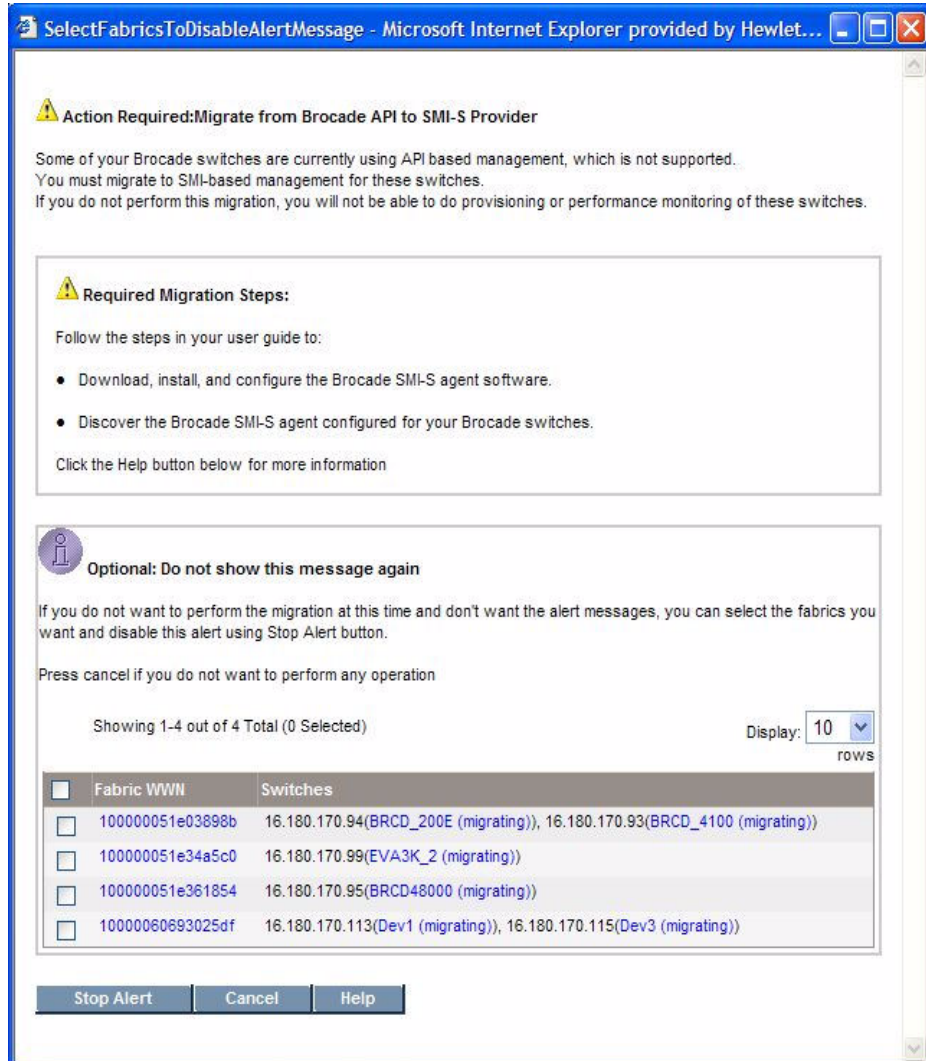
The quarantined API-managed Brocade switches retain their historical data and that data remains intact during the migration to the SMI-A provider.

After migrating the Brocade switches to SMI-A, the Brocade SMI-A proxy server is placed in its own discovery group. This new discovery group is not part of any Get Details schedule. If the Brocade switches were part of a Get Details schedule prior to migration, you must manually adjust those schedules to run Get Details for the migrated Brocade switches. If the schedules are not adjusted manually, Get Details will not run for the migrated switches as per pre-migration schedules.

However, new data will not be collected for the quarantined Brocade switches until you migrate the switches to the SMI-A provider. Follow these steps to migrate your Brocade switches to the Brocade SMI-A provider:

1. Download the Brocade SMI Agent v120.6.0a provider software and its Installation Guide from the Brocade website:  
<http://www.brocade.com/support/SMIAGENT.jsp>  
See the support matrix for your edition for details on the latest supported version for the management server.
2. Install the Brocade SMI Agent with a minimum version of 120.6.0a and configure the proxy servers on the server with which you will manage your Brocade access points following the installation and configuration instructions included in the Brocade v120.6.0a Installation Guide. Refer to the Brocade document for SMI-A requirements.

3. Log on to the management server. The management server alerts you to migrate your Brocade Fabric Access API switches when you first log on.




Your Brocade switches are quarantined until you migrate to the SMI-A provider. The migration message is displayed each time you log on to the management server until each Brocade switch is migrated to the new Brocade SMI-A provider or you choose to disable the message.

4. Run Discovery Step 1 for the Brocade proxy server. See the chapter, "Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries."

5. Run Get Details. See the chapter, “Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries.”

The Brocade switches are migrated to the SMI-A provider.

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

6. If you were using discovery schedules to collect details for Brocade switches prior to migrating them to SMI-A, add the new discovery group for the Brocade proxy server to your pre-existing Get Details schedules as described in the following steps:
  - a. Access the Discovery page by selecting **Configuration > Discovery**.
  - b. Click the **Edit** () button corresponding to the discovery schedule you want to modify.
  - c. Click the **Discovery Groups** tab.
  - d. Select the Brocade proxy under the list of discovery groups.
  - e. Click **Add Selected Groups To Schedule**.
  - f. Click **Finish**.

## Upgrading the Management Server for Windows

### Important Upgrade Requirements

- Do not upgrade Oracle separately. The upgrade steps have changed with this release of the product. The upgrade wizard migrates and upgrades the Oracle database automatically. Be sure to start the upgrade with the management server CD-ROM (not the Oracle DVD).
- Exit all external utilities that use Oracle before starting the upgrade wizard.

### Step 1 – Read the Support Matrix and Release Notes

Read the support matrix to make sure the servers on which you are upgrading the management server meet or exceed the requirements. Management server requirements are listed on the Mgr platform tab of the support matrix. Also read the release notes for late breaking issues not covered in the installation guide. The release notes and support matrix can be found on the top-level of the management server CD and the CIM extension CDs. Additionally, see “Installation and Upgrade Requirements (Cannot Proceed with Install/Upgrade if Not Met)” on page 87.



## Step 2 – Verify that You are Running Build 5.1 Service Pack 4 or a Later Build 5.1 Service Pack

Verify that you have a working version of the Build 5.1 SP4 management server before upgrading to Build 6.0. Existing installations that are at Build 5.1 SP1, Build 5.1 SP2, or Build 5.1 SP3 must upgrade to Build 5.1 SP4 or later before upgrading to Build 6.0.

## Step 3 – Save Configuration Files for the Global Change Management Business Tool

Make a copy of the configuration files saved through the Global Change Management Business Tool. The configuration files are not retained after you upgrade the product. These files are located in the advisors/saved-configuration area on the management server. Place these files back after the upgrade or re-install. If you do not use Global Change Management or do not wish to keep the old configurations, you can ignore this step.

## Step 4 – Manually Export the Database

Manually export the database and create an image of the server.

Export the database and create an image as described in the following steps.

---

**Caution** – Make sure you save the backup in a directory structure that is not part of the management server installation directory.

---

1. Stop the service for AppStorManager before you run the Database Admin Utility.
2. Use the Database Admin Utility to export your Oracle database. See “Database Maintenance and Management” on page 263.

As a best practice it is highly recommended that you backup the management server to create a restorable image of the server using the backup tool of your choice.

## Step 5 – Start the Upgrade Wizard

1. Exit all external utilities that use Oracle before starting the upgrade wizard.

2. Put the Windows Management Server installation CD in the CD-ROM drive of the management server. The installer starts automatically and the Welcome screen is displayed.
3. Click **Next**. The System Inspection screen is displayed briefly while the installer scans your system and determines that you are upgrading. As long as the system requirements are met, the Getting Started with an Upgrade screen is displayed.

---

**Caution** – The upgrade wizard stops AppStorManager, the service for the management server host, even if you cancel the upgrade program without making any changes. Restart the service after cancelling setup.exe to bring your system back to an operational state.

---

The following checks are performed before the install wizard starts. If any of these checks fail, the install wizard will not start until the requirement is met. See “Pre-installation Checklist (Installations and Upgrades)” on page 86 and the support matrix (**Documentation** > **Support Matrix** accessible from any install wizard screen) for more details on the requirements:

- Only one instance of the installer can be running.
  - Screen resolution is less than 800x600 pixels.
  - You are logged into the machine without administrator privileges.
  - The server is running a non-supported operating system. Refer to the support matrix for a valid operating system.
  - Microsoft Internet Explorer is version 6.0 or earlier. Internet Explorer version 6.0 SP1 or later is required.
  - TCP/IP is not installed.
  - Insufficient disk space in %Temp% is detected. You must have at least 2 GB of free disk space on the drive where %temp% is located.
4. Read the overview information on the Getting Started with an Upgrade screen and click **Next**. The Upgrade Locations screen is displayed showing the directories in which the management server components are currently installed.
  5. Optional. Select the check box to copy your CIM extensions installers to the management server only if you want to overwrite the existing CIM extension files on extensions from the CIM Extension CD manually to the management server at a later time. Note that this option only copies the CIM extension files to the management server. It does not install the CIM extensions on your hosts.

---

**Caution** – The 6.0 CIM extensions are required on any backup manager hosts to continue collecting backup manager discovery data. Build 5.1 CIM extensions on backup manager hosts are not supported after upgrading. See “Deploying and Managing CIM Extensions” on page 203 for information on installing CIM extensions.

---

6. Optional. You can change the location of the Oracle database.
7. Click **Next** to continue. The Verify System Requirements screen is displayed. See the support matrix for complete system requirement details.

---

**Note** – The Port Availability requirement line may show a warning during an upgrade that can be ignored, as it indicates that the existing management server service has reserved the ports.

---

8. Click **Next**. The Upgrade Summary screen is displayed showing the selected components to be upgraded.
9. Click **Upgrade** to continue or **Previous** to make changes to the previous screen or **Cancel** if you need to make changes to the server. Once you click **Upgrade**, the installer begins migrating the Oracle database and will not allow you to cancel until the migration is complete. The automated Oracle database migration creates a backup of your Oracle 9i database, exports the database, installs Oracle 10g Standard Edition, and imports the database during the upgrade. You can cancel the upgrade once the database migration is complete if desired.

If you click **Cancel** during the installation, the installer completes the installation of the current component before stopping. Once the component installation is complete, the installer prompts you to confirm that you want to cancel. Click **Yes** to cancel or **No** to continue with the installation.

The Installation Complete screen is displayed when the installer completes upgrading each component.

---

**Note** – If you specified any customized changes using the **Product Health > Advanced** option in a prior release, a record of those changes is saved in the `%mgr_dist%\logs\custom.txt` file after upgrading.

---

10. Click **Finish** to reboot the management server.

## Step 6 – Customize Database Passwords

The database passwords are reset during the upgrade. Use the Database Admin Utility to customize your database passwords.

During the upgrade, all Oracle passwords are reset to their defaults, including the TNS listener password, and the passwords for the SYS, SYSTEM, DB\_SYSTEM\_USER, RMAN\_USER accounts. Please use the Database Admin Utility to change these passwords after upgrading.

## Step 7 – Enable RMAN Backup if Desired

RMAN Backup is disabled by default as part of the upgrade process. When you log into the management server after upgrading, you see a message informing you that RMAN Backup is disabled. You should re-enable RMAN backup as soon as possible to continue backing up your data.

## Step 8 – Upgrade Select CIM Extensions

Upgrade CIM extensions on servers with the following functionality:

- Backup Manager Hosts—Backup information is not gathered from legacy CIM extensions. In order for backup information to be gathered by the management server, the CIM extensions on the Backup Manager Hosts must be at the same build number as the management server. When you upgrade your management server, upgrade the CIM extensions on your Backup Manager Host in order to continue to see backup data.
- Windows hosts using SecurePath—SecurePath information is not retrieved from legacy CIM extensions.
- \*Host that you want to retrieve cluster information for example: Veritas Cluster Server on Solaris cluster and Microsoft Cluster Server
- \*Linux hosts that support QLogic failover

\*This is new functionality that requires Build 6.0 of the CIM extension.

## Step 9 – Rediscover all Elements

You should rediscover all elements after you do an upgrade by running Get Details.

Discovery is important because:

- Better scalability is provided after discovery.
- Cluster functionality. To use the new functionality, upgrade the CIM extensions to Build 6.0 and rediscovery is required.
- You will see the following issues until you do Discovery:

- Reports and Capacity Manager/Capacity Explorer show incorrect raw capacity data for storage systems.
- There is no trunked status indication on Brocade fabrics.
- No NPIV status indication.
- No provisioning for 3PAR storage systems and HP StorageWorks EVA arrays using Command View EVA.
- New host modes on storage systems are not available.
- Backup data collection would be suspended until CIM extensions on Backup Manager Hosts are upgraded to Build 6.0 and they are rediscovered.

## Steps That Can be Run Anytime After the Upgrade

The following steps can be completed any time after the upgrade; however, you will have reduced functionality with the product until you complete these steps.

### Re-add Remote Sites in Global Reporter

---

**Caution** – After the upgrade, all remote sites in the Global Reporters are removed. This is done so you can upgrade the remote sites to the same version before Global Reporter attempts to gather data. Before you re-add the remote sites, be sure to upgrade them to the same build number as the management server (Build 6.0 CIM extensions).

---

All sites that provide global reports must be upgraded to the latest build of the management server. Install this build 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, click the Global Reporter tab 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 upgrade the database with data from the added sites, click the **Refresh Now** button at the bottom of the page.

## Upgrade your CLI Clients

CLI clients earlier than Build 6.0 do not work with Build 6.0 of the management server. Refer to the CLI Guide for more information about upgrading your CLI clients.

## Upgrading your CIM Extensions

See “About Upgrading Your CIM Extensions” on page 213 " for details.

## Migrate Your Brocade Switches to SMI-A

After successfully upgrading the management server, any Brocade switches that use the Brocade Fabric Access API provider must be migrated to the Brocade SMI-A provider. The management server will prompt you to migrate your Brocade switches the first time you log on to the management server after the upgrade and will display the Brocade API switches that need to be migrated.

Until you migrate your Brocade switches to SMI-A, data such as topology and zoning from the Brocade switch will be stale and you will be unable to use the Brocade switch to perform provisioning or gather port performance statistics through the Brocade switch. The Brocade Fabric Access API switches are quarantined and you will have the option to migrate to the Brocade SMI-A provider at your discretion in case your SAN policy requires that you validate the new Brocade SMI Agent provider before migrating your Brocade switches.

The quarantined API-managed Brocade switches retain their historical data and that data remains intact during the migration to the SMI-A provider.

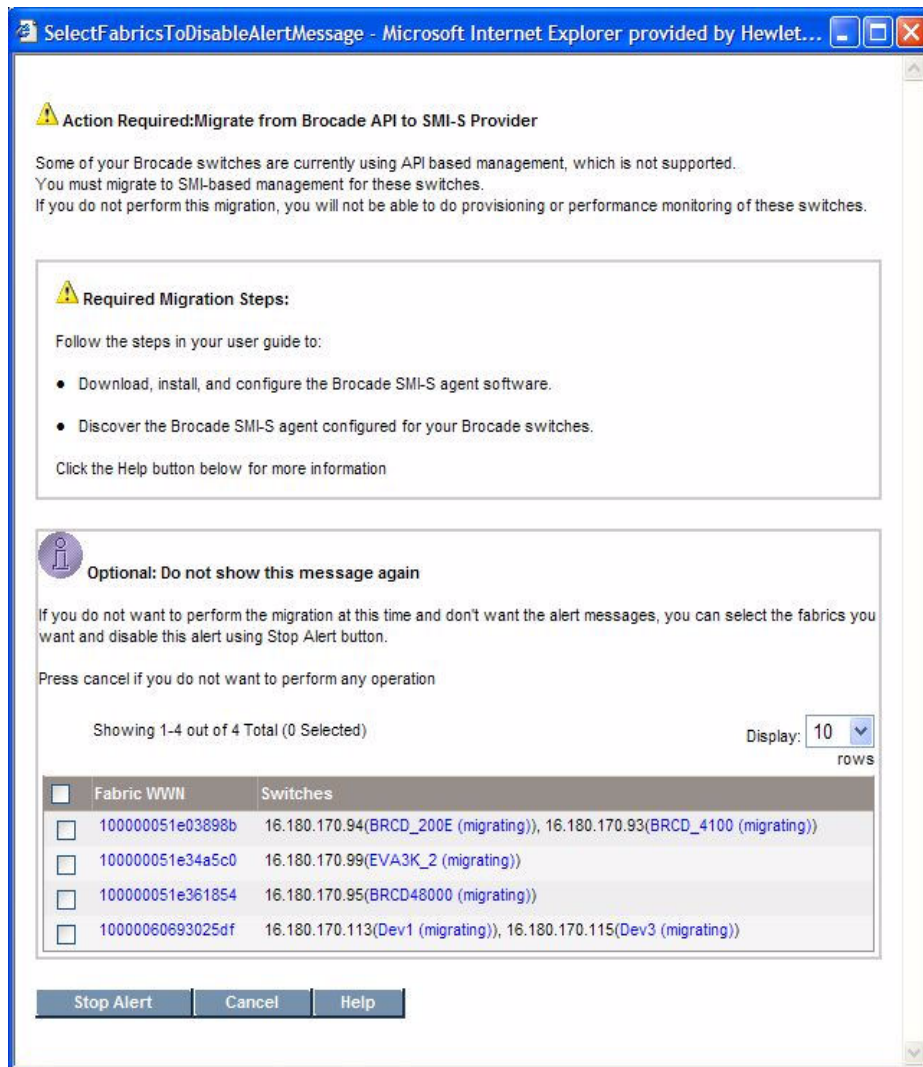
However, new data will not be collected for the quarantined Brocade switches until you migrate the switches to the SMI-A provider.

After migrating the Brocade switches to SMI-A, the Brocade SMI-A proxy server is placed in its own discovery group. This new discovery group is not part of any Get Details schedule. If the Brocade switches were part of a Get Details schedule prior to migration, you must manually adjust those schedules to run Get Details for the migrated Brocade switches. If the schedules are not adjusted manually, Get Details will not run for the migrated switches as per pre-migration schedules.

Follow these steps to migrate your Brocade switches to the Brocade SMI-A provider:

1. Download the Brocade SMI Agent v120.6.0a provider software and its Installation Guide from the Brocade website:  
<http://www.brocade.com/support/SMIAGENT.jsp>  
See the support matrix for your edition for details on the latest supported version for the management server.
2. Install the Brocade SMI Agent with a minimum version of 120.6.0a and configure the proxy servers on the server with which you will manage your Brocade access points following the installation and configuration instructions included in the Brocade v120.6.0a Installation Guide. Refer to the Brocade document for SMI-A requirements.

- Log on to the management server. The management server alerts you to migrate your Brocade Fabric Access API switches when you first log on.




Your Brocade switches are quarantined until you migrate to the SMI-A provider. The migration message is displayed each time you log on to the management server until each Brocade switch is migrated to the new Brocade SMI-A provider or you choose to disable the message.

- Run Discovery Step 1 for the Brocade proxy server. See the chapter, "Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries."



5. Run Get Details. See the chapter, “Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries.”  
The Brocade switches are migrated to the SMI-A provider.

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

6. If you were using discovery schedules to collect details for Brocade switches prior to migrating them to SMI-A, add the new discovery group for the Brocade proxy server to your pre-existing Get Details schedules as described in the following steps:
  - a. Access the Discovery page by selecting **Configuration > Discovery**.
  - b. Click the **Edit** () button corresponding to the discovery schedule you want to modify.
  - c. Click the **Discovery Groups** tab.
  - d. Select the Brocade proxy under the list of discovery groups.
  - e. Click **Add Selected Groups To Schedule**.
  - f. Click **Finish**.

## Check any McDATA and Connectrix Switches

As mentioned earlier, by default after upgrading, the management server is configured to use the SMI-S provider to manage and discover McDATA and Connectrix switches. The migration to SMI-S is not required for McDATA and Connectrix switches as it is with the Brocade Fabric Access API provider.

You must do one of the following after upgrading:

- Before you can discover McDATA and Connectrix switches with SMI-S, you must download and install the McDATA SMI-S provider software. See your switch documentation for more information.
- See the following section to change the default from SMI-S:  
“Changing the Discovery Settings” on page 150

---

# 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.

In Navisphere add the following to the privilege user section:

```
root@name_of_my_management_server
```

```
root@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

The management server service needs to be restarted after installing EMC Navisphere CLI.

## Removing the Management Server

Follow these steps to remove the management server and Oracle.

To remove the management server:

1. Stop the service for the management server by doing the following:
  - a. Go to the Services window (**Start > 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 or Remove Programs window (**Control Panel > Add or Remove Programs**).
3. Do the following to uninstall the management server:

- a. In the Add or Remove Programs window, select the management server.
  - b. Click the **Change/Remove** button. The Uninstall wizard starts.
  - c. In the Uninstall wizard screen, select the **Remove** option, then click **Next**.
  - d. Click **Uninstall**. The Uninstall Complete screen is displayed.
  - e. Select **No, I will restart my system myself**.
  - f. Click **Done**.
4. Do the following to remove Oracle and the Oracle instance for the management server:
- a. Open a Command Prompt window on the management server (**Start > Run > cmd.exe**, click **OK**).
  - b. Put the Oracle DVD in the DVD drive of the management server.
  - c. Change directory (CD) to the root of the Oracle DVD.
  - d. Enter the following at the command prompt window on the management server to remove Oracle and the management server database instance:  

```
cscript removeOracle10g.vbs
```

Oracle is removed from the management server.
5. Delete the old management server installation directory. If the directory is set with Read Only permissions do the following:
- a. Right-click the directory and select **Properties > Security**.
  - b. Highlight (click) **Administrator** and click **Full Control** under the **Allow** column.
  - c. Select the **General** tab and clear the **Read-only** check box.
  - d. Click **OK** and select **Apply changes to this folder, sub-folders and files** radio button.
  - e. Click **Ignore All** if you see an error message.
  - f. Delete the directory.
6. Delete the installation log files:
- `del %systemdrive%\srnInstsallLogs\*.log`
  - `del %windir%\srmwiz.ini`



## Managing Licenses

This chapter contains the following topics:

- “Modifying the License Summary Page” on page 117

The management server restricts the number of elements it manages through its license. It is important you keep your license up to date with the requirements of your network. The management server has several different types of license restrictions, as shown in Table 5-1, “License Restrictions,” on page 113.

**TABLE 5-1** License Restrictions

| Type of Restriction | Description                                                                                                                                                                                                                                                                                                                                | Unit of Measurement |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| MAPs                | The management software restricts the number of hardware elements it manages through the use of managed access points (MAPs) for hardware. A MAP is the sum of all storage access ports of all hardware elements that the management server manages. See Table 5-2, “Determining Managed Access Points,” on page 115 for more information. | Number of MAPs      |
| Backup Size         | The management server determines licensing for Protection Explorer through gigabytes (GB). The management server compares the number of gigabytes for Protection Explorer with what you are backing up. If you are backing up more than your license allows, you are warned the next time you log onto the management server.              | Gigabytes (GB)      |
| Raw NetApp Capacity | The Raw NetApp Capacity is the total disk capacity (unformatted capacity) of all discovered NetApp filers.                                                                                                                                                                                                                                 | Terabytes (TB)      |

**TABLE 5-1** License Restrictions

| Type of Restriction        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Unit of Measurement                                            |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| Managed Exchange Instances | The management server determines licensing for Microsoft Exchange instances by counting the number of instances of Microsoft Exchange it manages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Number of instances of Microsoft Exchange the software manages |
| Managed Database Instances | <p>The total number of instances of the following databases the software manages:</p> <ul style="list-style-type: none"> <li>• Microsoft SQL Server</li> <li>• Oracle</li> <li>• Sybase Adaptive Server Enterprise</li> <li>• InterSystems Caché</li> </ul> <p>This total is broken down by each type of database in the table.</p>                                                                                                                                                                                                                                                                                                  | Number of managed databases                                    |
| For File Server SRM        | <p>The management server determines licensing for File Server SRM through terabytes (TB). When you purchased File Server SRM, you were given a number of TB you were allowed by the management server to monitor.</p> <p>The management server detects the number of TB that are being monitored on file servers and verifies that number is at or below the purchased amount.</p> <p>You do not have to monitor everything associated with your file server. You can choose to manage only the mount points that are important to you. Only the files associated with these mount points are counted toward the file server TB.</p> | Terabytes (TB)                                                 |

---

**Caution** – The management server Current Usage Summary is first updated six hours after the management server (AppStorManager) starts, and then the updates occur every 24 hours thereafter. Elements the management server has discovered before the update are not reflected in the Current Usage Summary table. The time for the update is determined when the management server is first started. For example, the first update of the Current Usage Summary table occurs six hours after the management server is first started. The following updates occur every 24 hours.

If the management server is started for the first time at noon, the first update of the Current Usage Summary table would occur at 6 p.m. All following updates would always occur at 6 p.m.

---

MAPs are determined as described in Table 5-2, “Determining Managed Access Points,” on page 115.

**TABLE 5-2** Determining Managed Access Points

| Element         | Managed Access Point                                                                                                                                                                                                                                                                                                                          |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hosts           | The managed access points (MAPs) are the number of Fibre Channel ports with a minimum of one MAP. If a host has no Fibre Channel ports, the software assumes one MAP. The software does count direct attached storage, provided it is supported by the management server.                                                                     |
| Switches        | All ports on a switch are counted as MAPs.                                                                                                                                                                                                                                                                                                    |
| Storage systems | The MAPs are the sum of all front-facing ports. Storage systems with FA ports the software does not support, such as mainframe attached FICON, are still counted as MAPs. However, the management server does not count MAPs from storage systems it does not support. See the release notes for information about supported storage systems. |

**Example 1:**

Assume you have the following environment:

- Brocade (two switches of 12 ports each, one switch of 16 ports) — Total 40 ports
- McDATA (one switch of 64 ports) — Total 64 ports
- Windows 2000 and Solaris Hosts (10 hosts with two Fibre Channel connection each) — Total 20 ports
- EMC Subsystem (one subsystem with 16 Fibre Channel ports) — Total 16 ports

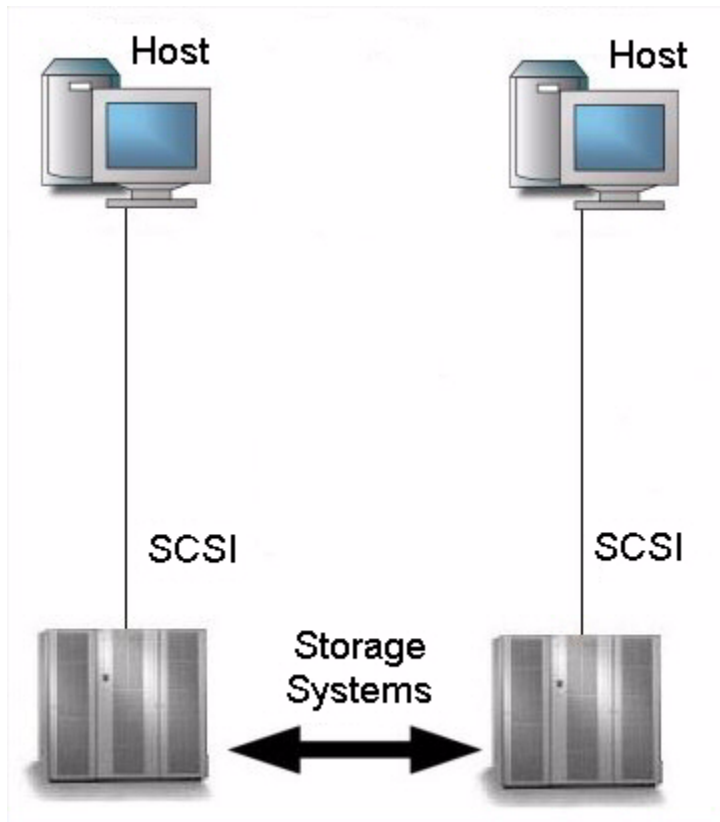
The software calculates 140 MAPs in this environment.

**Example 2:**

Assume you have the same configuration above, and you add several devices to your network that the management server does not support. There are still 140 MAPs in this environment, since the management server does not count the ports from devices it does not support.

**Example 3:**

Assume you have the same configuration as the first example, with two Windows 2000 hosts that are directly attached to storage systems, with no Fibre Channel (FC) connections and with a total of 0 FC ports, as shown in the following figure:



**FIGURE 5-1** An Example of Direct Attached Storage

The software calculates four MAPs (see the figure), since we assume one MAP for each host, even though it has no Fibre Channel ports. The storage systems are counted, since they are supported by the management server. If you include the MAPs from the first example (140 MAPs), it brings the total to 144 MAPs.

If we had a configuration which included a switch, two managed hosts, and several unmanaged hosts, the MAPs would not be used against the unmanaged hosts.

Some switches allow the user to turn off an unused GBIC. (Gigabit Interface Converter). If a GBIC is turned off, the port is not counted. However, if the GBIC is turned on, or if there is no GBIC, the port is counted.



---

# Modifying the License Summary Page

If you have purchased additional elements, you must modify the License Summary page. For example, assume you purchased an additional 200 MAPs, which lets you monitor 200 more devices, such as hosts, switches, and storage systems. To make the management server aware of these changes, you must enter the new total of MAPs you are licensed to use on the License Summary page.

---

**Caution** – Select only the applications you are licensed to access. Enter only the MAPs, terabytes and instances, you are authorized to use.

---

To modify the License Summary page:

1. Select **Security > Licenses**.
2. Select the applications you have recently purchased.
3. If you have added one or more of the following, add the amount you have purchased to the total listed.
  - MAPs
  - Gigabytes that will be backed up by Protection Explorer.
  - Terabytes that will be scanned by File SRM
  - Number of instances of each type of application you want to monitor.
4. Select **Save Changes**.
5. When you are shown the license agreement, accept the license if you agree with its terms.



## Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries

---

Before you can use the management server, you must execute the discovery process to make the software aware of the elements on your network, such as switches, storage systems, NAS devices, and tape libraries. Discovery obtains a list of discovered elements and information about their management interface and dependencies.

---

**Note** – The management server can discover only elements with a suitable management interface. Refer to the support matrix for information about supported hardware.

---

This chapter contains the following information:

- “Discovery Steps” on page 120
- “Overview of Discovery Features” on page 122
- “Discover Switches” on page 132
- “Discover Storage Systems, NAS Devices and Tape Libraries” on page 155
- “Building the Topology” on page 186
- “Get Details” on page 188
- “Using Discovery Groups” on page 190
- “Deleting Elements from the Product” on page 194
- “Working with Quarantined Elements” on page 196
- “Updating the Database with Element Changes” on page 197
- “Notifying the Software of a New Element” on page 199
- “Viewing Log Messages” on page 199
- “Viewing the Status of System Tasks” on page 200

---

# Discovery Steps

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

1. Discover your switches. See “Discover Switches” on page 132.
2. Discover your storage systems, tape libraries, and NAS devices. See “Discover Storage Systems, NAS Devices and Tape Libraries” on page 155.
3. If you want to view the topology quickly in System Explorer, obtain the topology as described in “Building the Topology” on page 186 (Optional). Keep in mind this step only gathers the information necessary for displaying the topology.
4. Perform Get Details. Get Details is required to obtain detailed information from the elements you discovered, including provisioning information. See “Get Details” on page 188.

---

**Note** – Running Get Details takes time. You might want to perform this process when the network and the managed elements are not busy. See “Get Details” on page 188 for more information.

---

## Overall Discovery Tasks

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

Before you begin the discovery process, note the following:

- Get Details does not default to an automatic schedule. In most cases, we recommend running Get Details once a day during off-peak hours. For more information, see “Get Details” on page 188.
- Make sure the credentials you enter are correct. When credentials are not supplied, the default user names and passwords are tried for the element.
- For elements that support multiple discovery protocols (for example, SNMP and SMI-S), only one protocol at a time is supported for a given element. If you want to change the protocol used to discover an element that has already been discovered, delete the element before attempting to rediscover it with a different protocol. For more information, see “Deleting Elements from the Product” on page 194.
- Elements discovered through SMI-S and hosts discovered with CIM extensions from Build 5.1 and later of the product cannot be added to discovery groups. These elements are listed separately and can be placed independently into

scheduled Get Details tasks without being part of a discovery group. This allows you greater flexibility when gathering discovery data. (For more information, see “Creating Custom Discovery Lists” on page 191).

- If you have a problem discovering an element, try enabling Troubleshooting Mode. For more information, see “Troubleshooting Mode” on page 467.
- 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.

---

**Note** – Since CIM extensions have not been installed yet, the management server will not be able to obtain this data when you perform discovery for elements. For more information, see “Deploying and Managing CIM Extensions” on page 203 and “Discovering Applications, Backup Hosts and Hosts” on page 345.

---

- 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. LSI 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 requires additional steps for discovery. See “Discovering EMC Solutions Enabler” on page 158 for more information.

The process for making the management server aware of the elements on your network consists of four stages:

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. For more information, see “Setting Default User Names and Passwords” on page 122.
2. Discover your switches. For information on how to discover the types of switches in your network, see “Discover Switches” on page 132.
3. Discover your storage systems, NAS devices and tape libraries. For more information, see Table 6-3, “Discovery Requirements for Storage Systems, Tape Libraries & NAS Devices,” on page 155.
4. Perform Get Details (**Discovery > Details**), which is required to obtain information from your discovered elements.

---

**Note** – Running Get Details takes time. You might want to perform this process when the network and the managed elements are not busy. See “Get Details” on page 188 for more information.

---

## Overview of Discovery Features

Discovery features allow you to:

- 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.
- Import or save discovery settings to a file.

This section contains the following topics:

- “Setting Default User Names and Passwords” on page 122
- “Adding an IP Range for Scanning” on page 125
- “Adding a Single IP Address or DNS Name for Discovery” on page 127
- “Modifying a Single IP Address Entry for Discovery” on page 128
- “Removing Elements from the Addresses to Discover List” on page 129
- “Importing Discovery Settings from a File” on page 129
- “Saving Discovery Settings to a File” on page 131

## 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 that 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.

---

**Caution** – 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, before you begin, 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 **Set Default User Name and Password**.

The Set Default User Name and Password pane appears (Figure 6-1, “Setting Default User Names and Passwords,” on page 124).

**Setting User Names and Passwords**

You can specify up to three user names and passwords. These user names and passwords are used during discovery if your IP Address does not have a user name and password specified.

If you are specifying a user name for a Windows host, prepend the user name with the Windows domain name.

For example: **mydomain\user**

|                  |                                        |
|------------------|----------------------------------------|
| User Name:       | <input type="text" value="admin"/>     |
| Password:        | <input type="password" value="•••••"/> |
| Verify Password: | <input type="password" value="•••••"/> |

|                  |                                           |
|------------------|-------------------------------------------|
| User Name:       | <input type="text" value="jsmith"/>       |
| Password:        | <input type="password" value="••••••••"/> |
| Verify Password: | <input type="password" value="••••••••"/> |

|                  |                                           |
|------------------|-------------------------------------------|
| User Name:       | <input type="text" value="pjones"/>       |
| Password:        | <input type="password" value="••••••••"/> |
| Verify Password: | <input type="password" value="••••••••"/> |

OK Cancel Help

**FIGURE 6-1** Setting Default User Names and Passwords

4. In the User Name box, enter the user name for one or more elements.
5. In the Password box, enter the corresponding password for the user name entered in the previous step.



6. In the Verify Password box, re-enter the password.
7. Repeat steps 4 through 6 for other default user names and passwords you want to add.
8. Click **Add System**.

## Adding an IP Range for Scanning

The management server can be set up so that when scanning, instead of adding each IP address individually the 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 a 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. For Microsoft Windows systems, the check the proxy service status 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 port 2001. The management server does not allow port numbers in the scanning of IP ranges, so you are not able to specify the port. For more information, see “Discovering HDS Storage Systems” on page 163.
- Enter a range within the same subnet. The management server cannot scan IP ranges across subnets.
- One way to detect multiple IP addresses at one time is to add an IP range for scanning. The management server scans the IP range for elements and populates the discovery list with the elements it could contact. You can then discover those elements.

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 **Add Range**.

The Add Range for Scanning pane appears (Figure 6-2, “Adding an IP Range for Scanning,” on page 126).

### Add Range for Scanning

If you are specifying a user name for a Windows host, you can prepend the user name with the Windows domain name.

For example, **mydomain\user**

|                   |                      |
|-------------------|----------------------|
| From IP Address:* | 192.168.1.2          |
| To IP Address:*   | 192.168.1.95         |
| User Name:        | admin                |
| Password:         | ••••                 |
| Verify Password:  | ••••                 |
| Comment:          | Servers in Marketing |

\* required fields

OK Cancel Help

**FIGURE 6-2** Adding an IP Range for Scanning

4. In the From IP Address box, enter a lowest IP address in the range to be scanned.
5. In the To IP Address box, enter the highest IP address in the range to be scanned.
6. In the User Name box (optional), enter a common user name for elements in the IP range.
7. In the Password box (optional), enter a common password for elements in the IP range.
8. In the Verify Password box, re-enter the password.
9. In the Comment box, enter a brief description of the servers; for example, "Servers in Marketing."
10. Click **OK** to close the Add Range for Scanning pane.
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

The following steps provide general information on how to discover an element. For more information, see Table 6-1, “Discovery Requirements for Switches,” on page 132, Table 6-3, “Discovery Requirements for Storage Systems, Tape Libraries & NAS Devices,” on page 155.

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 **Add Address**.
4. In the IP Address/DNS Name box, enter the IP address or DNS name of the device you want to discover.
5. In the User Name box (optional), enter the user name. This box can be left blank if you are discovering an LSI storage system or if the element's user name and password are one of the default user names and passwords.
6. To set the password, take one of the following actions:
  - If you do not want to do provisioning on a storage system, leave the Password box blank. For LSI storage systems, you must also select the **Do Not Authenticate** option.
  - If you want to do provisioning on a storage system, enter the corresponding password for controller or proxy and make sure the **Do Not Authenticate** option is not selected.
  - For all elements other than storage systems, provide the password if it is required for authentication. If the element does not require a password, leave the Password box blank.
7. If you entered a password in the previous step, re-enter the password in the Verify Password box.
8. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
9. Click **OK**.
10. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

# 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, if the password for a host was changed, you would need to update the management server database with the new password.

---

**Caution** – 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 **Edit** () button for the element whose user name and/or password you want to modify.
3. To change the user name, enter the new user name in the User Name box.
4. To add or change a comment, enter a comment in the Comment box.
5. To change the password:
  - a. Click **Change password**.
  - b. Enter the new password in the New Password box.
  - c. Enter the password again in the Verify Password box.
  - 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 **Get Topology**.

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, and then click **Delete**.
  - Click the **Delete** () button corresponding to the elements you want to remove from the Addresses to Discover list.

---

**Caution** – The elements associated with these addresses are not removed from the management server. For information about how to remove an element from the management server, see “Deleting Elements from the Product” on page 194.

---

## 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 allows you to import the following information to the Discovery list:

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

Note the following:

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

---

**Caution** – When you import a file, your previous settings are overwritten.

---

- If you receive an error message when you try to import the discovery settings, verify that you are using the right password. If you are using the correct password, there is a possibility that the file is corrupt.
- When you save the discovery settings to a file, the management server is not included in the list and you must rediscover the management server. For instructions, see “Importing a File” on page 130 and “Re-discovering the Management Server” on page 130.

## Importing 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 **Browse** to find the file.
  - In the Filename box, enter a complete path to the file.
4. In the Password box, enter the password for the discovery list. If the discovery list did not have a password assign to it, leave this field blank.
5. Click **OK**. The information on the following tabs is updated:
  - IP Addresses
  - IP Ranges
  - Applications
  - Windows Proxy tab

## Re-discovering the Management Server

1. Click **Discovery**, and then click **Setup** in the upper-right pane of the window.
2. Click the **Monitoring Product Health** link.

The Monitoring Product Health window appears.

3. Click **Add**.

The Discovery Setup, Step 1 - Setup page shows the management server as localhost.

4. Select the check box next to localhost and click **Start Discovery**.

When Step 1 discovery is finished, the management server is put into the default discovery group.

5. Select **Discovery > Details**.
6. Run **Get Details** for the discovery group that contains the `localhost` entry.

## 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 information:

- 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 box, enter the password for the management server.
5. In the Verify Password box, enter the password from the previous step, and then click **OK**.
6. When you are asked if you want to open or save the file, choose **Save**.

The Downloading window appears.

7. Enter a name for the \*.xml file and select the directory to which you want to save the file. The default name of the file is `DiscoverySettings.xml`.
8. In the Password box, provide a password for the discovery list.

---

**Note** – This password is required later when you import the file. Choose a password you will remember.

---

9. Click the **Save** button in the Save As window. The file is saved.

---

# Discover Switches

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

**TABLE 6-1** Discovery Requirements for Switches

| Element                                               | Discovery Requirements                                                                                                                                                   | Additional Information                                                                                    |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Brocade switches (SMI-S)                              | IP address or DNS name, and the user name and password from the Brocade SMI Agent security setup.                                                                        | See “Discovering Brocade Switches” on page 133.                                                           |
| CNT switches                                          | IP address and the port number for the InVsn Software that manages the switch and the user name and password.                                                            | See “Discovering CNT Switches” on page 137.                                                               |
| Cisco switches (SMI-S)                                | IP address/DNS name of the Cisco switch and the user name and password of the switch.                                                                                    | See “Discovering Cisco Switches” on page 138.                                                             |
| Cisco switches (SNMP)                                 | 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 138.                                                             |
| QLogic, and HP M-Series switches (SMI-S)              | Enter the IP address/DNS name of the SMI-S switch as well as the user name and password of the switch.                                                                   | See “Discovering Sun StorEdge, QLogic and HP StorageWorks M-Series for p-Class BladeSystems” on page 140. |
| Sun StorEdge, HP M-Series, and QLogic switches (SNMP) | IP address/DNS name of the Sun StorEdge, QLogic, or HP M-Series switch. Enter the SNMP read-only community string as the user name. You do not need to enter a password. | See “Discovering Sun StorEdge, QLogic and HP StorageWorks M-Series for p-Class BladeSystems” on page 140. |
| 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 142.                                         |

---

**Note** – If your Web browser has an option for blocking pop-ups, disable it. The management server uses pop-ups for dialog boxes.

---



# Discovering Brocade Switches

The management server uses the Brocade SMI-S Provider (also known as the Brocade SMI Agent) to discover Brocade switches. Before you can discover Brocade switches with SMI-S, however, you must first download and install the Brocade SMI Agent software. You can download the Brocade SMI Agent and documentation from the Brocade web site. For more information on Brocade SMI Agent versions, see the support matrix.

---

**Caution** – With this release, discovery of Brocade switches through the Fabric Access API is not supported. For information on migrating existing switches to SMI-S, see “Migrating Brocade API Switches to SMI-S After Upgrading” on page 133.

---

## Migrating Brocade API Switches to SMI-S After Upgrading

After successfully upgrading the management server, any Brocade switches that use the Brocade Fabric Access API provider must be migrated to the Brocade SMI-A provider. The management server will prompt you to migrate your Brocade switches the first time you log on to the management server after the upgrade and will display the Brocade API switches that need to be migrated.

Until you migrate your Brocade switches to SMI-A, data such as topology and zoning from the Brocade switch will be stale and you will be unable to use the Brocade switch to perform provisioning or gather port performance statistics through the Brocade switch. The Brocade Fabric Access API switches are quarantined and you will have the option to migrate to the Brocade SMI-A provider at your discretion in case your SAN policy requires that you validate the new Brocade SMI Agent provider before migrating your Brocade switches.

The quarantined API-managed Brocade switches retain their historical data and that data remains intact during the migration to the SMI-A provider.

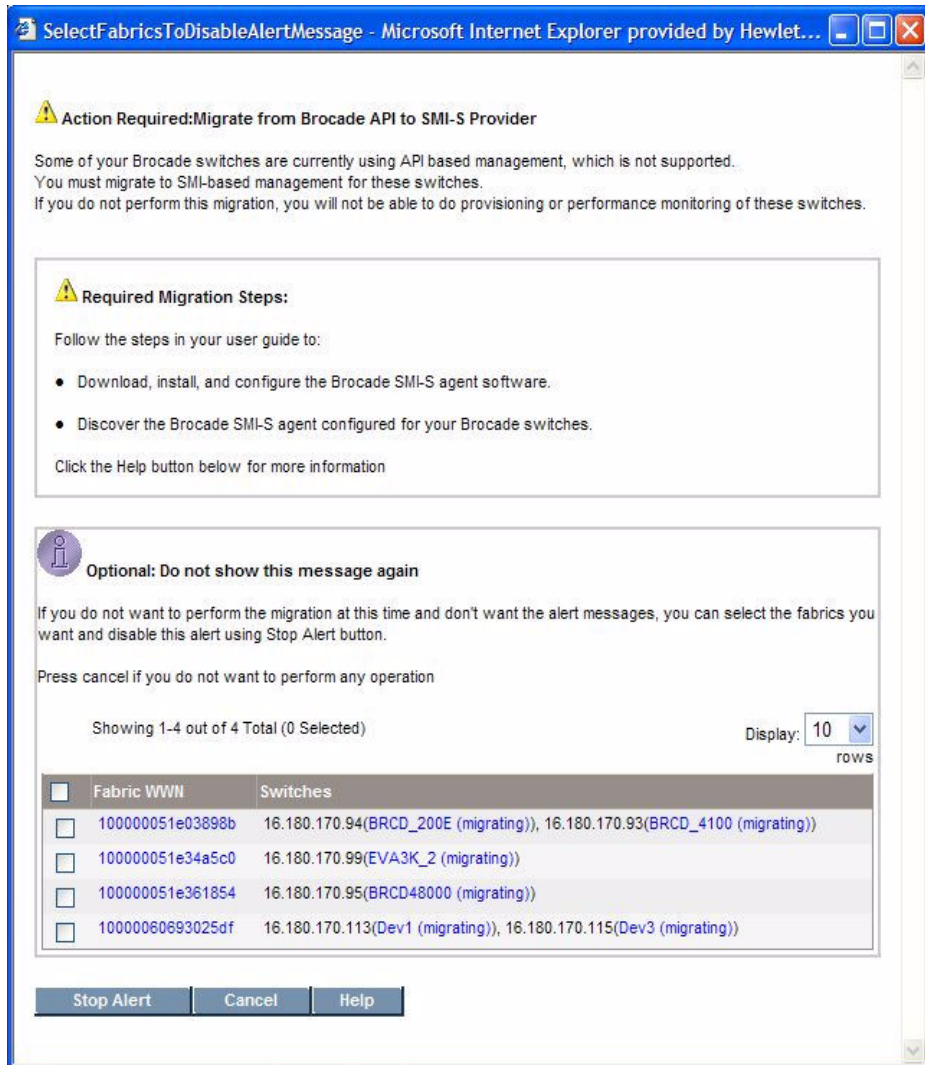
However, new data will not be collected for the quarantined Brocade switches until you migrate the switches to the SMI-A provider.

After migrating the Brocade switches to SMI-A, the Brocade SMI-A proxy server is placed in its own discovery group. This new discovery group is not part of any Get Details schedule. If the Brocade switches were part of a Get Details schedule prior to migration, you must manually adjust those schedules to run Get Details for the migrated Brocade switches. If the schedules are not adjusted manually, Get Details will not run for the migrated switches as per pre-migration schedules.

Follow these steps to migrate your Brocade switches to the Brocade SMI-A provider:

1. Download the Brocade SMI Agent v120.6.0a provider software and its Installation Guide from the Brocade website:  
<http://www.brocade.com/support/SMIAGENT.jsp>  
See the support matrix for your edition for details on the latest supported version for the management server.
2. Install the Brocade SMI Agent with a minimum version of 120.6.0a and configure the proxy servers on the server with which you will manage your Brocade access points following the installation and configuration instructions included in the Brocade v120.6.0a Installation Guide. Refer to the Brocade document for SMI-A requirements.

3. Log on to the management server. The management server alerts you to migrate your Brocade Fabric Access API switches when you first log on.




Your Brocade switches are quarantined until you migrate to the SMI-A provider. The migration message is displayed each time you log on to the management server until each Brocade switch is migrated to the new Brocade SMI-A provider or you choose to disable the message.

4. Run Discovery Step 1 for the Brocade proxy server. See the chapter, "Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries."

5. Run Get Details. See the chapter, “Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries.”

The Brocade switches are migrated to the SMI-A provider.

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

6. If you were using discovery schedules to collect details for Brocade switches prior to migrating them to SMI-A, add the new discovery group for the Brocade proxy server to your pre-existing Get Details schedules as described in the following steps:
  - a. Access the Discovery page by selecting **Configuration > Discovery**.
  - b. Click the **Edit** () button corresponding to the discovery schedule you want to modify.
  - c. Click the **Discovery Groups** tab.
  - d. Select the Brocade proxy under the list of discovery groups.
  - e. Click **Add Selected Groups To Schedule**.
  - f. Click **Finish**.

## To Discover Brocade SMI-S Switches

1. Click **Discovery**, and 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 **Add Address**.
5. In the IP Address/DNS Name box, enter the IP address of the proxy server that is running the SMI-S agent. (Some proxy servers require the following format:  
`http://IPADDRESS.`)
6. In the User Name box, enter the user name for the SMI-S proxy server.

This box 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 box, enter the password for the SMI-S proxy server.

This box 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.
8. If you entered a password in the previous step, re-enter the password in the Verify Password box.
  9. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
  10. Do not select the **Do Not Authenticate** option.
  11. Click **OK**.
  12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Discovering CNT Switches

The management server uses the CNT SMI-S provider to discover CNT switches. 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 support matrix for the required InVSN version for your switch model.

---

**Caution** – 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.

---

When discovering CNT switches, note the following:

- SNMP is not supported for CNT switches.
- 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. Take the following steps 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. Make the following entry in the file:  
`cimomenabled=TRUE`
  - c. Save the file, and then restart the InVsn software.
2. In the IP Address/DNS Name box, enter 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 box, enter the user name for the login to the InVsn software.
4. In the Password box, enter the password for the login to the InVsn software.
5. In the Verify Password box, enter the password you provided in step 4.
6. Click **Start Discovery**.

## Discovering Cisco Switches

The management server discovers Cisco switches through SNMP and SMI-S connections depending on the switch model. See the support matrix for details on supported switch models and firmware revisions.

Note the following when discovering Cisco switches with SNMP:

- 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, which 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.
- No ports are reported for uninstalled blades or GBICs.
- To receive events from Cisco switches, verify that the SNMP trap community string is set to match the community string defined in the custom properties (the default is `public`), and make sure the SNMP traps are configured to be sent to

the management server. For more information, see “Changing the SNMP Trap Listener Port and Community String for Switches Discovered with SNMP” on page 155.

Note the following when discovering Cisco switches with SMI-S:

- Before you can discover Cisco switches with SMI-S, you must download and install the Cisco cimserver software. See your Cisco documentation for more information.
- Enable the CIM Server for Cisco switches discovered through the SMI-S provider.
  - a. On the Cisco switch, enter the following command to display the Common Information Models (CIM) configurations and settings:  
`cisco_switch# show cimserver`
  - b. To enter configuration mode, enter the following:  
`cisco_switch# config`
  - c. To enable access to the server, enter the following:  
`cisco_switch# cimserver enableHttps`  
And/or  
`cisco_switch# cimserver enableHttp`
  - d. To enable the CIM Server, enter the following:  
`cisco_switch(config)# cimserver enable`
  - e. To exit configuration mode, enter the following:  
`cisco_switch(config)# exit`
- When you discover a Cisco SMI-S switch you need to provide a user name and password.
- If you are using the SMI-S provider, discover all Cisco switches in a fabric. If you discover only one switch, inactive zones and zone sets residing on other switches are not displayed on the management server.

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 **Add Address**.
5. In the IP Address/DNS Name box, enter the DNS name or primary IP address of the Cisco switch you want to discover.
6. Take one of the following actions:

- For **Cisco** switches with SNMP connections:  
In the User Name box, enter the user name for the switch. This is the public community SNMP string for the switch. This box 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 box, enter the switch user name.
7. Take one of the following actions:
- For **Cisco** switches with SNMP connections:  
Leave the Password box blank.
  - For **Cisco** switches with SMI-S connections:  
In the Password box, enter the switch password.
8. Take one of the following actions:
- For **Cisco** switches with SNMP connections:  
Leave the Verify Password box blank.
  - For **Cisco** switches with SMI-S connections:  
In the Verify Password box, enter the switch password again.

## Discovering Sun StorEdge, QLogic and HP StorageWorks M-Series for p-Class BladeSystems

The management server discovers Sun StorEdge switches through an SNMP connection and QLogic and HP M-Series switches are discovered through SNMP or SMI-S. See the support matrix for details on supported switch models and firmware revisions.

Note the following when discovering these switches with SNMP:

- When you discover these switches, you do not need to provide a password.
- The management server does not support provisioning for Sun StorEdge, QLogic, and HP M-Series switches. Only the active zone set and its zone members are reported.
- To manage a fabric of Sun StorEdge, QLogic, or HP M-Series 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 switches is 162. To change this port, see "Changing the SNMP Trap Listener Port and Community String for Switches Discovered with SNMP" on page 155.
- To receive events from Sun StorEdge, QLogic, and HP M-Series switches, verify that the SNMP trap community string is set to match the community string defined in the custom properties (the default is `public`), and make sure the



SNMP traps are configured to be sent to the management server. For more information, see “Changing the SNMP Trap Listener Port and Community String for Switches Discovered with SNMP” on page 155.

Note the following when discovering these switches with SMI-S:

- Before you can discover these switches with SMI-S, you must download and install the cimserver software. See your switch documentation for more information.
- 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.

---

**Note** – You may see an error replicating the switch fabric name for QLogic-based switches. This error can be ignored.

---

To discover Sun StorEdge or QLogic switches:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the DNS name or primary IP address of the switch you want to discover.
6. Take one of the following actions:
  - For switches with SNMP connections:  
In the User Name box, enter the user name for the switch. This is the public community SNMP string for the switch. This box can be left blank if the element's user name and password are one of the default user names and passwords.
  - For switches with SMI-S connections:  
In the User Name box, enter the user name for this switch. All SMI-S switches require a user name and password.
7. Take one of the following actions:
  - For switches with SNMP connections:  
Leave the Password box blank.
  - For switches with SMI-S connections:  
In the Password box, enter the password for this switch.
8. Take one of the following actions:
  - For switches with SNMP connections:  
Leave the Verify Password box blank.

- For switches with SMI-S connections:  
In the Verify Password box, enter the password of the switch again.

## Discovering McDATA and EMC Connectrix Switches

McDATA and EMC Connectrix switches use SMI-S, the Fibre Channel Switch Application Programming Interface (SWAPI), or SNMP to communicate with devices on the network. The management server can discover multiple instances of Enterprise Fabric Connectivity (EFC) Manager. Use one of the following methods to discover McDATA and Connectrix switches:

**TABLE 6-2** Discovery Settings for McDATA and Connectrix Switches

| Method                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SMI-S Discovery</b>                | SMI-S is the default discovery method for new installations.<br>The SMI-S 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 and nicknames are not supported.                                                                                                                                                                                  |
| <b>SWAPI setting through a Proxy</b>  | You will need to connect through the proxy instead of the switch. For more information, see “Discovering McDATA and Connectrix Switches through a Proxy with SWAPI” on page 145.<br>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.                                                                                              |
| <b>SNMP setting Through a Proxy</b>   | 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. For more information, see “Discovering McDATA and Connectrix Switches through a Proxy with SNMP” on page 147.<br>This SNMP setting through a proxy does not let you manage or access information about zones, zone sets or zone aliases.                                                      |
| <b>Contacting the switch directly</b> | Contact the switch by its IP address or DNS name. This connection uses SNMP. See the support matrix for details on switch models ( <b>Help &gt; Documentation Center</b> ). For more information, see “Discovering McDATA and Connectrix Switches through a Direct Connection and SNMP” on page 148.<br>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. |

Keep in mind the following:

- SMI-S is the default method for discovering McDATA and Connectrix switches. If you need to migrate to SMI-S or change the discovery settings, see “Changing the Discovery Settings” on page 150.

- You can only choose one discovery method for McDATA and Connectrix switches. For example, if you use SMI-S, you cannot discover additional McDATA and Connectrix switches with SWAPI or SNMP.
- If you use EFC Manager or Connectrix Manager, see the support matrix to verify the version requirements.
- Brocade 5000ni switches running in McDATA mode are managed by the Brocade SMI Agent and not by McDATA SMI-S. For more information, see “Discovering Brocade Switches” on page 133.
- If you change the discovery settings, the user ID and password will no longer work. For this reason, set this property before discovering any McDATA or Connectrix switches. If you must change the configuration, see “Changing the Discovery Settings” on page 150.
- After you discover a McDATA or Connectrix switch through a proxy, the IP address displayed next to the name of the switch is 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 the 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 “Managing McDATA and EMC Connectrix Switches” on page 152.
- All McDATA or Connectrix switches in a fabric must be managed by the same EFC Manager or Connectrix Manager. Do not have more than one EFC Manager or Connectrix Manager to a fabric for McDATA or Connectrix switches.
- If you want the management server to receive SNMP traps 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 only on the Connectrix Manager or EFC Manager, not on the individual switches.
  - If you discovered Connectrix or McDATA switches directly, enable SNMP trap forwarding on the switches, not in any other management software.
- For more information about the SNMP port and community string, see “Changing the SNMP Trap Listener Port and Community String for Switches Discovered with SNMP” on page 155.

## Discovering McDATA and Connectrix switches with SMI-S

Before you can discover McDATA and Connectrix switches with SMI-S, you must download and install the McDATA SMI-S provider software. See your switch documentation for more information.

Note the following when discovering these switches with SMI-S:

- Before attempting to discover your switches, ensure that EFC Manager or Connectrix Manager is installed and configured or add your switches to the SMI-S provider.

- For upgrades only: To migrate your existing switches to SMI-S, follow the procedure in “Changing the Discovery Settings” on page 150.
- Discovering McDATA and Connectrix switches with SMI-S is the default setting. To view or change the discovery settings, see “Changing the Discovery Settings” on page 150.
- You can install only one instance of the SMI-S provider on the management station.
- Installation of the McDATA SMI-S provider is not supported on Linux systems.
- A McDATA or Connectrix switch cannot be managed by more than one SMI-S provider.
- When you install the SMI-S provider, there are two modes:
  - In coexist mode the SMI-S provider communicates with EFC Manager or Connectrix Manager and adds all the switches in the managed list of EFC Manager or Connectrix Manager.
  - In direct mode, you must add each switch to the SMI-S provider with its IP address, credentials and switch type. You can use a McDATA’s `manageswitch.bat` file to manage the addition and deletion of switches.
- If you selected direct mode during the SMI-S provider installation, when you add switches, you must enter the switch type based on the McDATA model number even if your switch is an OEM model. For more information about the switch type, see your McDATA documentation.
- The SMI-S provider can be installed on the same server as EFC Manager or Connectrix Manager.
- If you selected coexist mode during the SMI-S provider installation you can have only one EFC Manager or Connectrix Manager server.
- If you are using EFC Manager or Connectrix Manager you cannot add managed switches in direct mode. To add switches in direct mode you must remove them from EFC Manager or Connectrix Manager first.
- If the SMI-S provider is installed on a machine other than the management server, network links between them must pass http traffic on port 5988 (default) or https on port 5989. The port used by the SMI-S provider can be configured. See your switch documentation for more information.

To discover the proxy:

1. Select **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 **Add Address**.
5. In the IP Address/DNS Name box, enter the IP address or DNS name of the proxy you want to discover.
6. In the User Name box, enter the user name.
7. In the Password box, enter the password.

---

**Note** – The user name and password are defined during the SMI-S provider installation. These credentials might be different from the EFC Manager credentials.

---

8. Re-enter the password in the Verify Password box.
9. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.  
  
Discovery is complete when the software displays the DISCOVERY COMPLETED message in the Log Messages box.

---

**Caution** – 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 186 and “About Get Details” on page 188.

---

## Discovering McDATA and Connectrix Switches through a Proxy with SWAPI

With the SWAPI setting, the management server contacts a proxy to obtain information about the switches connected to it. Use EFC Manager or Connectrix Manager for this option. If you do not have EFC Manager or Connectrix Manager, see “Discovering McDATA and Connectrix Switches through a Direct Connection and SNMP” on page 148.

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.

---

**Caution** – EMC customers using the EMC Connectrix Manager (EMC’s rebranded EFC Manager) 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 it

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 cannot discover EMC Connectrix switches using SWAPI. You must discover them through the SNMP provider, either directly or through a proxy. For more information, see "Discovering McDATA and Connectrix Switches through a Proxy with SNMP" on page 147 and "Discovering McDATA and Connectrix Switches through a Direct Connection and SNMP" on page 148 .

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 Connectrix switches using SWAPI, you should check with your EMC or McDATA representative to determine the implications of this configuration.

---

1. For McDATA switches only, install the McDATA Bridge Agent. To communicate with EFC Manager, the management server requires the Bridge Agent. Consult your McDATA representative for more information about the Bridge Agent.
2. Change the discovery setting for McDATA and Connectrix switches to SWAPI following the steps in "Changing the Discovery Settings" on page 150.
3. Discover the Proxy:
  - a. Click **Discovery**, then click **Setup** in the upper-right pane of the window.
  - b. Select **Step 1** at the top of the page.
  - c. Click the **IP Addresses** tab.
  - d. Click **Add Address**.
  - e. In the IP Address/DNS Name box, enter the IP address or DNS name of the EFC Manager or Connectrix Manager you want to discover.
  - f. In the User Name box, enter the user name for EFC Manager or Connectrix Manager.

This box 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.

In the Password box, enter the corresponding password for EFC Manager or Connectrix Manager.

This box can be left blank if one or more of the following conditions is fulfilled:

The element's user name and password are one of the default user names and passwords.

The element does not require authentication.

- g. If you entered a password in the previous step, re-enter the password in the Verify Password box.
- h. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
- i. Click **OK**.
- j. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

Discovery is complete when the software displays the DISCOVERY COMPLETED message in the Log Messages box.

## Discovering McDATA and Connectrix Switches through a Proxy with SNMP

---

**Note** – Discovering McDATA or Connectrix switches through a proxy using the SNMP protocol does not let you manage or access information about zones, zone sets or zone aliases.

---

You can use this option with EMC Connectrix™ Manager and Enterprise Fabric Connectivity (EFC) Manager to contact the switch.

1. Change the discovery setting for McDATA and Connectrix switches to SNMP following the steps in “Changing the Discovery Settings” on page 150.
2. Discover the Proxy:
  - a. Select **Discovery**, then click **Setup** in the upper-right pane of the window.
  - b. Select **Step 1** at the top of the page.
  - c. Click the **IP Addresses** tab.
  - d. Click **Add Address**.
  - e. In the IP Address/DNS Name box, enter the IP address or DNS name of the proxy you want to discover.

- f. In the User Name box, enter 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.
- g. Leave the Password and Verify Password boxes blank. The password does not matter since the management server is not doing any configurations through SNMP.
- h. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
- i. Do not select the **Do Not Authenticate** option.
- j. Click **OK**.
- k. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

Discovery is complete when the software displays the DISCOVERY COMPLETED message in the Log Messages box.

---

**Caution** – 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 186 and “About Get Details” on page 188.

---

- 3. Make sure there are no port conflicts for receiving SNMP traps. When the management server is configured to contact the proxy by SNMP, it 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. For information about changing the port, see “Changing the SNMP Trap Listener Port and Community String for Switches Discovered with SNMP” on page 155.
- 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 from all switches managed by the proxy to the management server using the port you selected. For more information, see the documentation for your proxy.



## Discovering McDATA and Connectrix Switches through a Direct Connection and SNMP

The management server uses SMI-S or SWAPI to discover a McDATA or Connectrix switch through a proxy. If you want to discover McDATA or Connectrix switches directly, you must change the discovery settings to SNMP before you begin the following steps. See “Changing the Discovery Settings” on page 150. See the support matrix for McDATA switch details (**Help > Documentation Center**).

To discover a McDATA or Connectrix switch directly:

1. Make sure there are no port conflicts for receiving SNMP traps. When the management server is configured to contact the proxy by SNMP, it 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. For information about changing the port, see “Changing the SNMP Trap Listener Port and Community String for Switches Discovered with SNMP” on page 155.
2. 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 then sends traps from all switches managed by that proxy. See the proxy documentation for more information.
3. Select **Discovery**, then click **Setup** in the upper-right pane of the window.
4. Select **Step 1** at the top of the page.
5. Click the **IP Addresses** tab.
6. Click **Add Address**.
7. In the IP Address/DNS Name box, enter the IP address or DNS name of the switch you want to discover.
8. In the User Name box, enter 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.
9. If you are using SNMP leave the Password box (optional) blank. The password does not matter since the management server is not doing any configurations through SNMP. If you are using SMI-S enter the password of the admin account on the switch.
10. In the Verify Password box enter the same thing you entered in the password box.

11. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
12. Do not select the **Do Not Authenticate** option.
13. Click **OK**.
14. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.  
  
Discovery is complete when the software displays the `DISCOVERY COMPLETED` message in the Log Messages box.

---

**Caution** – 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 186 and “About Get Details” on page 188.

---

## Changing the Discovery Settings

To change the discovery settings for McDATA and Connectrix switches:

1. If you have already discovered your switches, 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, and then click **Delete**.
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 **Delete**.
3. Select **Configuration** > **Product Health**, and then click **Advanced** in the **Disk Space** tree.
4. Click **Show Default Properties** at the bottom of the page.

To enable SNMP:

- a. Uncomment the `cimom.useSnmpMcDataProvider` property by removing the pound sign (#) in front of it.
- b. Change the `cimom.mcdata.dontUseSmis` property as follows:  
`cimom.mcdata.dontUseSmis=true`

---

**Note** – The `cimom.mcdata.dontUseSmis` property exists only in upgrade installations. If the property does not exist on your system, enter it manually.

---

To enable SWAPI:

- a. Comment out the `cimom.useSnmppMcDataProvider` property by placing a pound sign (#) in front of it.
- b. Change the `cimom.mcdata.dontUseSmis` property as follows:  
`cimom.mcdata.dontUseSmis=true`

---

**Note** – The `cimom.mcdata.dontUseSmis` property exists only in upgrade installations. If the property does not exist on your system, enter it manually.

---

To enable SMI-S:

- a. Comment out the `cimom.useSnmppMcDataProvider` property by placing a pound sign (#) in front of it.
  - b. Change the `cimom.mcdata.dontUseSmis` property as follows:  
`cimom.mcdata.dontUseSmis=false`.
5. Click **Save**.
  6. Discover the switch. For instructions, see “Discovering McDATA and EMC Connectrix Switches” on page 142.

---

**Note** – If you change the discovery settings, when you discover the switch with the new method, make sure you enter the correct credentials. For example, if you change from SNMP to SMI-S, the required credentials are different. See the section for the specific discovery method for information on the credentials to enter.

---

## 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, modify the `cimom.mcdata.exclude` property. Set the property `cimom.mcdata.exclude` to a comma-separated list of Worldwide Names (WWN) 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 the following WWNs: 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.

---

**Caution** – 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**) when a provider instance has been created for an excluded element. You can ignore this log message.

---

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

1. Select **Configuration > Product Health**, and 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.
4. Return to the Advanced page (**Configuration > Product Health**, and then click **Advanced** in the Disk Space tree).
5. Paste the copied text into the Custom Properties box.
6. Make your changes to the text in the Custom Properties box. Remove the pound (#) symbol in front of the property to make sure it is not commented out.
7. Add the WWNs corresponding to the switches you want to exclude from discovery. Separate additional WWNs with a comma, as shown by the following example:  
  
`cimom.mcdata.exclude=1000080088A07024,1000080088A0D0B6`  
  
where 1000080088A07024 and 1000080088A0D0B6 are the WWN for McDATA and Connectrix switches.
8. When you are done, click **Save**.

## 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 by performing Get Details to obtain information about the new switches from the service processor. For more information about adding switches, see, “Adding McDATA and EMC Connectrix Switches” on page 152.

When you remove switches from the service processor, you must remove them from the management server. For more information about removing switches, see “Removing McDATA and EMC Connectrix Switches” on page 153.

When you replace McDATA or EMC Connectrix switches, you add and remove the switches as described previously. For more information, see “Replacing McDATA and EMC Connectrix Switches” on page 154.

### *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 142.

---

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

---

To run Get Details:

1. Select **Discovery > Details**.
2. Click **Get Details**.

During Get Details, the software status light changes from green to red. You can view the progress of gathering details by accessing the logs. For more information, see “Viewing Log Messages” on page 199.

### *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. Delete 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 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 that the switches have been removed from the elements list in Discovery Steps 2 and 3 by taking the following steps:
  - a. To verify that the switches have been removed from the element list in Discovery Step 3, select **Discovery > Details**.
  - b. To verify that the switches have been removed from the element list in Discovery Step 2, select **Discovery > Topology**.

### *Replacing 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 142.

To swap the switches, perform the following steps on the management server:

1. Delete the switches from the user interface by taking the following steps (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 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 that the switches have been removed from the element list in Discovery Steps 2 and 3 by doing the following:
  - a. To verify that the switches have been removed from the element list in Discovery Step 2, select **Discovery > Topology**.
  - b. To verify that the switches have been removed from the element list in Discovery Step 3, select **Discovery > Details**.
3. Select **Discovery > Details**.

4. Click **Get Details**.

During Get Details, the software changes its status light from green to red. You can view the progress of gathering details by selecting **Discovery > View Logs**.

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

## Changing the SNMP Trap Listener Port and Community String for Switches Discovered with SNMP

The default SNMP trap listener port for all switches is 162. To change this port for all switches that are discovered through SNMP, modify the `cimom.snmpTrapListenerPort` property.

The default SNMP trap community string is public. To change this port for all switches that are discovered through SNMP, modify the `cimom.snmpTrapListenerCommunityString` property.

1. Select **Manage Product Health**, and then click **Advanced** in the Disk Space tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Do one of the following:
  - Copy the `cimom.snmpTrapListenerPort` property.
  - Copy the `cimom.snmpTrapListenerCommunityString` property.
4. Click **Close** to return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Make your SNMP trap listener port or SNMP trap community string change in the Custom Properties box. Remove the pound (#) symbol in front of the property to make sure it is not commented out. For example:  
`cimom.snmpTrapListenerPort=162.`
7. Click **Save**.

# Discover Storage Systems, NAS Devices and Tape Libraries

The following table provides an overview of the discovery requirements for storage systems, NAS devices and tape libraries.

**TABLE 6-3** 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 157.                              |
| 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 161 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” on page 158 for more information.        |
| LSI storage systems                                                        | Can be discovered two ways: <ul style="list-style-type: none"><li>• Entering the IP address/DNS name, user name and password of a controller for an LSI storage system. Discovers only the corresponding IP address of the controller.</li><li>• Entering the IP address/DNS name, user name and password of a proxy that is used to manage an LSI storage system. Discovers all controllers known to the proxy.</li></ul> | See “Discovering LSI Storage Systems” on page 162.                               |
| HDS storage systems                                                        | Discover the server running HiCommand Device Manager.                                                                                                                                                                                                                                                                                                                                                                      | See “Discovering HDS Storage Systems” on page 163 for more information.          |
| HP MSA storage systems                                                     | Discover the server running the MSA SMI-S provider.                                                                                                                                                                                                                                                                                                                                                                        | See “Discovering HP StorageWorks MSA Arrays” on page 166.                        |
| HP EVA storage systems                                                     | Discover the server running Command View EVA.                                                                                                                                                                                                                                                                                                                                                                              | See “Discovering HP StorageWorks EVA Arrays” on page 167.                        |
| HP XP storage systems                                                      | Discover the server running the SMI-S provider or the built-in provider.                                                                                                                                                                                                                                                                                                                                                   | See “Discovering HP StorageWorks XP Arrays” on page 171.                         |



**TABLE 6-3** Discovery Requirements for Storage Systems, Tape Libraries & NAS Devices

| Element                    | Discovery Requirements                                                                                                                                                                                             | Additional Information                                                                                         |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| IBM Storage Systems        | Discover the CIMOM that talks to the IBM storage systems you want to monitor.                                                                                                                                      | See “Discovering IBM Storage Systems” on page 174.                                                             |
| 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 176.                                               |
| Sun StorEdge 6920 and 6940 | Discover the storage system directly.                                                                                                                                                                              | See “Discovering Sun StorEdge 6920 and 6940 Storage Systems” on page 178.                                      |
| 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 178.                                               |
| Xiotech Storage Systems    | Discover the storage system directly.                                                                                                                                                                              | See “Discovering Xiotech Storage Systems” on page 179.                                                         |
| HP NAS Devices             | Discover the device directly.                                                                                                                                                                                      | See “Discovering HP NAS Devices on Windows” on page 180 and “Discovering HP NAS Devices on Linux” on page 181. |
| NetApp Devices             | Discover the device directly.                                                                                                                                                                                      | See “Discovering NetApp NAS Devices” on page 182.                                                              |
| Sun NAS Devices            | Discover the server running the SMI-S provider for the Sun NAS Devices.                                                                                                                                            | See “Discovering Sun NAS Devices” on page 184.                                                                 |
| HP and IBM Tape Libraries  | Discover the server running the SMI-S provider for the tape library.                                                                                                                                               | See “Discovering HP and IBM Tape Libraries” on page 185                                                        |

## Discovering 3PAR Storage Systems

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, start the InForm CLI and run the following command:

```
startcim
```

This command starts the SMI-S server within a minute or so.

---

**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.

---

To discover a 3PAR storage system:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter 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. Re-enter the password in the Verify Password box.
9. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Discovering EMC Solutions Enabler

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. See the EMC documentation for details.

To discover Symmetrix storage systems, you must create and configure a VCM volume on the storage system. The VCM database on the Solutions Enabler host must also be configured. For more information, see the *EMC Solutions Enabler Symmetrix CLI Command Reference*.

---

**Caution** – 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. You 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)

## Using Only One Subnet

To allow Solutions Enabler to respond correctly, limit the management server to a single subnet. If your management server is on two or more subnets, discovering a storage array through Solutions Enabler might not work. Limiting the management server to a single subnet allows Solutions Enabler to respond correctly.

## Excluding EMC Symmetrix Storage Systems from Discovery

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

To exclude one or more Symmetrix storage systems from discovery, 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 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.

---

**Caution** – The IP addresses of excluded elements appear in the discovery (**Discovery > Setup**), topology (**Discovery > Topology**) and 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 when 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**, and 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.symmetrix.exclude=000183500570,000183500575
```
4. Click **Close** to return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Remove the pound (#) symbol in front of the property to make sure it is not commented out. 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**.

## 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 the 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.  

```
#cimom.emc.skipRefresh=000183500570,000183500575
```
4. Click **Close** to return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Remove the pound (#) symbol in front of the property to make sure it is not commented out. 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, and then click the **Properties** tab.
7. When you are done, click **Save**.
8. To force a refresh for elements that are not configured to skip the refresh, select the **Force Device Manager Refresh** option on the Get Details page.
9. Click **Get Details**.

## 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. 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.

---

**Caution** – Before you discover a CLARiiON storage system, you must have already installed all required software components for that CLARiiON storage system, such as the Navisphere Host Agent. See 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 LSI Storage Systems

When discovering LSI storage systems, note the following:

- Discover all controllers on an LSI storage system by entering the IP address of each controller. The management server discovers these controllers as one single storage system.
- The management server must have the User Name box populated to discover the LSI storage system. Even if your LSI storage system does not have a user name set, you must enter something in the User Name box.
- To obtain drive-related statistics, install a proxy host. Ensure that the proxy host has at least one LUN rendered by each controller of the array.
- 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.
- LSI storage systems do not require a password for Get Details. If you want do not want to use the management server for provisioning on LSI storage systems, select the **Do Not Authenticate** option. The management server will still monitor the LSI storage system; however, you will not be able to do provisioning tasks.

Do the following to discover LSI storage systems:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.

3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the IP address or DNS name of the controller or proxy you want to discover.
6. Enter the user name in the User Name box. If your LSI storage system does not have a user name, you must enter something in the User Name box, even though the storage system has no user name.
7. Leave the Password box blank if you do not want to do provisioning on the LSI storage system. If you want to do provisioning, enter the corresponding password for controller or proxy.
8. If you entered a password in the previous step, re-enter the password in the Verify Password box.
9. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in 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. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## 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 port 2001. The management server does not allow port numbers in the scanning of IP ranges, so 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 489.

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

1. Access the Discovery Setup page (**Discovery > Setup**).
2. Click **Add Address**.
3. In the IP Address/DNS Name box, enter 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 box, enter the user name for accessing HiCommand Device Manager.
5. In the Password box, enter the password for accessing HiCommand Device Manager.
6. In the Verify Password box, re-enter the password for accessing HiCommand Device Manager.
7. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in 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 can 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**) when 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**, and 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.hds.exclude=61038,61037
```
4. Click **Close** to return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Remove the pound (#) symbol in front of the property to make sure it is not commented out. Add the serial numbers corresponding to the HDS storage systems you want to exclude from 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**.

## 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.

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.

---

**Caution –** 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**, and 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.HdsSkipRefresh=61038,61037
```

4. Click **Close** to return to the Advanced page.

5. Paste the copied text into the Custom Properties box.

6. Remove the pound (#) symbol in front of the property to make sure it is not commented out. 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.

---

**Note –** To find the serial number, double-click the storage system in System Explorer, and then click the **Properties** tab.

---

7. When you are done, click **Save**.
8. To force a refresh for elements that are not configured to skip the refresh, select the **Force Device Manager Refresh** option on the Get Details page.
9. Click **Get Details**.

## Discovering HP StorageWorks MSA Arrays

Before you can discover MSA arrays, you must download and install the HP MSA SMI-S Provider software. See your array documentation for more information. Keep in mind the following:

- The Array Configuration Utility (ACU) application should not be running when the management server is using the MSA provider.
- The management URL on the Properties page for the MSA can be used only if the ACU is installed on the same host as the SMI-S provider and the Execution Mode is set to Remote Service. See the ACU *Readme* file for information about execution modes and how to change them.
- Selective Storage Presentation (SSP) for the array must be enabled for provisioning to work.
- MSA volumes must be deleted in the reverse order of their creation. For example, if you have six volumes, and you want to delete the second one you created, you must delete the volumes one at a time, starting with the volume created sixth and continuing with the fifth, fourth, third, and then the second.
- The MSA SMI-S provider updates its cache every four minutes. If the array is managed by an application other than the management server, changes to the array configuration might not be reflected by a Get Details task that ran before the cache update.

To discover HP MSA storage systems:

1. Select **Discovery > Setup** in the upper-right pane of the home page window.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the IP address or DNS name of the HP CIMOM you want to discover.
6. Enter the user name used to access the MSA SMI-S provider.
7. Enter the password used to access the MSA SMI-S provider.
8. If you entered a password in the previous step, re-enter the password in the Verify Password box.

9. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Discovering HP StorageWorks EVA Arrays

The management server uses the built-in EVA provider. Before discovering EVA arrays, note the following:

- HP StorageWorks Command View EVA must be installed on a server before you can discover an HP EVA storage system.
- If you have both active and standby Command View EVA proxy machines, you can discover both the proxy machine that is actively managing the array, and the proxy machine that is not actively managing the array. If you discover only the proxy machine that is not actively managing the array, then only top level array information is collected.

If both proxy machines are discovered, keep them in the same discovery group. They can be moved to other discovery groups, but they must be moved together to the same group at the same time. When discovering the proxy machines separately, the machine that has already been discovered must be in the Default discovery group. For more information about discovery groups, see “Using Discovery Groups” on page 190.

- EVA arrays can only be provisioned if they are actively managed by the Command View server that they are discovered through.
- When an EVA is discovered by the built-in EVA provider, a cache is created and populated with the current array configuration. Each subsequent cache refresh will start 30 minutes after completion of the previous cache refresh. The time between cache refresh starts depends on factors such as the EVA configuration, model, and SAN traffic.

When you perform a provisioning operation (creating, deleting, or modifying a pool or volume), the cache information about provisioning is immediately updated. If you provision an EVA using Command View EVA or a different management station, the cached information about the EVA will not be accurate until the cache is refreshed.

To discover an EVA array:

1. Select **Discovery** > **Setup** in the upper-right pane of the management server's home page 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 box, enter the IP address of the Command View server.
6. Enter the user name used to access the Command View server.
7. Enter the password used to access the Command View server.
8. If you entered a password in the previous step, re-enter the password in the Verify Password box.
9. (Optional) In the Comment box, enter any additional information. The information entered in this box is displayed in the Comment column in the Addresses to Discover list.
10. Do not select the Do Not Authenticate option.
11. Click **OK**.
12. To start discovering elements on the network, check the check box next to the elements you want to discover, and click **Start Discovery** on the IP Addresses tab.

## Obtaining SNMP Traps using Command View EVA

You must configure Command View EVA so it can send SNMP traps from the EVA to the management server. When the management server receives these SNMP traps, it converts them to WBEM Indications for display in its Event Manager.

### *Community String Requirements*

- The default community string for Command View EVA 6.x is `Public` and the default community string for is `public`. The community strings must be a case-sensitive match, so if you are using the default values in the management server and Command View EVA 6.x, you must change the community strings to a case-sensitive match.
- If you are using the default community strings for Command View EVA 7.x and the management server, no changes to the community strings are needed. If you change the community strings to non-default values, then they must be a case-sensitive match.

---

**Caution** – Other applications may be using the default community strings to communicate with Command View EVA. If you change the community string in Command View EVA, you might break Command View EVA's connection to other applications. If a change is needed, we recommend changing the community string on the management server to match the string in Command View EVA.

---

### *Obtaining SNMP traps from Command View*

To obtain SNMP traps from Command View EVA:

1. Verify that the community strings follow the rules in "Community String Requirements" on page 169. For information on viewing or changing community strings, see "Viewing or Changing the Community String" on page 170, "Viewing or Changing the Community String in Command View EVA 6.x" on page 170, or "Viewing or Changing the Community String in Command View EVA 7.x" on page 170.
2. Configure event and host notification. For instructions, see "Configuring event and host notification in Command View EVA" on page 171.

### *Viewing or Changing the Community String*

To view or change the community string:

1. Select .
2. Click **Advanced** in the Disk Space tree.
3. Click **Show Default Properties** at the bottom of the page.
4. Copy the `cimom.snmpTrapListenerCommunityString` variable.  
The management server uses the value that is listed last, so be sure to search to the end of the page to locate the latest build.
5. Click **Close** to return to the Advanced page.
6. Paste the copied text into the Custom Properties box.
7. Change the value by entering  
`cimom.snmpTrapListenerCommunityString=<value>` where <value> is the desired community string value.
8. Click **Save**.

## *Viewing or Changing the Community String in Command View EVA 6.x*

To view or change the community string:

1. Open the `c:\hsvmafiles\nsaserver.ini` file in a text editor on the Command View EVA server.
2. Find the line `Authority=Public`  
This example shows the Command View EVA 6.x default: `Public`.
3. Change the value to the desired community string. For example, if you want to change the community string to `public`, enter `Authority=public`
4. Restart the service for Command View EVA.

## *Viewing or Changing the Community String in Command View EVA 7.x*

To view or change the community string:

1. Open the `C:\Program Files\Hewlett-Packard\Sanworks\Element Manager for StorageWorks HSV\config\cveva.cfg` file in a text editor on the Command View EVA server.
2. Find the following command lines:  

```
Authority. Default = Public
authority Public
```
3. Change the community string to the desired value. For example, if you want to change the community string to `public`, enter `authority public`
4. Restart the service for Command View EVA.

## *Configuring event and host notification in Command View EVA*

See the HP StorageWorks Command View EVA user guide for instructions on configuring Command View EVA event notification.

# Discovering HP StorageWorks XP Arrays

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

- “Discovering HP XP Arrays by Using Command View XP and SMI-S” on page 171
- “Discovering HP XP Arrays Using Command View XP Advanced Edition” on page 172
- “Discovering HP XP Arrays by using the built-in XP Provider” on page 173

---

**Note** – HP StorageWorks Command View XP should be installed on a server before you discover an HP XP storage system.

---

## Discovering HP XP Arrays by Using Command View XP and SMI-S

Before you can discover XP arrays, you must download and install the XP SMI-S Provider software. See the support matrix for details.

---

**Caution** – The Command View XP SMI-S provider does not return information related to external storage available to the HP XP storage arrays, including the external LDEVs. As a result, that information is not available in the management server user interface or reports.

---

To discover an HP XP array using Command View XP and SMI-S:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the IP address or DNS name of the Command View XP server you want to discover.
6. Enter the user name for accessing the XP SMI-S provider.
7. Enter the password for accessing the XP SMI-S provider.

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 it for the default password.

8. If you entered a password in the previous step, re-enter the password in the Verify Password box.



9. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Discovering HP XP Arrays Using Command View XP Advanced Edition

HP StorageWorks Command View XP Advanced Edition must be installed on a server before you discover an HP XP storage system.

To discover an HP XP array using Command View XP Advanced Edition:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter 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 entered a password in the previous step, re-enter the password in the Verify Password box.
9. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Discovering HP XP Arrays by using the built-in XP Provider

To discover an HP XP array using the built-in XP Provider:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter 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.

---

**Note** – The account must be a Partition Storage Administrator account.

---

8. If you entered a password in the previous step, re-enter the password in the Verify Password box.
9. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## 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 IBM 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 best not to install the IBM CIM Agent on the management server. For more information, see the *CIM Agent for DS Open (API) - Installation and Configuration Guide* for details on configuring the CIM Agent. Briefly, this procedure entails:

1. Installing the software (ESS devices only).

The installation checks for the existence of the ESSCLI. If the ESSCLI is not installed, installation of the CIM Agent cannot proceed.

2. 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 best to use port 5988 and protocol HTTP.

3. Changing the default authentication method in order to discover the CIM Agent.

a. Stop the IBM CIM Agent service, and then edit the `cimom.properties` file in `C:\Program Files\IBM\cimagent`.

b. Open the `cimom.properties` file and change the following property to false:

```
DigestAuthentication=False
```

4. 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. The credentials are not necessarily the same as those used to login to the ESS Specialist management utility or the DS Storage Manager.

5. 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 with the necessary privileges to access and configure the ESS or DS storage systems.

a. Navigate to `\Program Files\ibm\cimagent\setdevice`.

b. Do one of the following:

For ESS devices, enter `cmd address <ipaddress> <username> <password>` where `ipaddress` is the IP address of the management console server of the ESS device and `username` and `password` are the management console credentials.

For DS devices enter `cmd addressserver <ipaddress> <username> <password>` where `ipaddress` is the IP address of the management console server of the DS device and `username` and `password` are the management console credentials.

6. Restarting the IBM CIM Agent service.

7. Verifying that the CIM Agent is able to communicate with the storage devices. Enter the following command to verify communication:

```
verifyconfig -u username -p password
```

where `username` and `password` are the credentials to access CIM Agent and were created by `setuser`.

---

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

---

**Note** – The IBM CIMOM user name and password are defined with the `setuser` command.

---

8. Re-enter the password in the Verify Password box.
9. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## 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. The packages can be found on the Sun Enterprise Storage Manager Accessory CD-ROM. Refer to the readme file on the Sun StorEdge™ ESM Accessory CD-ROM for information about configuring these three 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

---

**Caution** – 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. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter 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. Re-enter the password in the Verify Password box.
9. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Discovering Sun StorEdge 6920 and 6940 Storage Systems

To discover Sun StorEdge 6920 and 6940 storage systems:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter 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. Re-enter the password in the Verify Password box.
9. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

# Discovering Sun StorEdge 6130 Storage Systems

To discover Sun StorEdge 6130 storage systems:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the IP address or DNS name of the controller or proxy you want to discover.
6. Leave the User Name box blank.
7. If you do not want to do provisioning on the storage systems, leave the password box blank. If you want to do provisioning, enter the corresponding password for controller or proxy.
8. If you entered a password in the previous step, re-enter the password in the Verify Password box.
9. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in 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. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

# Discovering Xiotech Storage Systems

---

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

---

To discover a Xiotech storage system:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.

3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, 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. A user name and password are required. Enter anything for the user name and password.
7. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
8. Select the **Do Not Authenticate** option.
9. Click **OK**.
10. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## 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 and then modify one of its properties files. For instructions, see “Installing the CIM Extension for Microsoft Windows” on page 327.

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 `APPQCime/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.

To discover an HP NAS device on Windows:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter 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. Re-enter the password in the Verify Password box.
9. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Discovering HP NAS Devices on Linux

In order to discover an HP NAS device on Linux, you must first install a CIM extension on the device and then modify one of its properties files. For instructions, see “Installing the CIM Extension for SUSE and Red Hat Linux” on page 261.

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 `/opt/APPQTime/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 then close the file.
8. Restart the CIM extension.

To discover an HP NAS device on Linux:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter 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. Re-enter the password in the Verify Password box.
9. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

# 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 through SSL you must set the `cimom.providers.netapp.useSSL` property to `true`. This is a global setting and will cause all NetApp NAS devices to communicate using SSL. For more information, see “Enabling SSL Communication with a NetApp NAS Device” on page 183.
- 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.
- 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 you are restricting Administrative HTTP access, 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. For more information, see the NetApp NAS device documentation.

To discover a NetApp NAS device:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter 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. Re-enter the password in the Verify Password box.
9. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).

10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Enabling SSL Communication with a NetApp NAS Device

To enable SSL communication with a NetApp NAS device:

1. Select **Configuration > Product Health**, and then click **Advanced** in the **Disk Space** tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the following property:  
`#cimom.providers.netapp.useSSL=true`
4. Click **Close** to return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Uncomment the `cimom.providers.netapp.useSSL` property by removing the pound symbol (#) in front of `cimom.providers.netapp.useSSL`.
7. When you are done, click **Save**.

## 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. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter 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. Re-enter the password in the Verify Password box.
9. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery > Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

## Discovering HP and IBM Tape Libraries

Before you can discover an HP or IBM tape library, you must download and install the corresponding SMI-S provider software. Refer to the support matrix and your tape library documentation for more information.

To discover an HP or IBM tape library:

1. Select **Discovery > Setup**.
2. Select **Step 1** at the top of the page.
3. Click the **IP Addresses** tab.
4. Click **Add Address**.
5. In the IP Address/DNS Name box, enter the IP address or DNS name of the SMI-S provider for the tape library.
6. Enter the user name and password of the provider running the tape library. The user name and password are the provider's user name and password, not the credentials for the operating system's user name. The default user name/password for IBM is cimuser/cimpass and for HP it's administrator/administrator unless you've made changes.
7. Enter the **Password** of the system running the tape library.
8. Re-enter the password in the Verify Password box.

9. (Optional) In the Comment box, enter any additional information. The information entered into this box is displayed in the Comment column in the Addresses to Discover list (**Discovery** > **Setup**).
10. Do not select the **Do Not Authenticate** option.
11. Click **OK**.
12. Click the **Start Discovery** button on the IP Addresses tab to start discovering elements on the network.

---

## Building the Topology

This section contains the following topics:

- “Building the Topology View” on page 186
- “Modifying the Properties of a Discovered Address” on page 187
- “Deleting Elements from the Product” on page 194

## 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, if the number two is shown between a switch and a storage system, it means that 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 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 (select **Discovery** > **Topology**). The management server obtains enough information about where the element is connected in the topology; for example, showing where a switch connected to a host.

If the management server detects an element but it cannot obtain additional information about it, it marks the element with a question mark in the topology. To learn more about fixing detected and/or disconnected elements, see “Troubleshooting Topology Issues” on page 478.

---

**Caution** – 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. See “Recalculating the Topology” on page 492 for more information.

---

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

1. Click the **Discovery** menu in the upper-right corner of the home page.
2. Click **Topology** in the upper-right corner.  
The discovered elements are selected.
3. Select **All Discovery Groups** or click **Specified Discovery Groups** to specify a customized list. If you are obtaining the topology for the first time, select **All Discovery Groups**.

---

**Note** – For information on selecting a custom discovery list, see “Creating Custom Discovery Lists” on page 191.

---

4. Click **Get Topology**.

The management server obtains the topology for selected elements and 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.

---

**Note** – You can also access System Explorer by clicking **System Explorer** in the left pane.

---

5. Review the topology for errors and/or changes.
  - 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. For more information, see “Viewing Log Messages” on page 199 and “Troubleshooting Topology Issues” on page 478.
  - If the topology for an element in your network changes, select the element and click **Get Topology (Discovery > Topology)** to update the information.

## Modifying the Properties of a Discovered Address

You can modify the user name and password the management server uses to access a device. However, 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, if the password for a host was changed, you would need to update the management server database with the new password. For more information, see “Modifying a Single IP Address Entry for Discovery” on page 128.

---

**Note** – If you 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.

---

To change the discovery properties of an element:

1. Select **Discovery > Topology** or **Discovery > Details** in the upper-right pane.
2. Click the **Edit** () 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** menu.
4. Click **OK** in the Edit Discovered Element window.

---

## Get Details

This section contains the following topics:

- “About Get Details” on page 188
- “Running Get Details” on page 189
- “Stopping the Gathering of Details” on page 190

## About Get Details

Get Details is required to obtain 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:

- Running Get Details takes 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 **Get Topology** on the Topology tab.
- Reports show data from the last successful Get Details and report cache update. When a scheduled Get Details finishes, the report cache refreshes automatically. If you run Get Details manually, the report cache updates every 6 hours. For information about refreshing the report cache, see the User Guide.



- During Get Details the data you see in the user interface is not updated until the data collection is finished.
- 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.
- You can use discovery groups to break up Get Details. For example, instead of running Get Details for all elements, you could specify only the elements in Discovery Group 1. For more information, see “Using Discovery Groups” on page 190.
- When an element in a discovery group is updated, its dependent elements are also updated.
- You can quarantine elements to exclude them from Get Details. For example, if you want to get information about all the elements in a discovery group except for one, you can quarantine that element. For more information, see “Placing an Element in Quarantine” on page 196.
- If a problem occurs with a host or SMI-S element during Get Details, the host or element is automatically quarantined. To remove the element from quarantine, see “Removing an Element from Quarantine” on page 197.
- If you want to receive status reports about Get Details, see “Configuring E-mail Notification for Get Details” on page 468 for information about how to configure this option.
- If an element changes and you run Get Details while the provider cache is updating, an error might occur or the gathered details might be inconsistent with the actual element status.

## Running Get Details

To obtain details about the elements on the network:

1. Select **Discovery > Details**.
2. Select **Include infrastructure details**, which gathers the latest information about SAN details. 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. For information about discovering master backup servers, see “Step 1 — Discovering Your Hosts and Backup Manager Hosts” on page 345.
3. 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 such as HP, HDS, and EMC storage systems with the assumption that 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 160 and “Excluding HDS Storage Systems from Force Device Manager Refresh” on page 165.

4. Select **All Discovery Groups** or click **Specified Discovery Groups** to specify a customized list. If you are running Get Details for the first time, select **All Discovery Groups**.

---

**Note** – For information on selecting a custom discovery list, see “Creating Custom Discovery Lists” on page 191.

---

5. Click **Get Details**.

During Get Details, the software changes its status light from green to red and the log opens and shows the progress of Get Details.

When the software finishes getting all element details, it displays `GETTING ALL DETAILS COMPLETED` on the View Logs page and the status light turns green.

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.

---

**Caution** – If you stop the gathering of details, you should reschedule it. This type of collection obtains detailed information about elements in the network.

---

To stop the gathering of details:

1. Select **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.

---

**Note** – Existing operations will finish before the management server stops gathering details.

---

4. Schedule a time to resume getting details.

---

## Using Discovery Groups

The discovery groups feature is sometimes called *segmented replication* because it allows you to run Get Details/ for a segment of elements. Because The product runs more slowly when Get Details is in progress, it is helpful to break the process into segments which can then be run at night or on multiple days. For example, if Get Details for all elements takes twelve hours, you could break the elements into several small groups and schedule Get Details to run at night on multiple days.

---

**Note** – For more about data collection, see “About Get Details” on page 188.

---

When planning discovery groups, consider the following requirements and capabilities:

- By default, the product is configured with a default discovery group plus four additional groups.
- Discovery groups affect the amount of memory needed for the product. Before configuring discovery groups, check the support matrix and verify that your system meets the memory requirements for using discovery groups.
- Do not move elements between discovery groups when Get Details is running. If you do this, an error will occur when Get Details tries to discover elements that were moved.
- An element can be a member of one discovery group at a time.
- Elements discovered through SMI-S and hosts discovered with CIM extensions from Build 5.1 and later of the product cannot be added to discovery groups. These elements can, however, be placed independently into scheduled Get Details tasks without being part of a discovery group. This allows you greater flexibility when gathering discovery data. For more information, see “Creating Custom Discovery Lists” on page 191.
- When an element in a discovery group is updated, its dependent elements are also updated.
- Each discovery group communicates over a specific port. The defaults are:

**TABLE 6-4** Discovery Group Ports

|                   |      |
|-------------------|------|
| Default           | 5986 |
| Discovery Group 1 | 5984 |
| Discovery Group 2 | 5982 |
| Discovery Group 3 | 5980 |

**TABLE 6-4** Discovery Group Ports

|                   |      |
|-------------------|------|
| Default           | 5986 |
| Discovery Group 4 | 5978 |

## Creating Custom Discovery Lists

You can create a discovery list for Get Details or Get Topology, which will allow you to select a set of discovery groups to use the next time Get Details runs.

1. Select **Discovery > Details or Discovery > Topology**.

2. Click the **Specified Discovery Groups** link.

3. Select the check box next to each item you want to add to the discovery list.

Elements discovered through SMI-S and hosts discovered with CIM extensions from Build 5.1 and later of the product appear in the list individually. You can add individual elements, discovery groups, or both to the same discovery list.

4. Click **Add Selected Discovery Groups to Discovery List** to move them into the Discovery List.

---

**Caution** – Do not run Get Details for all discovery groups simultaneously.

---

5. Click **OK** to save and return to the previous window. The elements are selected in the elements table.

6. Click **Get Details** or **Get Topology**.

## Managing Discovery Groups

You can manage discovery groups from the Discovery Setup page.

---

**Note** – The Default discovery group cannot be edited.

---

1. Select **Discovery > Details or Discovery > Topology**.

2. Click **Manage Discovery Groups**.

The Discovery Groups page shows a list of your discovery groups, including the name, Port Number, and included elements.

3. Click **Edit** .

4. To rename the group, enter a new name in the Name box.
5. To add a member, select the member from the Potential Members section, and then click the **Add Selected Discovery Groups to Discovery Group** button to move it into the Current Members section.
6. To remove a member, select the member from the Current Members section, and then click the **Remove Selected Discovery Groups from Discovery Group** button to move it into the Potential Members section.

---

**Note** – The path to the log file for the discovery group is listed at the top of the page.

---

7. Click **OK**.
8. Click **Back to Discovery Page**.

## Moving Elements Between Discovery Groups

All elements are initially placed in the Default discovery group. You can move elements between discovery groups.

---

**Caution** – Do not move elements between discovery groups when Get Details is running. If you do this, an error will occur when Get Details tries to discover elements that were moved.

---

### *Method 1: Select Discovery Group*

To select a new discovery group for an element:

1. Select Discovery Setup (**Discovery > Details**).  
The Get Details page appears.
2. Select the check box for the element you want to move.
3. Click **Move to Discovery Group**.  
The Select Discovery Group window appears.
4. Select the new discovery group for the selected element.
5. Click **OK**.


The management server notifies you that it can take a few minutes to move an element.

6. Click **OK**.

The elements are moved to the new discovery group.

### *Method 2: Edit a Discovered Element*

To edit a discovered element:

1. Select Discovery Setup (**Discovery > Details**). The Get Details page appears.
2. Click the **Edit** () button next to the element you want to modify.
3. Select a new discovery group in the **Discovery Group** menu.
4. Click **OK**.

The management server notifies you that it can take a few minutes to move an element.

5. Click **OK**.

The elements are moved to the new discovery group.

---

## 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 menu. Right-click an element and select **Delete Element** from the 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 **Delete** () 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. Select **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.









|              |        |                                                       |       |                                                                                     |                                                                                     |
|--------------|--------|-------------------------------------------------------|-------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| 92.168.10.25 | Switch | <a href="#">QBrocade2</a> , <a href="#">QBrocade5</a> | admin |  |  |
| 92.168.10.21 | Switch | <a href="#">QBrocade1</a>                             | admin |  |  |
| 92.168.10.22 | Switch | <a href="#">QBrocade2</a> , <a href="#">QBrocade5</a> | admin |  |  |
| 92.168.10.24 | Switch | <a href="#">QBrocade3</a> , <a href="#">QBrocade4</a> | admin |  |  |

FIGURE 6-3 Deleting Elements from the Management Server

3. Select all of the access points for the element you want to delete, and 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. Assume also that 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.



---

# Working with Quarantined Elements

When an element is quarantined, it is not included in the Get Details process until it is removed from quarantine. For more information, see “Removing an Element from Quarantine” on page 197. If a problem occurs with a host or SMI-S element during Get Details, the host or element is automatically quarantined.

## 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. Assume you want to discover all the elements in a discovery group, except for one, which is being taken off of the network for maintenance. You can use the quarantine feature to exclude this element 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 **Set Quarantine**.
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 **Clear Quarantine**.
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, and 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 use a different procedure. For more information, see “Managing McDATA and EMC Connectrix Switches” on page 152.
- Running Get Details takes 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. Select **Discovery > Details**.
2. Select **Include infrastructure details**, which gathers information about SAN details.

---

**Note – Include backup details** is used for gathering information for Backup Manager. You do not need to select it unless you have already discovered hosts running backup applications and installed CIM extensions on those hosts. For more information about discovering master backup servers, see “Step 1 — Discovering Your Hosts and Backup Manager Hosts” on page 345.

---

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 based on the assumption the information in the external database is up-to-date.

For more information, see the following topics: “Excluding EMC Symmetrix Storage Systems from Force Device Manager Refresh” on page 160 and “Excluding EMC Symmetrix Storage Systems from Force Device Manager Refresh” on page 160.

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 199 for more information about the messages viewed in this tab.
6. Verify the topology is displayed correctly by accessing System Explorer. Access System Explorer by 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, and 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, in the command, you must provide a user name to 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 this is a new installation of the management server and you have Brocade switches, download and install the Brocade SMI Agent software as described in the Brocade SMI Agent documentation.
- Additional steps are required for discovering McDATA and EMC Connectrix switches; the steps vary according to your network configuration. For more information, see “Discovering McDATA and EMC Connectrix Switches” on page 142.
- EMC CLARiiON storage systems require additional steps for discovery. For more information, see “Discovering EMC CLARiiON Storage Systems” on page 161 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.

---

## Viewing Log Messages

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

- Discovery
- Building the Topology
- Backup details

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

To view logs for these operations:

1. Select **Discovery > View Logs**.
2. To view the progress of Get Details, click the **Infrastructure** tab.
3. To view the progress of Backup Details, click the **Backup** tab.
4. To obtain the latest status, click **Get Latest Messages**.

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 that 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 Windows Management Instrumentation (WMI).

---

**Note** – The logs show data from the most recent discovery, test, or data collection task.

---

# 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. Select **Discovery > System Tasks**.
2. To obtain the latest status, click **Get the Latest Status**.

The following task statuses are provided by the Task Dashboard:

**TABLE 6-5** 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.                                  |



# Deploying and Managing CIM Extensions

---

This chapter contains the following topics:

- “Remote CIM Extensions Management” on page 203
- “About SSH” on page 204
- “Copying the CIM Extensions to the Management Server” on page 205
- “Creating Default Logins for Hosts” on page 206
- “The CIM Extension Management Wizard” on page 206
- “The CIM Extensions Management Tool” on page 208
- “About Upgrading Your CIM Extensions” on page 213

---

## Remote CIM Extensions Management

Because every production environment is different, a variety of tools are provided for deploying and managing CIM extensions. The following options are available:

### **CIM Extensions Management Wizard**

The CIM Extensions Management Wizard is integrated with the management server’s discovery interface, and allows you to deploy CIM extensions based on your discovery list. Because the wizard uses information provided during the discovery of remote clients, you won’t have to reenter this information while deploying CIM extensions.

For more information about the wizard, see “The CIM Extension Management Wizard” on page 206.

### **CIM Extensions Management Tool**

The CIM Extensions Management Tool works well if you have many remote clients. It allows you to use host lists, and simplifies the task of creating custom host lists. This tool is not integrated into the discovery interface, so you will need to enter the necessary information for each remote host.

For more information, see “The CIM Extensions Management Tool” on page 208.

### **Third-Party Tools**

If your security environment requires that you customize the CIM extensions, or you have a corporate tool that standardizes the process so that the same procedure is used for every operating system, you may need to use a third-party tool to deploy CIM extensions. Third-party tools are commonly used in large environments that require the use of a request for change (RFC) process.

### **Command Line Interface**

CIM extensions can be remotely managed through the command line interface (CLI). See the CLI guide for information about installing the CLI and using the available commands.

---

## About SSH

Each host being managed must be running a supported SSH daemon. The root or Administrator user must be allowed to log in for most operations. The product ships with OpenSSH for Windows hosts, but we do not have rights to offer an SSH package for other hosts. To deploy CIM extensions on hosts other than Windows, you can choose any SSH package that meets the following criteria and use it with the CIM extension deployment tools:

- Supports SFTP file transfers
- Supports the EXEC channel method of executing remote commands

### **For UNIX hosts:**

The default SSH configuration on some hosts prohibits root login by default. Follow these steps to manually configure SSH to allow root login on UNIX hosts:

1. Use a text editor to open `/etc/ssh/sshd_config`.
2. Change the value of `PermitRootLogin` to `yes`.
3. Restart the SSH daemon.

### **For Windows hosts:**

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, do not specify the host name when deploying OpenSSH. For example, enter a user name of <admin>  
where
  - admin is the user name

If you are running the management server on Windows, you may deploy OpenSSH to Windows hosts using the CIM Extensions Management Tool. See “The CIM Extensions Management Tool” on page 208.

## 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 is displayed if you attempt to install CIM extensions before they have been copied to the management server:

```
CIM Extensions directory: ..\Extensions is missing or incomplete
```

---

**Caution** – 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, the management server will not operate correctly. You must uninstall the management server software and then re-install.

---

To copy the CIM extensions installation files onto a Microsoft Windows server:

1. Go to disk 1 of the CIM Extensions CD-ROMs.
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 disk 1 of the CIM Extensions CD-ROMs and change directory to where you mounted it.
3. Run **./CopyExtensionFiles.sh**.

---

**Note** – Do not change the default directory.

---

## Creating Default Logins for Hosts

You can create a default CIM extension login for each type of host on which you intend to install CIM extensions (AIX, HP-UX, Linux, Solaris, Windows). This eliminates the need to use the local OS user/password database for credential verification. The login username and password are known only to the CIM extensions and do not identify real users on the host systems.

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:

`%JBOS4_DIST%\Extensions\[Platform]`

where [Platform] is 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:

`%JBOS4_DIST%\Extensions\Windows\cxws.default.login`

The **cxws.default.login** file would contain the following:

`-credentials myname:password`

---

## The CIM Extension Management Wizard

CIM extensions can be remotely managed by using the CIM Extension Management Wizard from the management server web browser. The wizard is integrated with the management server’s discovery interface, and allows you to deploy CIM extensions based on your discovery list. After you select an operation, the wizard provides the steps to guide you through the process.

Each host being managed must be running a supported SSH daemon. See “About SSH” on page 204 for more information.

You must copy the CIM extensions to the management server before you can use the CIM Extension Management Wizard. See “Copying the CIM Extensions to the Management Server” on page 205 for more information.

The CIM Extensions Management Wizard can manage CIM extensions on the following operating systems:

- AIX
- HP-UX
- Linux (i386, IA64, and x86\_64)
- Tru64
- Windows
- Solaris

To start the CIM Extension Management Wizard:

1. Log on to the the management server.
1. Select **Discovery > Setup**.
2. Click **Manage CIM Extensions**.

The CIM Extension Management Wizard provides the following functionality:

- **Setup** - Installs OpenSSH on Windows hosts that have not been discovered.
- **Update** - Updates CIM extensions. You can update CIM extensions on individual managed hosts, or you can update all of the managed hosts in specific organizations. The wizard displays the version number of the CIM extension that is running on each host.
- **Install** - Installs and starts CIM extensions on hosts that have not been discovered.
- **Manage** - Stops, starts, restarts, or gets the status of CIM extensions. The wizard allows you to manage CIM extensions on individual managed hosts, or you can manage all of the managed hosts in specific organizations.
- **Un-install** - Removes CIM extensions.
- **Troubleshoot** - Downloads logs and configuration files from remote hosts. The files are saved to the following directory:

<Install Directory>\logs\download\<HOSTNAME>\tools\ (on Windows)

<Install Directory>/logs/download/<HOSTNAME>/tools/ (on Sun Solaris or Linux)

---

# 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 204 for more information.

You must copy the CIM extensions to the management server before you can use the CIM Extensions Management Tool. See “Copying the CIM Extensions to the Management Server” on page 205 for more information.

The CIM Extensions Management Tool can manage CIM extensions on the following operating systems:

- AIX
- HP-UX
- Linux (i386, IA64, and x86\_64)
- Solaris
- Tru64
- Windows

## Launching the CIM Extensions Management Tool

To launch the CIM Extensions Management Tool on a Windows management server:

1. Go to the %MGR\_DIST%\Tools\cimeMgmt directory on the management server.
2. Run `cimeMgmt.cmd`.



To launch the CIM Extensions Management Tool on a Sun Solaris management server:

1. Set the DISPLAY environment variable.
2. Enter the following commands:

```
cd $MGR_DIST/Tools/cimeMgmt
./cimeMgmt.sh
```

# Adding Remote Hosts

In order to use the CIM Extensions Management Tool, you must create a list of the remote hosts on which you will be deploying and managing CIM extensions. To create a list of remote hosts:

1. In the Hostname box, enter the name of a host.
2. In the Username box, enter the user name used for accessing the host.
3. In the Password box, enter the password used for accessing the host.
4. Click **Add** to add the host to the table.
5. Repeat steps 1 through 4 for each additional host you want to add.
6. Click the **Edit** () button if you want to edit the entry for a host.
7. Click the **Delete** () button if you want to delete a host from the list.

## Host Lists

Host lists allow you to save your list of hosts with associated username and password information for subsequent import. In the host list file, the host and user names are presented in clear text, while the passwords are encrypted using a “password” that you enter when exporting the list.

---

**Note** – The “password” is an encryption key. It does not protect or limit access to the file itself.

---

---

**Note** – The CIM extension passwords are always encrypted. If you do not specify a password, then a blank is used as the encryption key.

---

## Importing a Host List

To import a host list:

1. Click **Import hosts**.
2. Browse to the location of the host list file (which will be in .xml format), and click **Open**.

The Enter Password dialog box displays.

3. Enter the password that was used when the file was exported, and click **OK**.  
The host list is loaded into the tool.

---

**Note** – If the wrong password is entered, the following message is displayed:  
Unable to decrypt host list with specified password

---

## Exporting a Host List

To export a host list:

1. Click **Export hosts**.
2. Browse to the desired location, enter a file name (for example, `myhosts.xml`), and click **Save**.

The Enter Password dialog box displays.

3. Enter and confirm the password, and click **OK**.

## 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. Any selected action is run against all of the hosts in the table. The following actions are available:

- **Display host operating system** - Attempts to determine the remote operating system.
- **Display Installed CIM Extension Version** - Contacts the remote system and displays the version of the CIM extension currently installed on it.
- **Deploy CIM Extensions** - Installs the CIM extension on the remote system.
- **Deploy OpenSSH (Windows Hosts Only)** - Deploys OpenSSH on the remote Windows system. This action is only available from a Windows management server.
- **Uninstall CIM Extensions** - Uninstalls the CIM extension on the remote system.
- **Upgrade CIM Extensions** - Upgrades the CIM extension on the remote system.
- **Configure CIM Extensions** - Configures the CIM extension on the remote system. You can configure the TCP port to listen on, the IP address to bind to, and custom credentials for the extension to use.

---

**Note** – You can 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 host name used to connect to the host.

---

- **Download configuration** - Downloads the configuration files from the CIM extension on the remote system. The files are saved to the following directory on the management server:

<Install Directory>\logs\download\<remote host name> (on Windows)

<Install Directory>/logs/download/<remote host name> (on Sun Solaris)

- **Download logs** - Downloads the log files from the CIM extension on the remote system. The files are saved to the following directory on the management server:

<Install Directory>\logs\download\<remote host name> (on Windows)

<Install Directory>/logs/download/<remote host name> (on Sun Solaris)

- **Start CIM Extensions** - Starts the CIM extension on the remote system.
- **Stop CIM Extensions** - Stops the CIM extension on the remote system.
- **Get CIM Extensions Status** - Checks the running status (started or stopped) of the CIM extension on the remote system.

## Configuring CIM Extensions

Click the **Go** button next to the **Configure CIM Extensions** action to configure CIM extensions on remote hosts.

The **Configure CIM Extensions** dialog box 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 host name that was entered in the Hostname box to start the CIM extensions.

---

**Note** – You cannot use the IP Address box when multiple hosts are listed.

---

The **Start Extensions on Custom Port** checkbox will start the CIM extension on the specified port.

---

**Note** – If you configure a CIM extension to use a custom port, you must specify the custom port when setting up data collection from the management server for that host.

---

The **Use Custom Credentials** checkbox configures the CIM extensions to use a user name and password that you specify. This username and password are known only to the CIM extensions and do not identify a real user on the host system.

---

**Note** – If you configure a CIM extension to use a non-default username and password, you must specify those credentials rather than those for the host’s “root” or “administrator” user when setting up data collection from the management server for that host .

---

## Log Files





When you install, remove, or upgrade CIM extensions using the CIM Extensions Management Tool, the log files are saved to the following location:

<Install Directory>\logs\cedeploy.<CIME Host Name>.log

## Status Icons


A status icon for each host is displayed in the column to the right of the host name. The following table lists all the status icons and their meanings:

**TABLE 7-1** Status Icons

| Icon                                                                                | Status                                                                |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
|  | The host has been added to the list, but no action has been selected. |
|  | The action is waiting to begin or is in progress.                     |
|  | The last action completed with a warning.                             |
|  | The last action completed successfully.                               |



**TABLE 7-1** Status Icons

| Icon                                                                              | Status                  |
|-----------------------------------------------------------------------------------|-------------------------|
|  | The last action failed. |

## About Upgrading Your CIM Extensions

You must upgrade your CIM extensions to obtain new functionality such as the following:

- QLogic failover on Linux hosts
- SecurePath support
- PowerPath support on Microsoft Windows
- Backup support - Backup information is not gathered from legacy CIM extensions. For backup information to be gathered by the management server, the CIM extension on the Backup Manager Host must be at the same software build as the management server. When you upgrade your management server, upgrade the CIM extensions on your Backup Manager Host to continue to see backup data.
- Cluster discovery

Keep in mind the following:

- After you upgrade a CIM extension on a Backup Manager Host, you must run Discovery Step 1, and then Get Details. The order of these steps is important. If you do Get Details first, and then Discovery Step 1, Protection Explorer data becomes corrupted.
- The Discovery Step 1 and Get Details is required for Backup Collections to work.

1. Upgrade the CIM extension as described in the *Installation Guide*.
2. Run Discovery Step 1. See “Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries” on page 119 for more information.
3. Run Get DetailsSee “Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries” on page 119 for more information.

---

**Caution** – After an upgrade, you need to specify again which hosts are Backup Manager Hosts by selecting **Include backup details** before you Get Details.

---



## Installing the CIM Extension for IBM AIX

---

This chapter contains the following topics:

- “About the CIM Extension for IBM AIX” on page 216
- “Prerequisites” on page 216
- “Verifying SNIA HBA API Support” on page 217
- “Installing the CIM Extension” on page 218
- “Setting Up Monitoring” on page 219
- “Starting the CIM Extension Manually” on page 220
- “How to Determine if the CIM Extension Is Running” on page 220
- “Configuring CIM Extensions” on page 221
- “Finding the Version of a CIM Extension” on page 223
- “Stopping the CIM Extension” on page 224
- “Rolling Over the Log Files” on page 224
- “Fulfilling the Prerequisites” on page 224
- “Removing the CIM Extension from AIX” on page 226

---

**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 203.

---

---

**Caution** – 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.

---

**Caution** – 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/](http://www.snia.org/tech_activities/hba_api/)

The installation creates the following directories in the `/opt/APPQcime` directory:

- **jre** - The Java runtime 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 “Rolling Over the Log Files” on page 224.

### 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

### 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 457.

### `bos.perf.libperfstat` Required for Performance Data

The file `bos.perf.libperfstat` is required for the management server to obtain 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. The `hbatest` program, which is accessible from the CIM Extension CD-ROM, lists the name and number for all HBAs 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.

---

**Caution** – The Emulex driver does not contain the required library that is required by the management server. You must install Emulex HBAnywhere software so that the management server can discover hosts configured with HBAnywhere and `hbatest` can detect the Emulex host bus adapter.

---

To run `hbatest`:

1. Go to the `Aix/tools` directory on the CIM Extension 1 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

---

**Caution** – The following steps assume you know how to use the AIX System Management Interface Tool (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 4.2 and later of the CIM extension are compatible with this build of the management server.

To install the CIM Extension for AIX:

---

**Caution** – You must install the CIM extension for IBM AIX to the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

---

1. Insert the CIM Extension 1 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 “Rolling Over the Log Files” on page 224.

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 219.
- Start the CIM extension. See “Starting the CIM Extension Manually” on page 220.
- *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 “Rolling Over the Log Files” on page 224.

---

## 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, enter 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 458.
- If you see the message “Fork Function Failed” 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 494.

When you enter the start command, the following message 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 this port is already in use, 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 enter 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.

---

## Adding a New Port Number to Discovery

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 box, enter 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 enter 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. See “Adding a New Port Number to Discovery” on page 221.

## Additional Parameters

The following table describes the parameters that can be specified in the `cim.extension.parameters` file:

**TABLE 8-1** Parameters for CIM Extensions

| Parameter                                                                                           | Description                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-port &lt;new port&gt;</code>                                                                 | The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See “Changing the Port Number” on page 221.                                                                                                                                                         |
| <code>-on &lt;ip address of NIC card&gt;</code>                                                     | Use this command to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See “Configuring the CIM Extension to Listen on a Specific Network Card” on page 222.                                                                                           |
| <code>-user</code>                                                                                  | The user defined in this parameter must be a valid existing 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. |
| <code>-credentials<br/>&lt;username from the<br/>management server&gt;<br/>:&lt;password&gt;</code> | 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.                                                                                                                                        |
| <code>-mgmtServerIP<br/>&lt;ip address&gt;</code>                                                   | This parameter 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. Enter the following at the command prompt:

```
./start -version
```

The version number of the CIM extension and the date it was built are displayed, 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.

---

## 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, with there being a maximum of three backup logs, as follows:

- `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

If your installation fails, you may be missing the following prerequisites. Refer to the information in this section on the required maintenance level and file sets.

---

**Caution** – 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, such as switches, are not displayed. 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. In the **Refine Your Search Section**, select **Tools/Utilities** from the **Limit by Type** menu.
2. Select **AIX** from the **Limit by Platform or Operating System** menu.
3. Select **5.0** from the **Limit by Version** menu.
4. In the Limit by Adding Search Terms box, enter 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.

---

# 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 described in “Stopping the CIM Extension” on page 224.
2. Enter 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.

## Installing the CIM Extension for SGI ProPack for Linux

---

This chapter contains the following topics:

- “About the CIM Extension for SGI ProPack for Linux” on page 228
- “Prerequisites” on page 228
- “Verifying SNIA HBA API Support” on page 229
- “Installing the CIM Extension” on page 230
- “Starting the CIM Extension Manually” on page 231
- “How to Determine if the CIM Extension Is Running” on page 233
- “Configuring CIM Extensions” on page 233
- “Stopping the CIM Extension” on page 236
- “Rolling Over the Log Files” on page 236
- “Removing the CIM Extension from SGI ProPack for Linux” 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 203.

---

---

**Caution** – 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.

---

**Caution** – 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/](http://www.snia.org/tech_activities/hba_api/)

---

## Prerequisites

The CIM Extension authenticates using PAM (Pluggable Authentication Module) and supports the following password encryption mechanisms:

- 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 457.

---

## Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The `hbatest` program, which is accessible from the CIM Extension CD-ROM, lists the name and number for all HBAs 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.

---

**Caution** – The Emulex driver does not contain the required library that is required by the management server. You must install Emulex HBA anywhere software so that the management server can discover hosts configured with HBA anywhere and `hbatest` can detect the Emulex host bus adapter.

---

1. Go to the `Altix/tools` directory on the CIM Extension 2 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

---

**Caution** – 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 4.2 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 2 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:

---

**Caution** – 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 enter `-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, and 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.

---

**Caution** – You must install the CIM extension for SGI ProPack for Linux to the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

---

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 Manually” on page 231.  
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 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 458.

To start the CIM extension, enter 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, enter 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 this port is already in use, 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 enter 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.

---

## Adding a New Port Number to Discovery

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 box, enter 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 enter 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. See “Adding a New Port Number to Discovery” on page 234.

## 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                                                                                                                                                                                                               |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-port &lt;new port&gt;</code>             | The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See “Changing the Port Number” on page 233.                                                               |
| <code>-on &lt;ip address of NIC card&gt;</code> | Use this command to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See “Configuring the CIM Extension to Listen on a Specific Network Card” on page 234. |

**TABLE 9-1** Parameters for CIM Extensions *(Continued)*

| Parameter                                                               | Description                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -user                                                                   | The user defined in this parameter must be a valid existing 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<br><username from the<br>management server><br>:<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.                                                                                                                                        |
| -mgmtServerIP<br><ip address>                                           | This parameter restricts the CIM extension to listen only to a specific management server IP address.                                                                                                                                                                                                               |

---

## 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 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, with there being a maximum of three backup logs, as follows:

- `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 ProPack for Linux

To remove the CIM extension for SGI ProPack for Linux:

1. Change 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_APPQcime_CIM_Extensions
```



## Installing the CIM Extension for SGI IRIX

---

This chapter contains the following topics:

- “About the CIM Extension for SGI IRIX” on page 239
- “Prerequisites” on page 240
- “Verifying SNIA HBA API Support” on page 240
- “Installing the CIM Extension” on page 241
- “Starting the CIM Extension Manually” on page 242
- “How to Determine if the CIM Extension Is Running” on page 243
- “Configuring CIM Extensions” on page 243
- “Stopping the CIM Extension” on page 247
- “Rolling Over the Logs” on page 247
- “Removing the CIM Extension from SGI IRIX” on page 248

---

**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 203.

---

---

**Caution** – 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.

---

**Caution** – 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/](http://www.snia.org/tech_activities/hba_api/)

---

## Prerequisites

The installation requires the SGI Origin system, and one of the following operating systems:

- IRIX version 6.5.22, limited to internal processors 27 and 35.
- IRIX version 6.5.20, patch 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 457.

---

## Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The `hbatest` program, which is accessible from the CIM Extension CD-ROM, lists the name and number for all HBAs 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.

---

**Caution** – The Emulex driver does not contain the required library that is required by the management server. You must install Emulex HBAnywhere software so that the management server can discover hosts configured with HBAnywhere and `hbatest` can detect the Emulex host bus adapter.

---

1. Go to the `Irix/tools` directory on the CIM Extension CD-ROM2.

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 in 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

---

**Caution** – To upgrade the CIM extension, first remove the previous version before installing the latest version. Builds 4.2 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 Extension 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.

---

**Caution –** You must install the CIM extension for SGI IRIX to the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

---

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 Manually” on page 242.

---

## 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 458.

To start the CIM extension, enter 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 this port is already in use, 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 enter 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.

---

## Adding a New Port Number to Discovery

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 box, enter 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 enter 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. See “Adding a New Port Number to Discovery” on page 244.

## 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                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-port &lt;new port&gt;</code>                                                                 | The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See “Changing the Port Number” on page 243.                                                                                                                                                         |
| <code>-on &lt;ip address of NIC card&gt;</code>                                                     | Use this command to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See “Configuring the CIM Extension to Listen on a Specific Network Card” on page 244.                                                                                           |
| <code>-user</code>                                                                                  | The user defined in this parameter must be a valid existing 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. |
| <code>-credentials<br/>&lt;username from the<br/>management server&gt;<br/>:&lt;password&gt;</code> | 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.                                                                                                                                        |

**TABLE 10-1** Parameters for CIM Extensions (*Continued*)

| Parameter                     | Description                                                                                           |
|-------------------------------|-------------------------------------------------------------------------------------------------------|
| -mgmtServerIP<br><ip address> | This parameter 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 appqcime 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. Enter the following at the command prompt:

```
./start -version
```

The version number of the CIM extension and the date it was built are displayed, 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

- xxxx is the year
- x.x.x.x is the version of the CIM extension

---

## 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, with there being a maximum of three backup logs, as follows:

- `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 SGI IRIX:

1. Stop the CIM extension as described in “Stopping the CIM Extension” on page 247.
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`

# Installing the CIM Extension for HP-UX

---

This chapter contains the following topics:

- “About the CIM Extension for HP-UX” on page 249
- “Prerequisites” on page 250
- “Verifying SNIA HBA API Support” on page 250
- “Installing the CIM Extension” on page 251
- “Starting the CIM Extension Manually” on page 253
- “How to Determine if the CIM Extension Is Running” on page 253
- “Configuring CIM Extensions” on page 254
- “Stopping the CIM Extension” on page 258
- “Rolling Over the Log Files” on page 258
- “Fulfilling the Prerequisites” on page 259
- “Removing the CIM Extension from HP-UX” on page 259

---

**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 203.

---

---

**Caution** – 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.

---

**Caution** – 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/](http://www.snia.org/tech_activities/hba_api/)

---

## Prerequisites

Refer to the HP tab of the support matrix for the prerequisites. If the installation fails, see “Fulfilling the Prerequisites” on page 259.

FC SNIA HBA API software is bundled with the driver and is installed at the same time the driver 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 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 457.

---

## Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The hbatest program, which is accessible from the CIM Extension CD-ROM, lists the name and number for all HBAs 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.

---

**Caution** – The Emulex driver does not contain the required library that is required by the management server. You must install Emulex HBAnywhere software so that the management server can discover hosts configured with HBAnywhere and hbatest can detect the Emulex host bus adapter.

---

To run hbatest:

1. Go to the `HPUX/tools` directory on the CIM Extension 1 CD-ROM.
2. Enter the following at the command prompt:

```
./hbatest
```

The program runs its diagnostics.

HP SNIA adapters AXXXXA come from fileset FC-FCD, FC-TACHYON-TL. Unless separated purposely during the installation of 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 opposed 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 following the instructions in this section, and then performing 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 4.2 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. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

To install the CIM extension:

1. Login as root.
2. Insert the CIM Extension 1 CD-ROM into the CD-ROM drive on the HP-UX server.
3. Create the `/cdrom` directory on the 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 the c, t, and d numbers correspond to CD-ROM device numbers.

To find out c#t#d# for your CD-ROM, run the `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 the following message is displayed: `analysis and execution succeeded`

6. Eject/unload the CD-ROM by unmounting the CD-ROM with the following command and pressing eject 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. Enter 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 458.

To start the CIM extension, enter 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. 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 fewer privileges, for example `jsmythe`. First, you would add the user to the parameters file. You would then log on 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 enter the following line:

```
-users myname
```

where `myname` is a valid HP-UX user name.

---

**Note** – You can enter multiple users by separating them with a colon. For example `-users myname:jsmythe`.

---

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 this port is already in use, 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 enter 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.

---

## Adding a New Port Number to Discovery

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 box, enter 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 enter 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. See “Adding a New Port Number to Discovery” on page 255.

## 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                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -port <new port>                                                     | The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See “Changing the Port Number” on page 255.                                                                                                                                                         |
| -on <ip address of NIC card>                                         | Use this command to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See “Configuring the CIM Extension to Listen on a Specific Network Card” on page 256.                                                                                           |
| -user                                                                | The user defined in this parameter must be a valid existing 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<br><username from the management server><br>:<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.                                                                                                                                        |
| -mgmtServerIP<br><ip address>                                        | Restricts the CIM extension to listen only to a specific management server IP address.                                                                                                                                                                                                                              |

## Finding the Version of a CIM Extension

To find the version number of a CIM extension:

1. Go to the `/opt/APPQcime/tools` directory.
2. Enter the following at the command prompt:

```
./start -version
```

The version number of the CIM extension and the date it was built are displayed, 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 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 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, with there being a maximum of three backup logs, as follows:

- `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 in this section to determine if you have the required software.

To verify the 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 the host has more than one HBA, enter the following at the command prompt:

```
fcmsutil /dev/td1
```

The 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 258.
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
```



# Installing the CIM Extension for SUSE and Red Hat Linux

---

---

**Caution** – Do not install the CIM extension onto the management server.

---

This chapter contains the following topics:

- “About the CIM Extension for Red Hat Linux Advanced Server and SUSE Linux” on page 262
- “Prerequisites” on page 262
- “Verifying SNIA HBA API Support” on page 262
- “Installing the CIM Extension” on page 264
- “Starting the CIM Extension Manually” on page 267
- “How to Determine if the CIM Extension Is Running” on page 267
- “Configuring CIM Extensions” on page 268
- “Stopping the CIM Extension” on page 271
- “Rolling Over the Log Files” on page 271
- “Removing the CIM Extension from Red Hat or SUSE Linux” on page 272

Keep in mind the following:

- 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 203.
- 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.
- The 6.0 management server requires that any managed Tru64 or OpenVMS hosts be running at least version 5.1.0 SP4 (5.1.4) of the CIM Extensions. If the Tru64 and OpenVMS CIM Extensions are not at the minimum levels, the 6.0.0 management server will be unable to gather information from those hosts, and there will be various replication errors in the management server logs. It is preferable to upgrade all CIM Extensions to the same version as the management server, as some functionality may be unavailable when earlier CIM Extensions are used.

---

# 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.

---

**Caution** – 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/](http://www.snia.org/tech_activities/hba_api/)

---

## Prerequisites

During the installation, a “requires” rpm is run first to check for dependencies. You will be notified if you are missing any required packages.

### 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 457.

---

## Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The hbatest program, which is accessible from the CIM Extension CD-ROM, lists the name and number for all HBAs that support the SNIA HBA API.

To run hbatest:

1. Go to the `linux/tools` directory on the CIM Extension 1 CD-ROM.
2. Enter the following at the command prompt:  
`./hbatest`

The program runs its diagnostics.

## Driver Information for Verifying Emulex SNIA Adapters

The Emulex driver does not contain the required library that is required by the management server. You must install Emulex HBAnywhere software so that the management server can discover hosts configured with HBAnywhere and the HBATool can detect the Emulex host bus adapter.

After you install the HBAnywhere software, you can find the location of the libraries as follows in the `/etc/hba.conf` file.

**For the 64-bit hosts running the Linux operating system, following is displayed in hba.conf file:**

To view the `hba.conf` file, enter the following:

```
cat /etc/hba.conf
```

The library name is listed first and then the path, as shown in the following example:

```
com.emulex.emulexapilibrary /usr/lib64/libemulexhbaapi.so
com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so
```

**For 32-bit hosts running the Linux operating system, the following is displayed in hba.conf file:**

To view the `hba.conf` file, enter the following:

```
cat /etc/hba.conf
```

The library name is listed first and then the path, as shown in the following example:

```
com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so
```

# Driver Information for Verifying QLogic SNIA Adapters

QLogic SNIA adapters come from a separate package, `qlapi-vX.XXX-rel.tgz`, found in the QLogic driver. The adapters are installed separately after the 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/libqlsdrm.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 opposed 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 following the instructions in this section, and then performing 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 4.2 and later of the CIM extension are compatible with this build of the management server.
- The installation is a two-step process where a “requires” rpm is run first to check for dependencies, and then the full rpm is installed.
- You must install the CIM extension for SUSE and Red Hat Linux to the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

To install the CIM extension:

1. Login as root.
2. Go to the `Linux/requires_rpm` directory on the CIM ExtensionCD1 CD-ROM by entering the following at the command prompt:  

```
cd /cdrom/linux/requires_rpm
```

where `/cdrom` is the name of the CD-ROM drive.
3. Use the appropriate “requires” rpm from the list below for the version of the OS you are installing.

---

**Note** – The version and release number of the “requires” rpm will change based on the version and release.

---

### **Redhat EL/AS 3**

- 32 bit on x86:  
RHEL3/APPQcime-Requires-<Version> <Release>.i386.rpm
- 32 bit / 64 bit on x86\_64:  
RHEL3/APPQcime-Requires-<Version>-<Release>.x86\_64.rpm

### **Redhat EL/AS 4**

- 32 bit on x86:  
RHEL4/APPQcime-Requires-<Version>-<Release>.i386.rpm
- 2 bit / 64 bit on x86\_64:  
RHEL4/APPQcime-Requires-<Version>-<Release>.x86\_64.rpm
- IA64:  
RHEL4/APPQcime-Requires-<Version>-<Release>.ia64.rpm

### **Redhat EL/AS 5**

- 32 bit on x86:  
RHEL5/APPQcime-Requires-<Version>-<Release>.i386.rpm
- 32 bit / 64 bit on x86\_64:  
RHEL5/APPQcime-Requires-<Version>-<Release>.x86\_64.rpm
- IA64:  
RHEL5/APPQcime-Requires-<Version>-<Release>.ia64.rpm

### **SLES 9**

- 32 bit on x86:  
SLES9/APPQcime-Requires-<Version>-<Release>.i386.rpm
- 32 bit on x86\_64:  
SLES9/APPQcime-Requires-<Version>-<Release>.x86\_64.rpm
- IA64:  
SLES9/APPQcime-Requires-<Version>-<Release>.ia64.rpm

### **SLES 10**

- 2 bit on x86:  
SLES10/APPQcime-Requires-<Version>-<Release>.i386.rpm
- 32 bit on x86\_64:  
SLES10/APPQcime-Requires-<Version>-<Release>.x86\_64.rpm
- IA64:  
SLES10/APPQcime-Requires-<Version>-<Release>.ia64.rpm

After running this “requires” rpm you will get one or more dependency errors. A dependency on the rpm package APPQcime is expected. For example:

APPQcime is needed by APPQcime-Requires-6.0.0-224.i386.rpm

If you get an additional dependency error, you must install the required packages before continuing.

4. After running the "requires" rpm and getting just the one expected dependency error, enter one of the following commands:

For 64-bit Linux Itanium servers:

```
rpm -idvh APPQcime--<Version>--<Release>-ia64.rpm
```

For all other servers:

```
rpm -idvh APPQcime--<Version>--<Release>-i386.rpm
```

The following output is displayed:

```
Preparing... ##### [100%]
1:APPQcime ##### [100%]
```

The installation is done when you are returned to the command prompt.

5. *Optional:* Rerun the "requires" rpm from step 3. You should no longer receive any errors.

Example of steps 3 - 5:

```
3. rpm -idvh RHEL3/APPQcime-Requires-6.0.0-224.i386.rpm
```

Error: Failed dependencies:

APPQcime is needed by APPQcime-Requires-6.0.0-224.i386.rpm

This error is the expected result, but if there were more errors, they would need to be addressed.

If you only received one error (as in this example), it means the other dependant libraries are all installed, so the full APPQcime package should now be installed.

```
4. rpm -idvh APPQcime-6.0.0-224-i386.rpm
```

(Install APPQcime package)

```
5. rpm -idvh RHEL3/APPQcime-Requires-6.0.0-224.i386.rpm
```

(No failed dependencies, so no messages appear.)

Optionally, verify packages were installed:

```
rpm -qa | grep APPQcime-Requires
```

```
rpm -qa | grep APPQcime
```

To uninstall packages, uninstall the "requires" rpm first. For example:

```
rpm -e APPQcime-Requires-6.0.0-224
```

```
rpm -e APPQcime
```

(Verified packages were uninstalled. No error messages appear.)

---

## 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 458.

To start the CIM extension, enter 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...
```

Note that when you start the CIM extension, you can change the port number the CIM extension uses. See “Configuring CIM Extensions” on page 268 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 this port is already in use, 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 enter 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.

---

## Adding a New Port Number to Discovery

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 box, enter 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 enter 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. See “Adding a New Port Number to Discovery” on page 268.

## 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                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-port &lt;new port&gt;</code>                                                                 | The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See “Changing the Port Number” on page 268.                                                                                                                                                         |
| <code>-on &lt;ip address of NIC card&gt;</code>                                                     | Use this command to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See “Configuring the CIM Extension to Listen on a Specific Network Card” on page 269.                                                                                           |
| <code>-user</code>                                                                                  | The user defined in this parameter must be a valid existing 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. |
| <code>-credentials<br/>&lt;username from the<br/>management server&gt;<br/>:&lt;password&gt;</code> | 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.                                                                                                                                        |
| <code>-mgmtServerIP<br/>&lt;ip address&gt;</code>                                                   | This parameter restricts the CIM extension to listen only to a specific management server IP address.                                                                                                                                                                                                               |

## Finding the Version of a CIM Extension

To find the version number of a CIM extension:

1. Go to the `/opt/APPQcime/tools` directory.
2. Enter 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:

---

## 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 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, with there being a maximum of three backup logs, as follows:

- `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 271.
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.

## Installing the CIM Extension for NonStop

---

This chapter describes the following:

- “About the CIM Extension for NonStop” on page 273
- “Prerequisites” on page 274
- “Installing the CIM Extension” on page 275
- “Verifying SNIA HBA API Support” on page 277
- “Starting the CIM Extension Manually” on page 277
- “Stopping the CIM Extension” on page 283
- “Finding the Status of the CIM Extension” on page 282
- “Rolling Over the Logs” on page 283
- “Fulfilling the Prerequisites” on page 284
- “Increasing the native logging level” on page 284
- “Removing the CIM Extension from NonStop” on page 284

---

### About the CIM Extension for NonStop

The CIM extension for NonStop gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

---

**Caution** – Install the CIM extension on each host that 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 supports communication only 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/](http://www.snia.org/tech_activities/hba_api/)

---

## Prerequisites

The installation checks for the requirements described in the next two sections:

---

**Note** – If the installation fails, see “Fulfilling the Prerequisites” on page 284.

---

### NonStop G06.27 or later Software Requirements

- Ensure that the OSS subsystem is running on the NonStop host.
- Enter the `osh` command from the TACL prompt to access the OSS environment.
- Ensure that the process `$ZPMON` is running.
- Ensure that adequate swap space is available.

### Network Port

By default, the CIM extension uses port 4673 to communicate with the management server.

To ensure that your network port is working properly:

- Verify that the network port is open. Refer to the documentation accompanying your NonStop 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 457.

---

# Installing the CIM Extension

Use the following procedure to install the CIM extension for NonStop:

1. Navigate to the default directory.
2. Transfer the depots and install scripts to the host using FTP. NonStop hosts do not support CD drives.
3. Place the CIM extension CD-ROM into the CD-ROM drive on any local host. Select one of the following options:
  - **UNIX/Linux host:** Enter the following command at the command prompt to go to the NonStop directory:  

```
cd /cdrom/nsk/NSR
```
  - **Windows:** Browse to your compact disk drive. Enter the following command:  

```
C:\>D:
```

where D: is the drive where your compact disc resides.

You can also get this information using Windows Explorer.
4. Navigate to the NSR folder of the CIM extension CD-ROM by entering the following command:  

```
D:\>cd/nsk/NSR
```
5. Enter the following command to FTP the NonStop depots and install scripts to the NonStop host:  

```
ftp <NonStop host name>
```
6. Enter the superuser's username and password when you are prompted. For example:  

```
User (XXX.YYY.hp.com:(none)): super.super
331 Password required for SUPER.SUPER.
Password: XXXXXXXX
230 User SUPER.SUPER logged in.
```
7. Enter the OSS subsystem at the command prompt:  

```
ftp> quote oss
257 OSS API enabled.
```
8. Enter the binary mode of the file transfer by entering the following at the command prompt:  

```
ftp > bin
```

200 Type set to I.

9. Create a directory on the NonStop host to store the depots and scripts, and transfer the files to that directory by entering the following commands:

```
ftp> mkdir /tmp/NonStopdepots
ftp> cd /tmp/NonStopdepots
ftp> put APPQCIMENSR.pax
ftp> put APPQJAVANSR.pax
ftp> put nsk_local_install.sh
ftp> put nsk_local_uninstall.sh
```

---

**Note** – Ensure that the directory on the NonStop host is part of the OSS layer. Do not transfer the depots to a Guardian volume or subvolume. For example, do not transfer the depots to a directory or subdirectory of /G directory when accessed from OSS. The Guardian layer imposes a filename length limit of eight characters.

---

10. Log in to the NonStop host (where you have transferred the depot files), as superuser. Select one of the following options:
  - If OSS is enabled during Telnet, choose that option.
  - Enter the `osh` command from the TACL prompt to access the OSS subsystem.

11. Go to the directory where you have transferred the depot files by running:

```
/home/super: cd /tmp/NonStopdepots
```

12. Enter the following at the command prompt to install the JRE on NonStop:

```
/tmp/NonStopdepots:./nsk_local_install.sh APPQJAVA
```

When the installation is complete, the following message appears:

```
Installation of APPQJAVANSR was successful. Package is installed
under
```

```
/opt/APPQcime directory. Install log can be found at /tmp/
nsk_local_install.log
```

---

**Caution** – You must install the CIM extension for NonStop to the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

---

13. Enter the following at the command prompt to install the APPQCIME agent:

```
/tmp/NonStopdepots:./nsk_local_install.sh APPQCIME
```

When the installation is complete, the following message appears:

```
Installation of APPQCIMENSR was successful
```



```
Package is installed under /opt/APPQcime directory
Starting HP NSK CIM Extensions on current node
Install log can be found at /tmp/nsk_local_install.log
```

---

## Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The hbatest program lists the name and number for all HBAs 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.

---

**Caution** – The Emulex driver does not contain the required library that is required by the management server. You must install Emulex HBAnywhere software so that the management server can discover hosts configured with HBAnywhere and hbatest can detect the Emulex host bus adapter.

---

To run hbatest:

1. Verify that you have installed the CIM extension.
2. Go to the `/opt/APPQcime/tools/hbatest` directory on the host where you installed the CIM extension.
3. Enter the following at the command prompt:  
`./hbatest`

The program runs its diagnostics.

---

## Starting the CIM Extension Manually

The management server can obtain information from this host only when the CIM extension is running.

Keep in mind the following:

1. You must have superuser 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 superuser has enough privileges to provide the information the management server needs.
2. To configure UNIX CIM extensions to run behind a firewall, see “Configuring UNIX CIM Extensions to Run Behind Firewalls” on page 458.

To start the CIM extension, enter `./start` in the `/opt/APPQcime/tools` directory.

---

**Note** – Ensure that you have installed the CIM extension in the `/opt` directory.

---

The following message is displayed:

```
Starting CIM extension for NonStop.....
```

The CIM extension is ready to be contacted by the management server when a message similar to the following example appears:

```
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

Keep in mind the following:

- Depending on your terminal type and processor speed, the message `CXWS x.x.x.x on /192.168.1.5:4673 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 are allowed to 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 entering:

```
/start -help
```

---

## Restricting the Users Who Can Discover the Host

The `./start -users` command provides greater security by restricting access. When you use the management server to discover the host (**Discovery > Setup**), provide a username that was specified in the `-users` parameter in the start command, for example:

```
./start -users myname
```

The variable `myname` is a valid NonStop username that must be used to discover this NonStop host. For example, assume you want to use the management server to discover a NonStop host, but you do not want to provide the password to the superuser account. You can provide the password to another valid NonStop user account that has fewer privileges, for example `jsmythe`. You would log in to the NonStop host as superuser and start the CIM extension by using the following command:

```
./start -users jsmythe
```

The variable `jsmythe` is a valid NonStop username.

Log in to the management server, access the Discovery page (**Discovery > Setup**), and click **Add Address**. In the Add Address for Discovery page, provide the username and password for `jsmythe`. Only the username and password for `jsmythe` can be used to discover the NonStop host. This is because you used `jsmythe` in the `./start -users` command.

Another variation of the start command lets you provide multiple users in a colon-separated list, for example:

```
./start -users myname:jsmythe
```

One of the names listed (`myname` or `jsmythe`) must be used to discover the NonStop host (**Discovery > Setup**) on the management server. Other usernames and passwords, including `root`, will not work.

---

## Changing the Port Number

The CIM extension uses port 4673 by default. If the port is already used, enter the `./start -port port_number` command to change the port that the CIM extension will access.

---

**Caution** – The steps in this section provide information about temporarily changing the port of the CIM extension. If you want to make the change permanent, see “Permanently Changing the Port a CIM Extension Uses (UNIX Only)” on page 457.

---

To change the port, enter the following:

```
./start -port 1234
```

The variable 1234 is the port the CIM extension will listen on for all available network cards

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 box, 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
```

The designation 192.168.1.2 is the IP address of the host and 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 add it again. You cannot have more than one listing of the host with different ports.

---

**Caution** – If you specify a port in the `./start` command, the host can be discovered by any account that has access to the NonStop server.

---

---

## Specifying the CIM Extension to Listen on a Specific Network Card

You can specify the CIM extension to listen only on a specific network interface card (NIC) by using the `-on` command line option in the start command, for example:

```
./start -on 192.168.2.2
```

The CIM extension listens only on the NIC that has the IP address 192.168.2.2.

Specifying a NIC requires some changes to the NonStop host configuration also.

All NonStop nodes can be configured to have multiple IPs. Each IP has its corresponding TCP/IP process. This means that any TCP/IP operation for a particular IP is handled by its corresponding TCP/IP process. To start the agent with a particular IP, ensure that the corresponding TCP/IP process is set to default. Otherwise, the agent fails to start, and the following message is displayed:

```
Can't assign requested address: Unable to accept connections on
specifiedIP port portNo
```

The following table lists the commands that are used to display and set the default TCP/IP process.

**TABLE 13-1** TCP/IP Process Display Commands

| Command or Argument                | Definitions and Output Examples                                                                                                              |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <code>info_define all</code>       | Displays the default TCP/IP process                                                                                                          |
| <code>scf info subnet \$*.*</code> | Uses GTACL commands to check and set the TCP/IP process for the IP address.                                                                  |
| <code>alter define</code>          | <p>Displays multiple IP addresses on a host, along with their TCP/IP processes.</p> <pre>alter define= TCPIP^PROCESS^NAME, FILE \$ZTC4</pre> |
|                                    | <p><b>Note</b> – ZTC4 is the TCP/IP process of an IP.</p>                                                                                    |

The following table lists port arguments.

**TABLE 13-2** Port Arguments

| Argument           | Definition and Output Examples                                                                                                                                                                                                                                                                                                                                          |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-on</code>   | <p>Can specify a port specification. For example:</p> <pre>./start -on 192.168.2.2:3456</pre> <p>Instead of listening on the default port, the CIM extension listens on IP address 192.168.2.2 and the indicated port 3456 of the designated NIC.</p>                                                                                                                   |
| <code>-port</code> | <p>Can be used in conjunction with the <code>-on</code> command option. Any <code>-on</code> arguments that do not specify a port number use the <code>-port</code> argument as the port number. For example:</p> <pre>./start -on 192.168.1.1 -port 1170</pre> <p>The CIM extension listens on Port 1170 of the designated NIC with the IP address of 192.168.1.1.</p> |

## Finding the Version of a CIM Extension

To find the version number of a CIM extension:

1. Go to the `/opt/APPQcime/tools` directory.
2. Enter the following at the command prompt:

```
./start -version
```

The CIM extension and build date are displayed, as shown in the following example:

```
CXWS for mof/cxws/cxws-nsk.mof
```

```
CXWS version x.x.x.x, built on Mon 19-March-xxxx 17:28:30 by
Administrator
```

where X.X.X.X represents the version of the CIM extension and the letters XXXX represent the year of the build.

## Combining Start Commands

You can also combine the `-users` and `-port` commands. Select from one of the following options:

- `./start -users myname -port 1234`
- `./start -port 1234 -users myname`

where `myname` is the username that must be used to discover this Tru64 UNIX host. The new port number is 1234.

---

## Finding the Status of the CIM Extension

You can check the status of the CIM extension by entering `./status` in the `/opt/APPQcime/tools` directory.

The CIM extension is running when the following message appears:

```
CIM extension Running: Process ID: 93
```

---

## Stopping the CIM Extension

To stop the CIM extension, enter the `./stop` at the command prompt in the `/opt/APPQcime/tools` directory.

Keep in mind the following:

- You must have superuser 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. The `cxws.log` files roll over when the files become larger than the configured size, for example 30 MB. The information in `cxws.log` is moved to `cxws.log.1`. If `cxws.log.1` already exists, `cxws.log.2` is created. The numbering for the files continues sequentially.

The maximum size and the number of old logs that can be stored are configured in the `log4j.appender.File.MaxFileSize` and `log4j.appender.File.MaxBackupIndex` properties in the `/opt/APPQcime/conf/cxlog4j.properties` file.

The `cxws.out` file contains logging information, such as starting the CIM extension, which is recorded in case something unexpected happens with the Java Virtual Machine. The `cxws.out` file is rewritten each time the CIM extension restarts.

The `cxws_native.log` contains logging information for NonStop system calls. 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` specified in the configuration file, the `cxws_native.log` 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 for NonStop system calls. The configuration information for `cxws_native.log` is maintained in `/opt/APPQcime/conf/cxws_native.cfg`. Detailed logging information can be obtained by increasing the log level. To increase the log level, set `LOG_LEVEL` to 3 in `cxws_native.cfg` and restart the CIM extension.

---

## Fulfilling the Prerequisites

Use the commands mentioned in this section to determine if you have the required software. To test whether OSS environment is running, enter the following command from the TACL prompt:

```
$SYSTEM SYSTEM 1> osh
```

The prompt switches to a UNIX style. For example:

```
/home/super:
```

---

## Removing the CIM Extension from NonStop

To remove the CIM extension:

1. Log in as superuser.
2. Go to the `/opt/APPQcime/scripts` directory.
3. Execute the script `nsk_local_uninstall.sh APPQCIME` to remove the CIM extension.

When you see the following message, the CIM extension has been removed:

```
Uninstallation of package APPQCIME was successful.
```

```
Uninstall log can be found at tmp/nsk_local_uninstall.log
```

4. Execute the script `nsk_local_uninstall.sh APPQJAVA` to remove the NonStop JAVA packaged with the extension.



When you see the following message, NonStop JAVA has been removed:

```
Uninstallation of package APPQJAVA was successful.
```

```
Uninstall log can be found at tmp/nsk_local_uninstall.log
```

5. Go to the `/opt` directory and enter the following at the command prompt to remove the APPQcime directory:

```
rm -r APPQcime
```

---

## Handling Daylight Savings Time Changes for the NonStop CIM Extension

The NonStop JDK packaged together with the NonStop CIM extension for S series does not contain daylight savings time (DST) changes. In order to obtain the DST changes, you must install conversion tool TZUpdater 1.1 which can be downloaded from [www.hp.com/go/javaDSTtool](http://www.hp.com/go/javaDSTtool).

This tool allows installed HP NonStop servers for Java (NSJ) JDK/JRE images to be updated with time zone data. TZUpdater 1.1 accommodates the U.S. 2007 DST changes originating with the U.S. Energy Policy Act of 2005. This tool also incorporates changes to the 2007-2008 New Zealand's DST, which starts at 2:00 A.M. on September 30, 2007, and ends at 3:00 A.M. on April 6, 2008.

To execute TZUpdater1.1:

1. Download and unzip `TZUpdater-1.1-2007f.zip` from [www.hp.com/go/javaDSTtool](http://www.hp.com/go/javaDSTtool) onto a local windows host.
2. FTP the `tzupdater.jar` from the unzipped folder to the NonStop host where the CIM extension is installed.
3. Use the binary mode of file transfer and FTP to the OSS subsystem.
4. Place `tzupdater.jar` in the `/opt/APPQcime/modjava` directory. The following is an example of this procedure:

```
ftp>quote oss
OSS API enabled.
ftp> bin
Type set to I.
ftp> cd /opt/APPQcime/modjava
ftp> put tzupdater.jar
```

5. Stop the CIM extension by entering:

```
../tools/stop
```

6. Point JAVA\_HOME and JREHOME variables to the instance of the NSJ JDK to be operated upon.

```
export JAVA_HOME=/opt/APPQcime/Java
```

```
export JREHOME=$JAVA_HOME/jre.
```

7. Run tzupdater by entering:

```
./java -jar tzupdater.jar -u -v
```

The following output is displayed:

```
/opt/APPQcime/modjava: ./java -jar ../tzupdater.jar -u -v
```

```
java.home: /opt/APPQcime/java/jre
```

```
java.vendor: Hewlett-Packard Company
```

```
java.version: 1.4.2_04
```

```
JRE time zone data version: tzdata2003a
```

```
Embedded time zone data version: tzdata2007f
```

```
Extracting files... done.
```

```
Renaming directories... done.
```

```
Validating the new time zone data... done.
```

```
Time zone data update is complete.
```

8. Restart the NonStop CIM extension:

```
../tools/start
```

## Installing the CIM Extension for OpenVMS

---

This chapter contains the following topics:

- “About the CIM Extension for OpenVMS” on page 287
- “Prerequisites” on page 288
- “Installing the CIM Extension” on page 289
- “Starting the CIM Extension Manually” on page 291
- “How to Determine if the CIM Extension is Running” on page 292
- “Finding the Version of a CIM Extension” on page 296
- “Stopping the CIM Extension” on page 298
- “Rolling Over the Log Files” on page 298
- “Increasing the Native Logging Level” on page 299
- “Removing the CIM Extension from OpenVMS” on page 299

---

**Note** – This chapter describes how to install and manage the CIM extension directly on the host.

---

---

**Caution** – 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. It then makes the information available to the management server.

---

**Caution** – 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/](http://www.snia.org/tech_activities/hba_api/)

---

**Caution** – The Emulex driver does not contain the required library that is required by the management server. You must install Emulex HBAnywhere software so that the management server can discover hosts configured with HBAnywhere and hbatest can detect the Emulex host bus adapter.

---

---

## Prerequisites

The prerequisites are as follows:

### Supported OpenVMS (Alpha) versions and required ECOs

---

**Note** – To verify installed patches, enter the following at the command prompt:  
`$ PRODUCT SHOW PRODUCT/FULL`

---

#### ■ OpenVMS Alpha 7.3-2

The following patches must be installed in the order specified:

- DEC-AXPVMS-VMS732\_PCSI-V0300 or later
- DEC-AXPVMS-VMS732\_UPDATE-V0600 or later
- DEC-AXPVMS-VMS732\_SYS-V1000 or later
- DEC-AXPVMS-VMS732\_FIBRE\_SCSI-V0900 or later
- **OpenVMS Alpha 8.2**
  - DEC-AXPVMS-VMS82A\_PCSI-V0100 or later
  - DEC-AXPVMS-VMS82A\_UPDATE-V0300 or later
  - DEC-AXPVMS-VMS82A\_SYS-V0400 or later
  - DEC-AXPVMS-VMS82A\_FIBRE\_SCSI-V0200 or later
- **OpenVMS Alpha 8.3** - The OpenVMS Alpha 8.3 comes with the required ECOs and patches.

### Supported OpenVMS Itanium versions and required ECOs

- **OpenVMS IA64 8.2-1**
  - HP-I64VMS-VMS821I\_PCSI-V0100 or later
  - HP-I64VMS-VMS821I\_UPDATE-V0300 or later
  - HP-I64VMS-VMS821I\_SYS-V0200 or later
  - HP-I64VMS-VMS821I\_FIBRE\_SCSI-V0200 or later
- **OpenVMS IA64 operating systems** - The OpenVMS IA64 operating system comes with the required ECOs and patches.

### Required Disk Space

The CIM extension for OpenVMS Alpha host requires 170 MB.

The CIM extension for OpenVMS IA64 host requires 400 MB.

### Network Port Must Be Open

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 294.

---

## Installing the CIM Extension

This section covers the following CIM extension installations for OpenVMS:

- “Installing the CIM Extension on a Standalone Host” on page 289
- “Installing the CIM Extension on a Cluster” on page 291

## Installing the CIM Extension on a Standalone Host

Keep in mind the following:

- The CIM extension on OpenVMS needs to be installed locally on each of the required hosts.
- You must be logged in using the “SYSTEM” account on each host to install the CIM extension for OpenVMS.

Follow these steps:

1. Log in as system.
2. Verify that the required ECOs and patches are installed; enter the following at the system prompt:

```
$ PRODUCT SHOW PRODUT/FULL
```

See “Prerequisites” on page 288 if needed.

3. 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 and OpenVMS IA64 8.2-1 is part of the following FIBRE\_SCSI ECO kits:
  - **OpenVMS Alpha 7.3-2** - DEC-AXPVMS-VMS732\_FIBRE\_SCSI-V0900 or later
  - **OpenVMS Alpha 8.2** - DEC-AXPVMS-VMS82A\_FIBRE\_SCSI-V0900 or later
  - **OpenVMS IA64 8.2-1** - HP-I64VMS-VMS8211\_FIBRE\_SCSI-V0200 or later for OpenVMS (IA64) 8.2-1.

---

**Note** – The SNIA HBA API library is shipped along with the operating system for OpenVMS Alpha 8.3 and OpenVMS IA64 8.3.

---

To verify the HBA supports the SNIA HBA API, check the OpenVMS host for the following files in the path specified:

```
$ DIRECTORY SYS$COMMON:[SYSLIB]HBA_VMS.EXE
$ DIRECTORY SYS$COMMON:[SYSLIB]HBA.CONF
```

4. Verify that the PIPE driver is installed by running the following command:

```
$ MCR SYSMAN IO SHOW DEVICE
```

Check for an entry similar to the following:

```

SYS$PIPEDRIVER
MPA 814D9F80 814DA000 814DA080
0 814D8F40

```

If SYS\$PIPEDRIVER is not listed, then the PIPE driver is not loaded. Run the following command to load the driver:

```
$ MCR SYSMAN IO CONNECT MPA0:/DRIVER=SYS$PIPEDRIVER/NOADAPTER
```

5. If the CD is already mounted, dismount it by entering:

```
$ DISMOUNT <CD-ROM device name>
```

6. Insert the CIM Extension CD-ROM in the CD-ROM drive.

7. Mount the CIM Extension CD-ROM by entering the following at the command prompt:

```
$ MOUNT /MEDIA=CDROM /UNDEFINED_FAT=STREAM:32767/OVERRIDE=
IDENTIFICATION DQB0 (or whichever is the CD-ROM device)
```

8. Change directory to the location of the OpenVMS Extension:

---

|                   |                              |
|-------------------|------------------------------|
| Alpha platforms   | \$ SET DEF DQB0:[OVMS.ALPHA] |
| Itanium platforms | \$ SET DEF DQB0:[OVMS.IA64]  |

9. Run the installation script by entering the following command:

```
$ @OVMSINST
```

10. Verify that the CIM extension process starts properly. You should see the following message:

```
CXWS now accepting 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 289 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

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. Enter the following command to start the CIM extension.

```
$ @SYS$COMMON:[OPT.APPQCIME.TOOLS]START
```

The following message is displayed:

```
STARTING OpenVMS CIME...
```

```
%RUN-S-PROC_ID, identification of created process is 00002976
```

```

```

```
Sun Oct 28 11:54:26 IST 2007
```

```
CXWS 6.0.0.269 on /127.0.0.1:4673 now accepting connections
```

```
Sun Oct 28 11:54:26 IST 2007
```

```
CXWS 6.0.0.269 on /15.154.53.91:4673 now accepting connections
```

---

## How to Determine if the CIM Extension is Running

You can determine if the CIM extension is running 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 `CIMEXTENSION.PARAMETERS` and is located in the `SYS$SPECIFIC:[OPT.APPQCIME.CONF]` directory on the host.



This directory also contains a file named `CIMEXTENSION.PARAMETERS-SAMPLE`. The `CIMEXTENSION.PARAMETERS-SAMPLE` file contains samples of available parameters which can be used as a template to create the `CIMEXTENSION.PARAMETERS` file.

## Restricting the Users Who Can Discover the Host

The `-USERS` parameter provides increased 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 fewer privileges, for example `jsmythe`. First, you would add the user to the parameters file. You would then log on 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 `SYS$SPECIFIC:[OPT.APPQCIME.CONF]` by entering the following command:

```
SET DEF SYS$SPECIFIC:[OPT.APPQCIME.CONF]
```

2. Open the `CIMEXTENSION.PARAMETERS` file in a text editor, and enter the following line:

```
-users jsmythe
```

where `jsmythe` is a valid OpenVMS user name.

---

**Note** – You can enter multiple users by separating them with a colon, as shown in the following example:

```
-users jsmythe:myname
```

---

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

---

**Note** – The CIM extension looks for parameters in the `CIMEXTENSION.PARAMETERS` file whenever it is started manually or when the host is rebooted.

---

## Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, follow these steps to change the port the CIM extension will access:

1. Go to `SYS$SPECIFIC:[OPT.APPQCIME.CONF]` by entering the following command:

```
SET DEF SYS$SPECIFIC:[OPT.APPQCIME.CONF]
```

2. Open the `CIMEXTENSION.PARAMETERS` file in a text editor, and enter 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 `CIMEXTENSION.PARAMETERS` file whenever it is started manually or when the host is rebooted.

---

## Adding a Port Number to Discovery

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 box, enter 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 `SYS$SPECIFIC:[OPT.APPQCIME.CONF]` by entering the following command:

```
SET DEFAULT SYS$SPECIFIC:[OPT.APPQCIME.CONF]
```

2. Open the `CIMEXTENSION.PARAMETERS` file in a text editor, and enter 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 `CIMEXTENSION.PARAMETERS` file whenever 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. See “Adding a Port Number to Discovery” on page 294.

## Additional Parameters

The following table describes additional parameters that can be specified in the `CIMEXTENSION.PARAMETERS` file:

**TABLE 14-1** Parameters for CIM Extensions

| Parameter                                                                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-port &lt;new port&gt;</code>                                                                 | The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See “Changing the Port Number” on page 294.                                                                                                                                                                                                                                                        |
| <code>-on &lt;ip address of NIC card&gt;</code>                                                     | Use this command to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See “Configuring the CIM Extension to Listen on a Specific Network Card” on page 295.                                                                                                                                                                                          |
| <code>-user</code>                                                                                  | The user defined in this parameter must be a valid existing 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 but the user must have the following system and process privileges: CMKRNL, SYSPRV and SYSLOCK. A colon-separated list can be used to specify multiple users. |
| <code>-credentials<br/>&lt;username from the<br/>management server&gt;<br/>:&lt;password&gt;</code> | 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.                                                                                                                                                                                                                                       |
| <code>-mgmtServerIP<br/>&lt;ip address&gt;</code>                                                   | Restricts the CIM extension to listen only to a specific management server IP address.                                                                                                                                                                                                                                                                                                                             |

---

## Finding the Version of a CIM Extension

To find the version number of a CIM extension:

1. Go to `SYS$COMMON:[OPT.APPQCIME.tools]` by entering the following command:

```
SET DEF SYS$COMMON:[OPT.APPQCIME.tools]
```

2. Enter the following at the command prompt:

```
$ @start -version
```

The version number is displayed.

---

## 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
- `1234` is the new port.

---

## Modifying the Boot Time Start Script (Optional)

When you install the CIM extension, its start script is put in the `SYS$COMMON:[OPT.APPQCIME.TOOLS]` directory with the file name `START.COM`. Optionally, this script can be used to start the CIM extension at boot time.

The following command must be included as the last line in the `START.COM` file:

```
$ @ SYS$COMMON:[OPT.APPQCIME.TOOLS]START
```

Parameters you can add when you manually start the CIM extension, such as `-port` and `-users`, can be enabled using the above command.

To modify the `SYS$STARTUP:SYSTARTUP_VMS.COM` file:

1. Open `SYS$STARTUP:SYSTARTUP_VMS.COM` in a text editor.
2. Find the following line of code:

```
$ EXIT
```

3. Add the following line before the line containing `$ EXIT`  
`$ @ SYS$COMMON: [OPT.APPQCIME.TOOLS] START`
4. Save the file.

The changes take effect the next time the script is executed when the host reboots.

---

## 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. Enter: `$ @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 `SYS$COMMON: [OPT.APPQCIME.TOOLS]` directory. The `CXWS_LOG` file rolls over once it becomes more than 30 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, with there being a maximum of three backup logs, as follows:

- `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, specify the desired log level 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 the CIM extension. It covers the following topics:

- “Uninstalling the OpenVMS CIM Extension on a Standalone Host” on page 299
- “Uninstalling the OpenVMS CIM Extension on a Cluster Host” on page 300

### Uninstalling the OpenVMS CIM Extension on a Standalone Host

To remove the CIM extension for OpenVMS on a standalone host:

1. Log in 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:

CIM Extension is Stopped...

The following product has been selected:

```
HP AXPVMS APPQCIME V6.0 Layered Product
```

The following product will be removed from destination:

```
HP AXPVMS APPQCIME V6.0 DISK$VMS_7_3_2:[VMS$COMMON.]
```

Portion done:

```
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
```

The following product has been removed:

```
HP AXPVMS APPQCIME V6.0 Layered Product
```

## 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 299 for each node on the cluster.



# Installing the CIM Extension for Sun Solaris

---

This chapter contains the following topics:

- “About the CIM Extension for Solaris” on page 301
- “Prerequisites” on page 302
- “Verifying SNIA HBA API Support” on page 303
- “Installing the CIM Extension” on page 304
- “Starting the CIM Extension Manually” on page 305
- “How to Determine if the CIM Extension Is Running” on page 306
- “Configuring CIM Extensions” on page 306
- “Stopping the CIM Extension” on page 311
- “Rolling Over the Log Files” on page 311
- “Removing the CIM Extension from Solaris” on page 312

---

**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 203.

---

---

**Caution** – 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.

---

**Caution** – 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/](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 the Solaris operating system has been installed.

You need the core set SUNWCreq. If you have only the core environment packages installed, install the following manually in the order listed:

1. SUNWlibC - Sun Workshop Compilers Bundled libC
2. SUNWlibCf - SunSoft WorkShop Bundled libC (cfront version)
3. SUNWlibCx - Sun Workshop Bundled 64-bit libC

Keep in mind the following:

- Solaris does not support the upgrading of the CIM extension. Before loading a new CIM extension, see “Removing the CIM Extension from Solaris” on page 312 to verify no agent exists.
- 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:

- **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.
- **Protection Explorer** - Make sure you have at least 500 MB if you are using the host as a master backup server in a large environment, for example 300 clients, 25,000 jobs and 500,000 images.

### 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 457.

---

## Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The `hbatest` program, which is accessible from the CIM Extension CD-ROM, lists the name and number for all HBAs 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.

Keep in mind the following:

- *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.
- The Emulex driver does not contain the required library that is required by the management server. You must install Emulex HBAnywhere software so that the management server can discover hosts configured with HBAnywhere and `hbatest` can detect the Emulex host bus adapter.

To run `hbatest`:

1. Go to the `Solaris/tools` directory on the CIM Extension 1 CD-ROM.

2. Enter the following at the command prompt:

```
./hbatest
```

The program runs its diagnostics.

Depending on the driver and version of the operating system, the SNIA API library may be installed with the driver or its utility program provided by the vendor. You can find the API library by entering the following at the command prompt:

```
more /etc/hba.conf
```

The following are examples of the library names and its path:

### Emulex

```
com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so
com.emulex.emulexapilibrary /usr/lib/sparcv9/libemulexhbaapi.so
```

### QLogic

qla2x00                    /usr/lib/libqlsdrm.so

## **JNI**

JniHbaLib /opt/JNIsnia/Solaris/Jni/32bit/JniHbaLib.so

JniHbaLib /opt/JNIsnia/Solaris/Jni/64bit/JniHbaLib.so

## **SUN Branded**

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:

- Solaris does not support the upgrading of the CIM extension. Before loading a new CIM extension, see “Removing the CIM Extension from Solaris” on page 312 to verify no agent exists.
- The instructions in this section apply if you are doing a local installation of the CIM extension, as opposed 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 following the instructions in this section, and then performing 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 4.2 and later of the CIM extension are compatible with this build of the management server.
- You must install the CIM extension for Sun Solaris to the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

To install the CIM extension:

1. Login as root.
2. Go to the Solaris directory on the CIM Extension 1 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 default directory

(/opt), and 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 312.

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 305.

---

## 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 458.

To start the CIM extension, enter 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 configurable text file that is read by the CIM extension at startup. The unconfigured file is named `cim.extension.parameters-sample` and is located in the `[Installation_Directory]/conf` directory on the host. This file contains samples of available parameters that will modify the behavior of the CIM extension and can be used as a template.

To manage the CIM extension using the parameters file:

1. Open the `cim.extension.parameters-sample` file and save a copy renamed as `cim.extension.parameters` to the same directory.
2. Edit the `cim.extension.parameters` file with the desired settings. See Table 15-1, "Parameters for CIM Extensions," on page 309.
3. Save and close the `cim.extension.parameters` file and then restart the service for the CIM extension by doing the following:

- a. Enter the following to go to the `tools` directory:

```
- cd /<Installation Directory>/tools directory
```

- b. Enter the following to stop the service:

```
- ./stop
```

- c. Enter the following to start the service:

```
- ./start
```

# 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 fewer privileges, for example `jsmythe`. First, you would add the user to the parameters file. You would then log on 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 enter the following line:

```
-users myname
```

where `myname` is a valid Solaris user name.

---

**Note** – You can enter 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 this port is already in use, 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 enter 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.

---

## Adding a New Port Number to Discovery

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 box, enter 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 enter 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. See “Adding a New Port Number to Discovery” on page 308.

## Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file:

**TABLE 15-1** Parameters for CIM Extensions

| Parameter                                       | Description                                                                                                                                                                                                               |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-port &lt;new port&gt;</code>             | The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See “Changing the Port Number” on page 307.                                                               |
| <code>-on &lt;ip address of NIC card&gt;</code> | Use this command to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See “Configuring the CIM Extension to Listen on a Specific Network Card” on page 308. |

**TABLE 15-1** Parameters for CIM Extensions (*Continued*)

| Parameter                                                            | Description                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -user                                                                | The user defined in this parameter must be a valid existing 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<br><username from the management server><br>:<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.                                                                                                                                        |
| -mgmtServerIP<br><ip address>                                        | This parameter restricts the CIM extension to listen only to a specific management server IP address.                                                                                                                                                                                                               |

## Finding the Version of a CIM Extension

To find the version number of a CIM extension:

1. Go to the `/opt/APPQcime/tools` directory.

2. Enter the following at the command prompt:

```
./start -version
```

The version number of the CIM extension and the date it was built are displayed, 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 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 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, with there being a maximum of three backup logs, as follows:

- `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 311.
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.
```

## Installing the CIM Extension for HP Tru64 UNIX

---

This chapter contains the following topics:

- “About the CIM Extension for Tru64 UNIX” on page 314
- “Prerequisites” on page 314
- “Installing the CIM Extension” on page 315
- “Verifying SNIA HBA API Support” on page 317
- “Starting the CIM Extension Manually” on page 318
- “How to Determine if the CIM Extension Is Running” on page 318
- “Configuring CIM Extensions” on page 319
- “Finding the Version of a CIM Extension” on page 322
- “Stopping the CIM Extension” on page 323
- “Rolling Over the Logs” on page 323
- “Fulfilling the Prerequisites” on page 324
- “Removing the CIM Extension from Tru64” on page 324

Keep in mind the following:

- 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 203.
- 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.
- The 6.0 management server requires that any managed Tru64 or OpenVMS hosts be running at least version 5.1.0 SP4 (5.1.4) of the CIM Extensions. If the Tru64 and OpenVMS CIM Extensions are not at the minimum levels, the 6.0.0 management server will be unable to gather information from those hosts, and there will be various replication errors in the management server logs. It is preferable to upgrade all CIM Extensions to the same version as the management server, as some functionality may be unavailable when earlier CIM Extensions are used.

---

# 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.

---

**Caution** – 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/](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 324.

Also, verify the following before you install the CIM extension:

### 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 box 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 box.

---

### 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 457.

---

## Installing the CIM Extension

---

**Caution** – You must install the CIM extension for Tru64 in the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

---

You can install the CIM extension for Tru64 in either of two ways:

- **On a Standalone Host** - See “Installing the CIM Extension on a Standalone Host” on page 315.
- **On a Cluster** - See “Installing the CIM Extension on a Cluster” on page 316.

## Installing the 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 drive 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 CD-ROM 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. Enter 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 a Standalone Host” on page 315.

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 following command 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 318.

---

## Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The hbatest program lists the name and number for all HBAs 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.

---

**Caution** – The Emulex driver does not contain the required library that is required by the management server. You must install Emulex HBAnywhere software so that the management server can discover hosts configured with HBAnywhere and hbatest can detect the Emulex host bus adapter.

---

To run hbatest:

1. Verify that you have installed the CIM extension.
2. Go to the /opt/APPQcime/tools/hbatest directory on the host where you installed the CIM extension.
3. Enter the following at the command prompt:

```
./hbatest
```

The program runs its diagnostics.

---

## Starting the CIM Extension Manually

The management server can only obtain information from this host when the CIM extension is running. 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 “Configuring CIM Extensions” on page 319 for more information. You can also access information about these topics by typing the following:

```
/start -help
```

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 458.

To start the CIM extension, enter 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...
```

---

## 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 fewer privileges, for example `jsmythe`. First, you would add the user to the parameters file. You would then log on 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 enter the following line:

```
-users myname
```

where `myname` is a valid Tru64 user name.

---

**Note** – You can enter 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 this port is already in use, 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 enter 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.

---

## Adding a New Port Number to Discovery

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 box, enter 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 enter 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. See “Adding a New Port Number to Discovery” on page 320.

## Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file:

**TABLE 16-1** Parameters for CIM Extensions

| Parameter                                                                                           | Description                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-port &lt;new port&gt;</code>                                                                 | The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See “Changing the Port Number” on page 320.                                                                                                                                                         |
| <code>-on &lt;ip address of NIC card&gt;</code>                                                     | Use this command to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See “Configuring the CIM Extension to Listen on a Specific Network Card” on page 321.                                                                                           |
| <code>-user</code>                                                                                  | The user defined in this parameter must be a valid existing 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. |
| <code>-credentials<br/>&lt;username from the<br/>management server&gt;<br/>:&lt;password&gt;</code> | 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.                                                                                                                                        |
| <code>-mgmtServerIP<br/>&lt;ip address&gt;</code>                                                   | This parameter 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. Enter the following at the command prompt:

```
./start -version
```

The version number of the CIM extension and the date it was built are displayed, 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, with there being a maximum of three backup logs, as follows:

- 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

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 324
- “Removing the CIM Extension from a Cluster” on page 325

### 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 324 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.



## Installing the CIM Extension for Microsoft Windows

---

---

**Caution** – Do not install the CIM extension onto the management server.

---

This chapter contains the following topics:

- “About the CIM Extension for Windows” on page 328
- “Verifying SNIA HBA API Support” on page 329
- “Installing the CIM Extension” on page 330
- “Installing the CIM Extension Using the Silent Installation” on page 331
- “Upgrading a Host with the Latest CIM Extension” on page 331
- “Configuring CIM Extensions” on page 332
- “Rolling Over the Log Files” on page 336
- “Removing the CIM Extension from Windows” on page 337

---

**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 203.

---

---

**Caution** – 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, devices and host bus adapters. It then makes the information available to the management server.

The CIM extension communicates with a host bus adapter (HBA) by one of two methods:

- The Microsoft HBAAPI.DLL
  - The Microsoft HBAAPI.DLL is available with Microsoft Windows 2003 SP1 and later. This is default method that the CIM extension uses.
  - The CIM Extension requires hbaapi.dll 5.2.3790.2753 which ships with Microsoft Windows 2003 SP2 or can be downloaded from Microsoft Knowledge Base KB922772 for earlier versions of Windows.
  - If you are running Windows 2000 or a version of the hbaapi.dll before version 5.2.3790.2753, the SNIA HBA API will be used.
- The SNIA HBA API (appiq\_hbaapi.dll)
  - The Host Bus Adapter Application Programming Interface (HBA API) created by the Storage Network Industry Association (SNIA).
  - The management server 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 website:  
[http://www.snia.org/tech\\_activities/hba\\_api/](http://www.snia.org/tech_activities/hba_api/)
  - The appiq\_hbaapi.dll file is installed as part of the CIM extension to provide access to the SNIA HBA API and it can be found in  
<Installation\_Directory>\CimExtensions\lib\.
  - The SNIA compliant HBA API provided by the HBA Vendor can be verified by checking the Windows registry for the following:

**For 32-bit operating systems** - \\HKEY\_LOCAL\_MACHINE\Software\SNIA\HBA

**For 64-bit operating systems** - \\HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\SNIA\HBA

To use the SNIA HBAAPI (appiq\_hbaapi.dll):

1. Set the following registry setting:

HKEY\_LOCAL\_MACHINE\SOFTWARE\AppIQ

2. Create a String Value named `HbaApiPath` with Value Data `<Installation_Directory>\CimExtensions\lib\appiq_hbaapi.dll`.
3. In the `<Installation_Directory>\CimExtensions\tools` directory on the host, the program `hbatest.exe` is available for testing if the HBA configuration is able to provide information.

---

## Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The `hbatest` program, which is accessible from the `<Installation_Directory>\CimExtensions\tools`, lists the name and number for all HBAs 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. Open a command window and change the directory to `<Installation_Directory>\CimExtensions\tools`.
2. Enter the following at the command prompt:

```
hbatest.exe
```

The `hbaapi.dll` must be upgraded or the SNIA HBA API must be used if the following configuration is used:

- You are using Emulex HBA's.
- The host has a version of `hbaapi.dll` that is earlier than version 5.2.3790.2753.
- The host is running HP MPIO multipathing.

When using Emulex HBA's and the SNIA library, remember that previous versions of HBAnyware provide the SNIA library; however, several later versions of HBAnyware do not ship with the SNIA library and rely upon the Microsoft SNIA library. Your configuration may require you to run the Emulex `setupelxhbaapi` program, which modifies the registry so that SNIA libraries can be detected by the CIM extension. To install the `setupelxhbaapi` program, download it from the Emulex website:

<http://www.emulex.com>

The `setupelxhbaapi` program installs the `hbaapi.dll` and Emulex `emulexhbaapi.dll` files into the program files\emulex\hbaapi folder and creates a registry key with the absolute path to the `emulexhbaapi.dll` file.

---

# Installing the CIM Extension

Keep in mind the following:

- You must have administrator privileges to install this software.
- 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 disable the “Explorer Enhanced Security Settings.”

Perform the following steps:

1. Insert the CD-ROM for the CIM extensions, go to the Windows directory, and 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 **Choose**. You can always display the default directory by clicking **Restore Default Folder**. When you are done, click **Next**.
5. Check the preinstallation summary. You are shown the following:
  - Product Name
  - Installation Folder
  - Version
  - Disk Space Information
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.
  - Click **Cancel** to exit the installer.

The CIM extension is installed.

7. When you have been told the installation is successful, click **Done** to quit the installation.

---

**Caution** – 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 extension.
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.

## Upgrading a Host with the Latest CIM Extension

When upgrading the CIM extension for Windows, the following issues may occur:

- The Host CIM Extension Version Report in Reporter still displays the previous version.
- The management server does not display the host bus adapter data for Windows hosts.

- File Server SRM scans are not possible.

To prevent these issues from occurring, perform the following steps:

1. Upgrade the management server.
  - **Sun Solaris** - See "Installing the Management Server on Sun Solaris" on page 49.
  - **Microsoft Windows** - See "Installing the Management Server on Microsoft Windows" on page 85.
  - **Linux** - See "Installing the Management Server on Linux" on page 7.
2. Upgrade the CIM extension on the Windows hosts. Install CIM extension over a previous version by following the installation steps as described in "Installing the CIM Extension" on page 330.

---

**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; for example they don't return FSRM data. It is strongly recommended you upgrade your CIM extensions on Windows as soon as possible.

---

3. On the management server, perform a discovery step 1 (**Discovery > Setup > Step 1**) for a re-discovery of the upgraded hosts. See "Discovering Applications, Backup Hosts and Hosts" on page 345 for more information about discovering hosts.
4. Do Get Details.
5. Refresh reports to update report data.

---

## Configuring CIM Extensions

Configuration information is stored in a configureable text file that is read by the CIM extension at start-up. The unconfigured file is named `cim.extension.parameters-sample` and is located in the `[Installation_Directory]\CimExtensions\conf` directory on the host. This file contains samples of available parameters that will modify the behavior of the CIM extension and can be used as a template.

To manage the CIM extension using the parameters file, do the following:

1. Open the `cim.extension.parameters-sample` file and save a copy renamed as `cim.extension.parameters` to the same directory.



2. Edit the `cim.extension.parameters` file with the desired settings. See Table 17-1, “Parameters for CIM Extensions,” on page 336.
3. Save and close the `cim.extension.parameters` file and then stop and restart the CIM service by rebooting the host or restarting the AppStorWin32Agent service from the Services window.

This section contains the following topics:

- “Changing the Port Number” on page 333
- “Configuring the CIM Extension to Listen on a Specific Network Card” on page 334
- “Defining UNC Volumes” on page 335
- “Additional Parameters” on page 336

## Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, follow these steps to change the port the CIM extension will access:

1. Go to the `[Installation_Directory]\CimExtensions\conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter 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.

---

## Adding a New Port Number to Discovery

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 box, enter 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]\CimExtensions\conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter 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. See “Adding a New Port Number to Discovery” on page 333.

# Defining UNC Volumes

You can use UNC shares to discover file system data from a server. If you want to scan UNC volumes, you must define them in a `UncShares.xml` file. To create the `UncShares.xml` file on a Windows host:

1. Confirm that a CIM extension is installed on the Windows host.
2. Go to the `<Installation_Directory>\CimExtensions\conf` directory.
3. Open the `UncShares.xml-sample` file in a text editor.
4. Identify the host through which the UNC shares' scan is planned. This is the host through which you will be scanning UNC shares from a different/remote host.
5. Add the host name and shared directory to the following line:

```
<!-- <UNC_SHARE PATH=" " /> -->
```

For example:

```
<UNC_SHARE PATH="\\RemoteSystem\MyShare1" />
```

Where `RemoteSystem` is the name of the host and `MyShare` is the name of the shared directory.

Repeat it for all of your shares, as shown in the following example:

```
<UNC_SHARE PATH="\\RemoteSystem\MyShare1" />
```

```
<UNC_SHARE PATH="\\RemoteSystem\MyShare2" />
```

```
<UNC_SHARE PATH="\\RemoteSystem\MyShare3" />
```

6. Save the file as `UncShares.xml`.
7. Restart the CIM Extension service on the managed host.
8. Update the element details for the host from the management server by running a Get Details
9. Edit the File System Viewer configuration page for the host selecting the desired UNC shares to scan.

The username and password combination you used for discovering the host should have at least read only permissions on the file shares which need to be scanned. So in most cases this would be a service account which you can have created in the active directory. This service account should be an admin on the “proxy FSV host” and should have read only (at least) access to the UNC share

---

**Note** – You can use the IP address of the host instead of the name.

---

If you want to discover multiple UNC shares which have different credentials, use different “proxy FSV hosts” as you can currently use only use one login / password pair [each UNC share has its own associated login / password in this release].

## Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file:

**TABLE 17-1** Parameters for CIM Extensions

| Parameter                                                                         | Description                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-user</code>                                                                | The user defined in this parameter must be a valid existing 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. |
| <code>-credentials</code><br><username from the management server><br>:<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.                                                                                                                                        |
| <code>-mgmtServerIP</code><br><ip address>                                        | This parameter restricts the CIM extension to listen only to a specific management server IP address.                                                                                                                                                                                                               |

## 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>/CimExtensions/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, with there being a maximum of three backup logs, as follows:

- `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 starting, stopping, and unexpected error conditions to the existing `cxws.out` file.

---

## Removing the CIM Extension from Windows

---

**Caution** – If you remove a CIM extension from a Windows host where there is a service that is using WMI (such as Microsoft Exchange), you are shown a message saying that the WMI service could not be stopped. Continue with the removal of the CIM extension. Reboot after the uninstall process completes.

---

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 **Change/Remove**.
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.



## Installing and Discovering the Windows Proxy

---

This chapter describes the following:

- “Installing the Windows Proxy” on page 340
- “Discovering the Windows Proxy” on page 341
- “Configuring Windows Proxy Authentication” on page 342
- “Decreasing the Maximum Java Heap Size” on page 343
- “Removing the Windows Proxy” on page 344

The Windows Proxy is required when the management server is on Sun Solaris or Linux and you want to obtain information from Microsoft Windows hosts that do not have a CIM extension installed. First, install the Windows Proxy as described in “Installing the Windows Proxy” on page 340. Then, discover the Windows Proxy as described in “Discovering the Windows Proxy” on page 341.

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 343.
- When the Windows proxy is installed on a new server, the Windows hosts must be re-discovered.

---

# Installing the Windows Proxy

---

**Caution** – 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 Utilities CD-ROM, 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.

---

**Caution** – Keep in mind that the Windows Proxy automatically starts when the system is restarted. The management server 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 341.



---

# Discovering the Windows Proxy

---

**Caution** – 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:

---

**Caution** – 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, “Discovering Applications, Backup Hosts and Hosts” on page 345.
  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.8=-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 **SUN 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.

## Discovering Applications, Backup Hosts and Hosts

---

This chapter describes the following:

- “Step 1 — Discovering Your Hosts and Backup Manager Hosts” on page 345
- “Step 2 — Setting Up Discovery for Applications” on page 353
- “Step 3 — Discovering Applications” on page 391
- “Changing the Oracle TNS Listener Port” on page 395
- “Changing the Password for the Managed Database Account” on page 395

---

### Step 1 — Discovering Your Hosts and Backup Manager 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 a CIM extension on the host if you want to obtain detailed information about the host and its applications, including those applications for backup. See the support matrix for information about which backup applications the management server supports.

For information about discovering clustered hosts, see “Host and Application Clustering” on page 399.

The management server automatically detects file 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 350.

The management server also detects the backup applications its supports, such as Veritas™ NetBackup™ or HP Data Protector. If you are licensed for Protection Explorer and you want to manage and monitor your backup applications, select **Include backup details** when you run Get Details, as described in “Step D — Get Details” on page 351.

Keep in mind the following:

- 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.
- Elements discovered through SMI-S and hosts discovered with CIM extensions from Build 5.1 and later of the product cannot be added to discovery groups. These elements are listed separately and can be placed independently into scheduled Get Details tasks without being part of a discovery group. This allows you greater flexibility when gathering discovery data. (For more information, see “Creating Custom Discovery Lists” on page 192).

If you are upgrading from a previous build of the product, and you rediscover your hosts, they will be moved out of their existing discovery groups. Each rediscovered host would be placed in its own discovery group. If the original discovery groups containing these hosts were included in scheduled Get Details tasks, the schedules would be modified to contain the new discovery groups for rediscovered hosts.

- After installing the CIM extension on a DataProtector system on Windows, check the Logon account for the DataProtector CRS service and verify that it matches the AppStorWin32Agent service. To determine the Logon account for the DataProtector CRS service, go to **Control Panel > Administrative Tools > Services**, select the DataProtector CRS service, access its Properties page, and select the **Logon** tab. To determine the Logon account for the AppStorWin32Agent service, go to **Control Panel > Administrative Tools > Services**, select the AppStorWin32Agent service, access its Properties page, and select the **Logon** tab.
- If you change the password of a host after you discover it, stop and restart the CIM extension running on the host, and change the host password in the discovery list.
- 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.
- If you want to receive status reports about Get Details, see “Configuring E-mail Notification for Get Details” on page 468 for information about how to configure this option.

- Depending on your license, you may not be able to access Protection Explorer, File Server SRM and/or monitor certain applications may not be available. See the List of Features to determine if you have access to Protection Explorer, File 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, see 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 490.
- Get Details can hang if obtaining information from an AIX host where SAN storage was previously available is no longer visible to the operating system. You may need to reboot the management server to resolve this issue.
- When discovering a Linux host from the management server, the operating system/server type is not available.
- If you started a CIM extension on a Sun Solaris host by using the `cim.extension.parameters` config file or 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.
- You can configure the management server to obtain information about your backup manager hosts at a set interval. See the topic, “Scheduling Backup Collection for Backup Managers” in the User Guide for more information about collectors.

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 347.
- **Topology** — Mapping the elements in the topology. See “Step B — Build the Topology” on page 350.
- “(Optional) Step C — View the Topology” on page 350
- **Details** — Obtaining detailed element information. See “Step D — Get Details” on page 351.

## Step A — Set Up Discovery for Hosts

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** box, enter the lowest IP address in the range of the elements you want to discover.
- d. In the **To IP Address** box, enter the highest IP address in the range of the elements you want to discover.
- e. In the **User Name (Optional)** box, enter 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)** box, enter the password corresponding to the user name entered in the User Name box.
- g. Enter the password from the previous step in the **Verify Password** box.
- h. In the **Comment** box, enter 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** box, enter the IP address or DNS name of the device you want to discover.
- d. In the **User Name (Optional)** box, enter the user name.

This box 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)** box, enter the corresponding password for the user name entered in the previous step.

This box 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 entered a password in the previous step, entered the password in the **Verify Password** box.
- g. In the **Comment** box, enter 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 DISCOVERY COMPLETED message is displayed in the Log Messages box.

## 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.

---

**Caution** – The management server’s 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 Log Message page is displayed by the management server. 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 478.

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 the **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 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 additional information about it. To learn more about fixing discovered and/or disconnected elements, see the topic, “Troubleshooting Topology Issues” on page 478.

## Step D — Get Details

After you obtain the topology of the network, you should obtain detailed information from the 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. Clusters won’t be recognized until Get Details is completed. Get Details must be run on all of the participating nodes of application clusters.

Keep in mind the following:

- Running Get Details takes 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 **Get Topology** on the Topology tab.

- Reports show data from the last successful Get Details and report cache update. When a scheduled Get Details finishes, the report cache refreshes automatically. If you run Get Details manually, the report cache updates every 6 hours. For information about refreshing the report cache, see the User Guide.
- During Get Details the data you see in the user interface is not updated until the data collection is finished.
- 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.
- You can use discovery groups to break up Get Details. For example, instead of running Get Details for all elements, you could specify only the elements in Discovery Group 1. For more information, see “Using Discovery Groups” on page 191.
- When an element in a discovery group is updated, its dependent elements are also updated.
- If you want to monitor and manage backup servers, select **Include backup details**. If you also want to manage and monitor the host itself, select **Include infrastructure details**; otherwise, the host appears as a generic element in the topology in System Explorer.
- If Get Details includes an AIX host, three SCSI errors (2 FSCSI error and 1 FCS error) per IBM adapter port are displayed in the system log. You can ignore these errors.
- You can quarantine elements to exclude them from Get Details. For example, if you want to get information about all the elements in a discovery group except for one, you can quarantine that element. For more information, see “Placing an Element in Quarantine” on page 197.
- If a problem occurs with a host or SMI-S element during Get Details, the host or element is automatically quarantined. To remove the element from quarantine, see “Removing an Element from Quarantine” on page 197.
- If you want to receive status reports about Get Details, see “Configuring E-mail Notification for Get Details” on page 468 for information about how to configure this option.

To obtain details:

1. Click **Discovery > Details** in the upper-right corner.
2. Verify the **Include backup details** option is selected if you want to monitor and manage backup applications in Protection Explorer.
3. Verify the **Include infrastructure details** option is selected. This option is required to manage and monitor your elements not related to the backup infrastructure.
4. 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 Get Details is finished GETTING ALL DETAILS COMPLETED is displayed on the View Logs page.

---

## 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 and Backup Manager Hosts” on page 345.

You can configure the management server to monitor hosts and applications, such as Oracle, Microsoft Exchange server, Caché, 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 installation guide.

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 and Backup Manager Hosts” on page 345, 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, map the elements in the topology, and then run 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 354
- “Monitoring Microsoft SQL Server” on page 363
- “Monitoring Sybase Adaptive Server Enterprise” on page 374
- “Monitoring Microsoft Exchange” on page 377
- “Monitoring Caché” on page 380

# Creating Custom Passwords on Managed Database Instances

Depending on the password policy, SQL Server 2005 may require that passwords be alphanumeric. For this reason, a managed SQL Server 2005 database instance might not accept the default managed database password (password) during APPIQ\_USER creation. A script is provided to input an alphanumeric password for SQL Server 2005. For all other applications, this script is optional.

Because the management server uses a single password for managing all types of databases, the script for specifying a custom password is provided for each managed database type (SQLServer, Oracle, Sybase, and Caché). If the password is changed on any managed database instance, you should run the respective custom password scripts for each of the other managed database instances, and specify the same password.

The script names for each database type are as follows:

**TABLE 19-1** Script Names for Managed Databases

| Database Type        | With Default Password                                      | With Custom Password                                                    |
|----------------------|------------------------------------------------------------|-------------------------------------------------------------------------|
| Oracle               | CreateOracleAct.sh (or .bat) or CRACCT.COM (for OpenVMS)   | CreateOracleActWithCustomPwd.sh (or .bat) or CUSTACCT.COM (for OpenVMS) |
| SQL Server           | CreateSQLServerAct.bat                                     | CreateSQLServerActCustomPwd.bat                                         |
| Sybase               | CreateSybaseAct.bat                                        | CreateSybaseActCustomPwd.bat                                            |
| Caché 5.0.20         | createCacheDB50User.sh (or .bat)                           | createCacheDB50UserCustomPwd.sh (or .bat)                               |
| Caché 5.2 and 2007.1 | createCacheDBUser.sh (or .bat) or CRUSER.COM (for OpenVMS) | createCacheDBUserCustomPwd.sh (or .bat) or CUSTUSER.COM (for OpenVMS)   |

After changing the password on all managed database instances, the password must be changed on the management server. To change the password on the management server:

1. Select **Discovery > Setup**.
2. Click the **Applications** tab.
3. Click **Change Password** in the Change Password for Managed Database Account section.
4. Enter the password that was used for creating APPIQ\_USER on the managed database instances.

# Monitoring Oracle

To monitor and manage Oracle, you must do the following:

- “Step A — Create the APPIQ\_USER Account for Oracle” on page 355
- “Step B — Provide the TNS Listener Port” on page 358
- “Step C — Set up Discovery for Oracle 10g” on page 359

After you complete these steps, you must discover Oracle, and perform Get Details. See “Step 3 — Discovering Applications” on page 391.

Keep in mind the following:

- 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.
- By default discovery of Oracle is not supported through autoscan. To enable autoscan, add the line - "oracleautoscan=true" in the Custom Properties window from the Advanced page in **Configuration > Product Health**. Then, click **Advanced** in the **Disk Space** tree. Auto scans are only supported for Oracle 9i. To discover Oracle 10g instances, you must enter the application information described “Step C — Set up Discovery for Oracle 10g” on page 359.

## 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 platforms) or `CRACCT.COM` (on OpenVMS) 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.

---

**Note** – To create the APPIQ\_USER with a custom password, run `CreateOracleActWithCustomPwd.bat` (on Microsoft Windows) or `CreateOracleActWithCustomPwd.sh` (on UNIX platforms) or `CUSTACCT.COM` (on OpenVMS). For more information, see “Creating Custom Passwords on Managed Database Instances” on page 353.

---

Keep in mind the following:

- The `CreateOracleAct.bat` script must run under SYS user.
- Create the APPIQ\_USER account on the 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. See 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.

- When creating the APPIQ\_USER account on an Oracle Real Application Cluster (RAC) Database, this script should be run only once, on any one of the instances of the Oracle RAC Database. Since all the instances of an Oracle RAC access the same Database, it is sufficient to create the APPIQ\_USER account on any one of the instances.
- 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 the 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/DBIQ/oracle/unix
```

where `/cdrom` is the name of the directory where you mounted the CD-ROM.

- **To run the script on Microsoft Windows**, go to the `DBIQ\oracle\win` directory on the CIM extensions CD-ROM.
- **To run the script on OpenVMS:**

Log into an account that has administrative privileges.

Mount the CIM Extensions CD-ROM (if not auto-mounted) using the following command.

```
$ MOUNT /MEDIA=CDROM
/UNDEFINED_FAT=STREAM:32767/OVERRIDE=IDENTIFICATION
DQB0
```

where `DQB0` is the CD-ROM drive.

Go to the directory containing the Oracle agent creation script using the following command.

```
$ SET DEF DQB0:[OVMS.DBIQ.ORACLE]
```

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 UNIX platforms) or `CRACCT.COM` (on OpenVMS) on the computer with the Oracle database. On OpenVMS, run



CRACCT.COM on the host using the following command.

```
$ @CRACCT.COM
```

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 the 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.
- Grants create session and select on dictionary tables privileges to APPIQ\_USER, enabling the 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 UNIX platforms) or `RMACCT.COM` (on OpenVMS).

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.

- When removing the APPIQ\_USER account from an Oracle RAC Database, this script should be run only once, on any one of the instances of the Oracle RAC Database. Since all the instances of an Oracle RAC access the same Database, it is sufficient to remove the APPIQ\_USER account from any one of the instances.

To remove the APPIQ\_USER account for that Oracle instance:

1. If you plan to remove the management software for Oracle from a UNIX platform, 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/DBIQ/oracle/unix
```

where /cdrom is the name of the directory where you mounted the CD-ROM.
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. If you plan to remove the management software for Oracle from a computer running OpenVMS do the following:
  - a. Mount the CIM Extensions CD-ROM (if not auto-mounted) using the following command:

```
$ MOUNT /MEDIA=CDROM
UNDEFINED_FAT=STREAM:32767/OVERRIDE=IDENTIFICATION
DQB0
```

where DQB0 is the CD-ROM drive.
  - b. Go to the directory containing the Oracle agent creation script using the following command:

```
$ SET DEF DQB0:[OVMS.DBIQ.ORACLE]
```
4. 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.
5. Run UninstallOracleAct.bat (on Windows) or UninstallOracleAct.sh or RMACCT.COM ( on OpenVMS).
6. This script removes the management software for the specified Oracle instance.

---

**Note** – You can use a remote Oracle client to run this script.


---

7. 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.
8. 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. Enter the new port number and click **OK**.
4. If necessary, click the  button to remove the old port number.

---

**Caution** – Monitoring Oracle 10g or Oracle clusters requires an additional step. If you are not monitoring Oracle 10g or Oracle clusters, go to “Step 3 — Discovering Applications” on page 391.

---

## Step C — Set up Discovery for Oracle 10g

---

**Note** – If you are discovering an Oracle cluster, see “Discovering Oracle Real Application Clusters (RAC)” on page 360.

---

---

**Note** – By default discovery of Oracle is not supported through auto scan. To enable autoscans, add the line - "oracleautoscan=true" in the Custom Properties window from the Advanced page in **Configuration** > **Product Health**. Then, click **Advanced** in the **Disk Space** tree. Autoscans are only supported for Oracle 9i. To discover Oracle 10g instances, you must enter the application information described in the following procedure.

---

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** box, enter the IP address or DNS name of the host running Oracle.  
The **Management IP/DNS Name** box is optional.
4. In the **Server Name** box, enter the Oracle System Identifier (SID) of the Oracle database you want to monitor.
5. In the **Port Number** box, enter 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.

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 Real Application Clusters (RAC)

Since Oracle RAC is an active-active application cluster, one RAC instance can provide information for the whole RAC. Regardless of the instance through which the database is accessed, the same sets of tables are accessed. This includes the data dictionary tables that are used to understand the logical and physical storage organization of the Oracle RAC application.

### Discovery of Oracle RAC Instances Using One Instance

Because one RAC instance can provide information for the whole RAC, it is possible to identify and discover all the instances in the Oracle RAC cluster from any one of its instances. This means that you can enter the application setup information for one instance of the Oracle RAC, and the management server will automatically discover the other instances, subject to certain conditions. The conditions to be satisfied for discovering all the instances of Oracle RAC using application setup information from one of its instances are as follows:

- Only the Oracle RAC instances running on hosts already discovered and identified as part of the same cluster will be discovered as part of the Oracle RAC on the management server.
- The management server is able to contact the hosts running Oracle RAC instances using the short host name. The management server can be configured to access the hosts running Oracle RAC instances using the short name in the following ways:
  - On the management server, add entries for each host running an Oracle RAC instance in `/etc/hosts` (on UNIX platforms) or `%WINDIR%\system32\drivers\etc\hosts` (on Windows).
  - Add the domain of the host in the domain search list of the management server under the search option of `/etc/resolv.conf` (on UNIX platforms) or Append these DNS suffixes (in order) on the **Advanced TCP/IP Settings > DNS** tab (on Windows).
- The listener is configured on the same IP address that is used to discover the host. For example, on the Application Setup page, the management IP address for the application should be the same as the host IP address.
- Typically, all the instances of Oracle RAC will be listening on the same TNS port number. If this is not the case, the port numbers for the other instances should be specified in the default port list in the Application Setup page. For example, if SID1 is listening on TNS port LP1, and SID2 is listening on TNS port LP2, then it is possible to automatically discover SID2, provided that TNS port LP2 is part of the default port list in the Application Setup page.

To discover Oracle RAC:

1. Install the CIM extension on each node in the cluster.
2. If the cluster is not automatically discovered by the management server, create the cluster using Cluster Manager. For more information about Cluster Manager, see “Host and Application Clustering” on page 399.
3. Create the APPIQ\_USER account on any one node in the cluster. See “Step A — Create the APPIQ\_USER Account for Oracle” on page 355.
4. Click **Discovery > Setup**, and 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 an IP Range for Scanning” on page 125.
5. Discover the first Oracle node as follows:
  - a. Select **Discovery > Setup**, and click the **Applications** tab.

- b. Click the **Create** button for the Database Information table.
- c. In the **Host IP/DNS Name** box, enter the IP address or DNS name of the host running Oracle.

In the **Management IP/DNS Name** box, enter 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` (on Windows)

`$ORACLE_HOME/network/admin/listener.ora` (on UNIX platforms)

- d. In the **Server Name** box, enter the Oracle System Identifier (SID) of the Oracle database you want to monitor.
- e. In the **Port Number** box, enter 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`

#### Unix Platforms:

`$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 = EXTPROC))
)
)
)
```

- f. Select **ORACLE** from the Database Type menu.
- g. Click **OK**.

6. If the conditions described in the “Discovery of Oracle RAC Instances Using One Instance” section are satisfied, then all the other instances in the Oracle RAC will also be discovered, and the Oracle RAC application cluster will also be constructed by the management server.
7. If the other instances of the Oracle RAC are not discovered in the previous step, repeat steps 4 and 5 for each node in the cluster.


### About Discovery of an Oracle RAC Application Cluster on a Host Cluster Discovered Using Cluster Manager

When the underlying host cluster is not discovered, the management server will be “Oracle RAC safe,” but not fully “Oracle RAC aware.” Each instance will show up as a standalone Oracle application, and data will be collected for each instance separately (even though both instances will return identical capacity data). However, the management server does not explicitly identify and construct the Oracle RAC application cluster. Also, when the underlying host cluster is not discovered, other instances of the Oracle RAC cannot be discovered automatically as described in the Discovery of Oracle RAC Instances Using One Instance section.

However, if you create the host cluster at a later point in time, subsequent discovery of any instance in Oracle RAC will identify and construct the Oracle RAC application cluster. The management server will shift to “Oracle RAC aware” mode on top of the host cluster that you created.

## Deleting Oracle Application Information

If you do not want the management server to monitor an Oracle 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 Oracle Application 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 SQL Server

---

**Note** – If you are planning to monitor Microsoft SQL Server clusters, see “Monitoring Microsoft SQL Server Clusters” on page 371

---

To manage and monitor Microsoft SQL Servers, you must do the following:

- “Step A — Create the appiq\_user Account for the Microsoft SQL Server” on page 365
- “Step B — Provide the Microsoft SQL Server Name and Port Number” on page 368

---

**Caution** – 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 364.

---

## Switching to Mixed Mode Authentication

---

**Caution** – 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:

### Microsoft SQL Server 2000:

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 and select **Properties**.  
The SQL Server Properties (Configure) window appears.
4. Click the **Security** tab.
5. For “Authentication,” select **SQL Server and Windows**.
6. If the SQL instance is a clustered instance, make sure that the Startup Service Account is that of a Domain Administrator account. If the SQL instance is not clustered, make sure that the Startup Service Account is that of System Account.

### Microsoft SQL Server 2005:

1. Open SQL Server Management Studio (**Start Menu > Programs > Microsoft SQL Server 2005 > SQLServer Management Studio**).
2. Connect to the Microsoft SQL Server 2005 instance.
3. Right-click the server name and select **Properties**. The SQL Server Properties (Configure) window is displayed.



4. Select **Security**.
5. For “Server Authentication,” select **SQL Server and Windows Authentication Mode**, and then click **OK**. You may be prompted to restart the SQL server.
6. Open SQL Server Configuration Manager (**Start Menu > Programs > Microsoft SQL Server 2005 > SQLServer Configuration Manager**). Make sure that the SQL instance is logged on with a Domain Administrator account if it is a clustered instance and System Account if it is a non-clustered instance.

## Step A — Create the appiq\_user Account for the Microsoft SQL Server

### Microsoft SQL Server 2000:

The management server accesses Microsoft SQL Server through the appiq\_user account. This account is created when you run the `CreateSQLServerAct.bat` or `CreateSQLServerActCustom.bat` script on the computer running the Microsoft SQL Server database you want to monitor. This account has create session and select dictionary privileges, which allow the management server to view statistics for the Microsoft SQL Server.

---

**Note** – For more information about creating the appiq\_user account with a custom password, see “Creating Custom Passwords on Managed Database Instances” on page 353.

---

Keep in mind the following:

- The script must run under the SA user account. 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
- 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 Microsoft SQL Server:

1. To run the script on Microsoft Windows, go to the `DBIQ\sqlserver\win` directory on the CIM Extensions CD-ROM.

---

**Caution** – 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. In a new command window, run the `CreateSQLServerAct.bat` script on the computer with the SQL Server database.

---

**Note** – You can use a remote SQL Server `isql` to run this script.

---

4. The script prompts you for the name of the Microsoft SQL Server on which to create the `appiq_user` account. If you are creating the account on a default instance, enter the host name if the instance is non-clustered and the `SQLNetwork Name` if the instance is clustered. If you are creating the account on a named instance, enter the host name and the instance name as follows:

**For a non-clustered instance:**

<Host Name>\<Instance Name>

**For a clustered instance:**

<SQL Network Name>\<Instance Name>

5. If you are running the `CreateSQLServerActCustom.bat` script, you will be prompted for a password for the `appiq_user` account. Provide a password that meets the password policy criteria described in “Creating Custom Passwords on Managed Database Instances” on page 353. If you are running the `CreateSQLServerAct.bat` script, the default password (`password`) is automatically used.
6. The script prompts you for the SA user password. Enter the password.  
The `appiq_user` account is created.
7. To determine if the `appiq_user` account was added correctly to your Microsoft 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. Click the refresh button in SQL Server Enterprise Manager. If the `appiq_user` is not listed, the management server is not able to discover the database.
8. 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.
9. Repeat these steps for each Microsoft SQL Server 2000 instance you want to manage.

### Microsoft SQL Server 2005:

The management server accesses Microsoft SQL Server through the appiq\_user account. To create this account, run the CreateSQLServerActCustomPwd.bat script on the computer running the Microsoft SQL Server database you want to monitor. This account has create session and select dictionary privileges, which allow the management server to view statistics for the Microsoft SQL Server.

Keep in mind the following:

- The script must run under the SA user account. 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
- 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 Microsoft SQL Server:

1. To run the script on Microsoft Windows, go to the DBIQ\sqlserver\win directory on the CIM Extensions CD-ROM.

---

**Caution** – 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. In a new command window, run the CreateSQLServerActCustomPwd.bat script on the computer with the SQL Server database.

---

**Note** – You can use a remote SQL Server isql to run this script.

---

4. The script prompts you for the name of the SQL Server on which to create the appiq\_user account. If you are creating the account on a default instance, enter the host name if the instance is non-clustered and the SQLNetwork Name if the instance is clustered. If you are creating the account on a named instance, enter the host name and the instance name as follows:

**For a non-clustered instance:**

<Host Name>\<Instance Name>

**For a clustered instance:**

<SQL Network Name>\<Instance Name>

5. The script prompts you for the password for the appiq\_user account. Provide a password that meets the password policy criteria described in “Creating Custom Passwords on Managed Database Instances” on page 353.
6. The script prompts you for the SA user password. Enter the password.  
The appiq\_user account is created.
7. To determine if appiq\_user was added correctly to your SQL server:
  - a. Open SQL Server Management Studio.
  - b. Expand the user interface for SQL Server Management Studio, and 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. Click the Refresh button in SQL Server Management Studio. If the appiq\_user is not listed, the management server is not able to discover the database.
8. To determine if the SQL Server is ready to accept connections from the management server:
  - a. Connect to the SQL Server installation through SQL Server Management Studio using the appiq\_user account and the password specified earlier.
  - 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.
9. Repeat these steps for each Microsoft SQL Server 2005 instance 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:

---

**Caution** – If you have name resolutions issues, your server may be discovered; however, your applications will not be discovered. You can address 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** box, enter the IP address or DNS name of the host running Microsoft SQL Server. You must provide the host name. You cannot use localhost or parenthesis.
4. You can leave the **Management IP/DNS Name** box blank. This box is for Oracle clusters. When you leave the **Management IP/DNS Name** box 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 box, enter 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. It is one of the following:

- The name specified at the time the SQL server was installed
- The Windows system name (Windows 2000)
- 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/SQL Server Management Studio, 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** box, enter the port that SQL is using.

To determine the correct SQL Port Number that the SQL Server is using, follow these steps:

#### **Microsoft SQL Server 2000**

- 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 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** box on the management server.

#### **Microsoft SQL Server 2005**

- a. Open SQL Server Configuration Manager.
  - b. Select the specific SQL Server 2005 Network Configuration entry for the SQL Server 2005 instance.
  - c. Select the TCP/IP entry on the right pane, and then click the Properties right click menu.
  - d. From the IP Addresses tab, obtain the Port Number configured for the instance. Provide this port number in the Port Number box on the management server.
7. Select **SQLSERVER** from the Database Type menu.
  8. Click **OK**.

---

**Caution** – Perform Get Details for your inputs to take effect. See “Step 3 — Discovering Applications” on page 391.

---

## Removing the appiq\_user Account for Microsoft SQL Server

---

**Caution** – 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 from the Microsoft 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.

---


**Caution** – 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 DropSQLServerAct.bat script on Microsoft Windows on the computer with the SQL Server database.
4. Enter the name of the SQL Server server.
5. Enter 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 Microsoft SQL Server Information

If you do not want the management server to monitor a Microsoft 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 Microsoft SQL Server Clusters

---

**Caution** – Make sure the Microsoft SQL Server cluster database is in “Mixed Mode authentication.” To switch to mixed mode authentication, see “Switching to Mixed Mode Authentication” on page 364.

---

To monitor and manage Microsoft SQL Server clusters:

1. Install CIM Extensions on each of the participating nodes.
2. Create the appiq\_user account as described in “Step A — Create the appiq\_user Account for the Microsoft SQL Server” on page 365.

---

**Note** – This step needs to be run on any one of the participating host nodes of the Microsoft SQL Server cluster.

---

3. Enter the server name and port number as described in “Provide the Microsoft SQL Server Name and Port Number for a Cluster” on page 372.

### *Provide the Microsoft SQL Server Name and Port Number for a Cluster*

The server name for the Microsoft SQL Server and port number for managing a Microsoft SQL Server cluster database must be provided in the following steps:

---

**Caution** – If you have name resolutions issues, your server may be discovered; however, your applications will not be discovered. You can address 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 Microsoft SQL Server cluster:

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** box, enter the IP address or DNS name of at least one of the participating host nodes running Microsoft SQL Server cluster. You must provide the host name. You cannot use localhost or parenthesis.
4. You can leave the Management IP/DNS Name box blank. When you leave the Management IP/DNS Name box 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 box, enter the SQL database server name you want to monitor.

The SQL Server name would be one of the following:

- The name specified at the time the SQL server was installed
- The Microsoft SQL Network Name (the default instance)

For example, if a Microsoft SQL Server cluster instance called SQLCLUSTER is running on a 2 node Windows 2003 cluster (individual host node IP address being 192.168.2.10 and 192.168.2.11) at the default SQL port (1433) and shows the name of Microsoft SQL Network Name within SQL Enterprise Manager / SQL Server Management Studio, the correct system application discovery settings on the management server would be either of the following:

- **Host IP/DNS Name:** 192.168.2.10
- **Database Server:** SQLCLUSTER
- **Port Number:** 1433
- **Database Type:** SQLSERVER

Or

- **Host IP/DNS Name:** 192.168.2.11
- **Database Server:** SQLCLUSTER
- **Port Number:** 1433
- **Database Type:** SQLSERVER

6. In the **Port Number** box, enter the port that SQL is using.

To determine the correct SQL Port Number that the SQL Server is using, follow these steps:

#### **Microsoft SQL Server 2000 Cluster**

- 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 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** box on the management server.

### Microsoft SQL Server 2005 Cluster

- a. Open SQL Server Configuration Manager.
  - b. Select the specific SQL Server 2005 Network Configuration entry for the SQL Server 2005 instance.
  - c. Select the TCP/IP entry on the right pane, and then click the Properties right click menu.
  - d. From the IP Addresses tab, obtain the Port Number configured for the instance. Provide this port number in the Port Number box on the management server. If Dynamic Ports are used, the Port Number is located under IPAll > TCP Dynamic Ports.
7. Select **SQLSERVER** from the Database Type menu.
  8. Click **OK**.

---

**Caution** – Perform Get Details for your inputs to take effect. See “Step 3 — Discovering Applications” on page 391.

---

## 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.

---

**Caution** – 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 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.

---

**Note** – To create the APPIQ\_USER with a custom password, run `CreateSybaseActCustomPwd.bat`. For more information, see “Creating Custom Passwords on Managed Database Instances” on page 353.

---

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.

---

**Caution** – 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 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. Enter 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

---

**Caution** – 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.

---

**Caution** – 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 the computer with the Sybase database.
4. Enter the name of the Sybase server.
5. Enter 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** box, enter the IP address or DNS name of the host running Sybase.
4. You can leave the **Management IP/DNS Name** box blank. This box is for Oracle clusters. When you leave the **Management IP/DNS Name** box 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** box, enter the Sybase database you want to monitor.
6. In the **Port Number** box, enter the port that Sybase is using.
7. Select **SYBASE** from the Database Type menu.
8. Click **OK**.


---

**Caution** – Perform Get Details for your inputs to take effect. See “Step 3 — Discovering Applications” on page 391.

---

## 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

---

**Note** – If you are planning to monitor Microsoft Exchange Clusters, see “Monitoring Microsoft Exchange Failover Clusters” on page 380.

---

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 (“Step 3 — Discovering Applications” on page 391).

## Adding Microsoft Exchange Domain Controller Access

Before adding a domain controller, note the following:

- The hosts should recognize the management server by name, because a reverse look-up is required by both operating system security and Microsoft Exchange. Make sure the domain controller, Exchange server host, and management server are accessible to one other using the host name and the fully-qualified domain name.

- The user name you provide must be the Common Name (CN) of the Active Directory User for accessing the Microsoft Exchange server. If you enter the Windows user name and it is different from the CN, the management server will not discover the Exchange instance.

To find the CN for a user on a domain controller server:

- a. Install the ADSIEdit MMC snap-in if it is not installed.
- b. Select **Start > Run** and enter `adsiedit.msc`.
- c. When the snap-in opens, expand the DOMAIN directory and navigate to the **CN=Users** folder to see the CN for each user in the Active Directory.

To provide information about your domain controllers:

1. Select **Discovery > Setup**, and then click the **Applications** tab.
2. In the Exchange Information section, click **Create**.
3. Click the **Add New Domain Controller** link.
  - a. In the Domain box, enter the domain name.
  - b. In the Domain Controller Name box, enter the fully qualified DNS name for the domain controller.
  - c. In the User Common Name box, enter the Common Name (CN) of the Active Directory User for accessing the Microsoft Exchange server.
  - d. In the Domain Password box, enter the corresponding password for accessing the Microsoft Exchange server.
  - e. In the Verify Password box, re-enter the password for verification.
4. Click **Add**.

The domain controller is added to the table.
5. Click **OK**.
6. Repeat these steps for each domain controller.
7. When all of your domain controllers are added, run `wmiadap /f` on the Exchange Server to refresh the Exchange data.

---

**Caution** – You must discover the host running Microsoft Exchange. See “Step 3 — Discovering Applications” on page 391.

---

## Editing a Microsoft Exchange Domain Controller

To provide information about your domain controllers:


1. Select **Discovery > Setup**, and then click the **Applications** tab.
2. Click the **Edit** button next to the Exchange domain controller you want to edit.
3. Enter a new User Common Name or Domain Password.
4. Click **Edit**.

The domain controller updates are added to the table.



Click **OK**.

## Deleting a Microsoft Exchange Domain Controller

To delete all of the domain controllers of a particular domain:

1. Select **Discovery > Setup**, then click the **Applications** tab.
2. Click the **Delete** () button corresponding to the domain you want to remove.
3. Run Get Details for your changes to take effect.

To delete a particular domain controller in a domain:

1. Select **Discovery > Setup**, then click the **Applications** tab.
2. Identify the domain for the domain controller you want to remove, and click the **Edit** () button corresponding to that domain.
3. In the Edit window, click the **Delete** () button corresponding to the domain controller you want to remove.
4. Run Get Details for your changes to take effect.

## Monitoring Microsoft Exchange Failover Clusters

To monitor and manage Microsoft Exchange Failover Clusters:



1. Install CIM Extensions on each of the participating nodes of Microsoft Exchange Failover Cluster.
2. Add information for Microsoft Exchange Domain Controller Access. See “Adding Microsoft Exchange Domain Controller Access” on page 378.
3. Perform Get Details on each of the participating nodes of the Exchange Cluster.

## Monitoring Caché

To monitor Caché, you must do the following:

- “Step A — Import the Wrapper Class Definitions into the Caché Instance” on page 380
- “Step B — Create APPIQ\_USER Account on the Caché Instance” on page 385
- “Step C — Provide the Caché Instance Name and Port Number” on page 390

After you complete these steps, you must discover Caché. See “Step 3 — Discovering Applications” on page 391.

---

**Note** – The required drivers for Caché were automatically installed along with the management server.

---

---

**Caution** – Before you begin these steps, make sure you purchased Caché IQ, which is the module that lets you monitor Caché. Contact your customer support if you are unsure if you purchased this module.

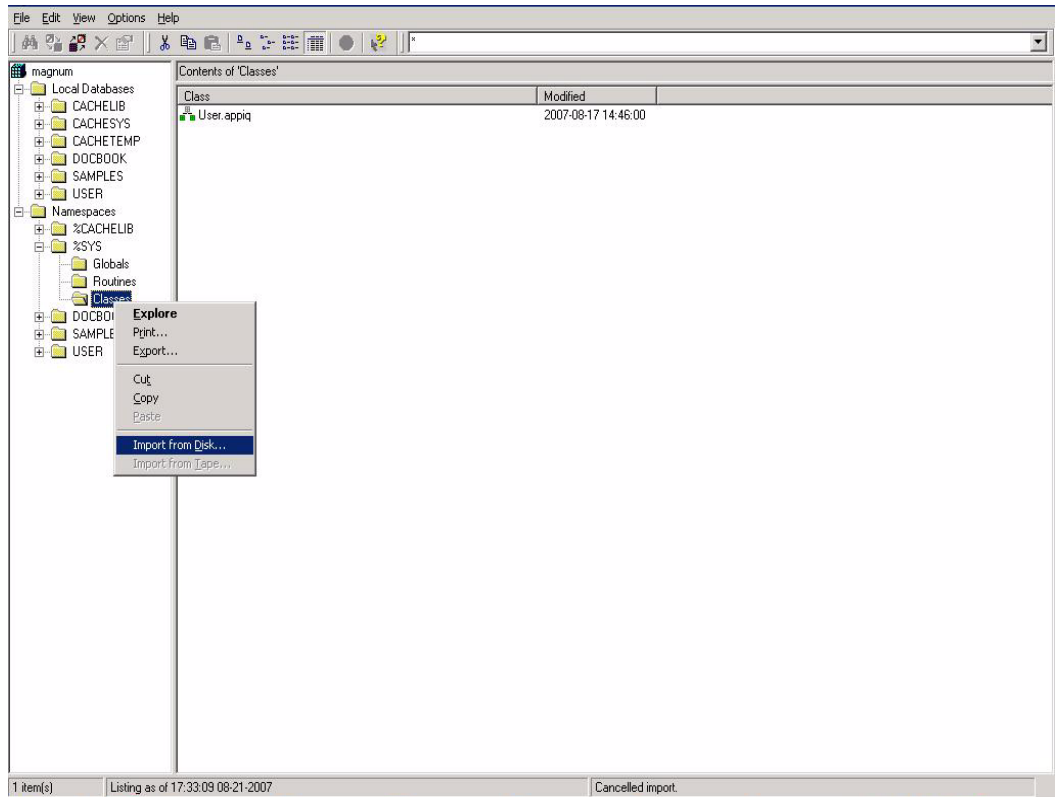
---

### Step A — Import the Wrapper Class Definitions into the Caché Instance

To import the wrapper classes:

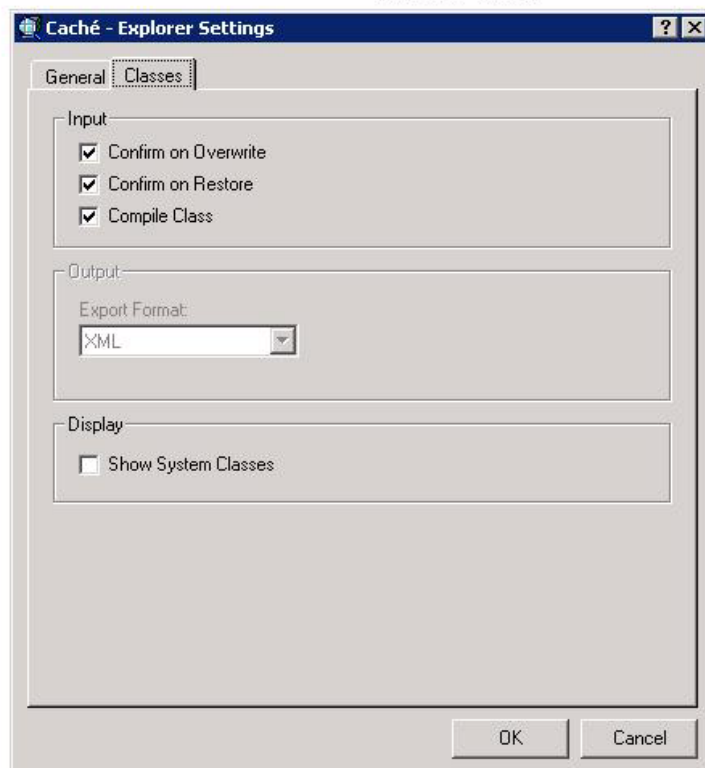
#### **For Caché 5.0 (5.0.20 onwards)**

1. Launch the Caché Explorer by right-clicking the Caché Cube icon in the system tray area of the Windows toolbar and selecting **Explorer**.
2. Right click the **Classes** folder located at **Namespaces > “%SYS” > Classes**.
3. Select **Import from disk**.



**FIGURE 19-1** Selecting Import from Disk

4. Browse the CIM Extension CD, select the wrapper xml file, and click **Open**.
  - On IBM AIX, Linux, or HP-UX, log into an account that has administrative privileges, and mount the CIM Extensions CD-ROM (if not auto-mounted). The wrapper file is  
`/cdrom/DBIQ/cachedb/unix/cachedb50_sqlprojs.xml`  
 where `/cdrom` is the name of the directory where you mounted the CD-ROM
  - On Microsoft Windows, the wrapper file on the CIM Extensions CD-ROM is  
`\DBIQ\cachedb\win\cachedb50_sqlprojs.xml`.
  - When the Import Classes window is displayed, click **Options**.
  - Select the **Classes** tab, enable the **Compile Class** checkbox, and click **OK**.



**FIGURE 19-2** Enabling Compile Class

5. In the Import Classes pop-up window, select `appiq.cls`, and click **Import**.

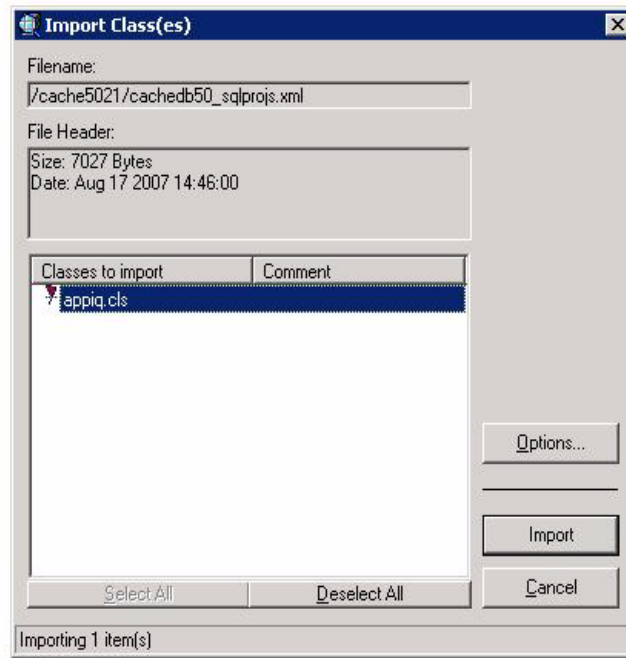


FIGURE 19-3 Selecting appiq.cls

### For Caché 5.2 and Caché 2007.1

1. Launch the Caché System Management Portal by right-clicking the Caché Cube icon in the system tray area of the Windows toolbar and selecting **System Management Portal**.
2. Click the **Classes** link under Data Management.
3. On the Classes page, select the **Namespaces** radio button, and then select **%SYS**.
4. Click **Import**.
5. Browse the CIM Extension CD, select the wrapper xml file, and click **Open**.
  - On IBM AIX, Linux, or HP-UX, log into an account that has administrative privileges, and mount the CIM Extensions CD-ROM (if not auto-mounted). The wrapper file is  
`/cdrom/DBIQ/cachedb/unix/cachedb_sqlprojs.xml`  
 where /cdrom is the name of the directory where you mounted the CD-ROM
  - On Microsoft Windows, the wrapper file on the CIM Extensions CD-ROM is  
`\DBIQ\cachedb\win\cachedb_sqlprojs.xml`.
  - On OpenVMS:

- a. Log in as system and mount the CIM Extensions CD-ROM.
- b. Copy the wrapper file (for example: `DQB0:[OVMS.DBIQ.CACHE]SQLPROJS.XML`), where `DQB0` is the CD-ROM drive, to any internal location on the OpenVMS host.

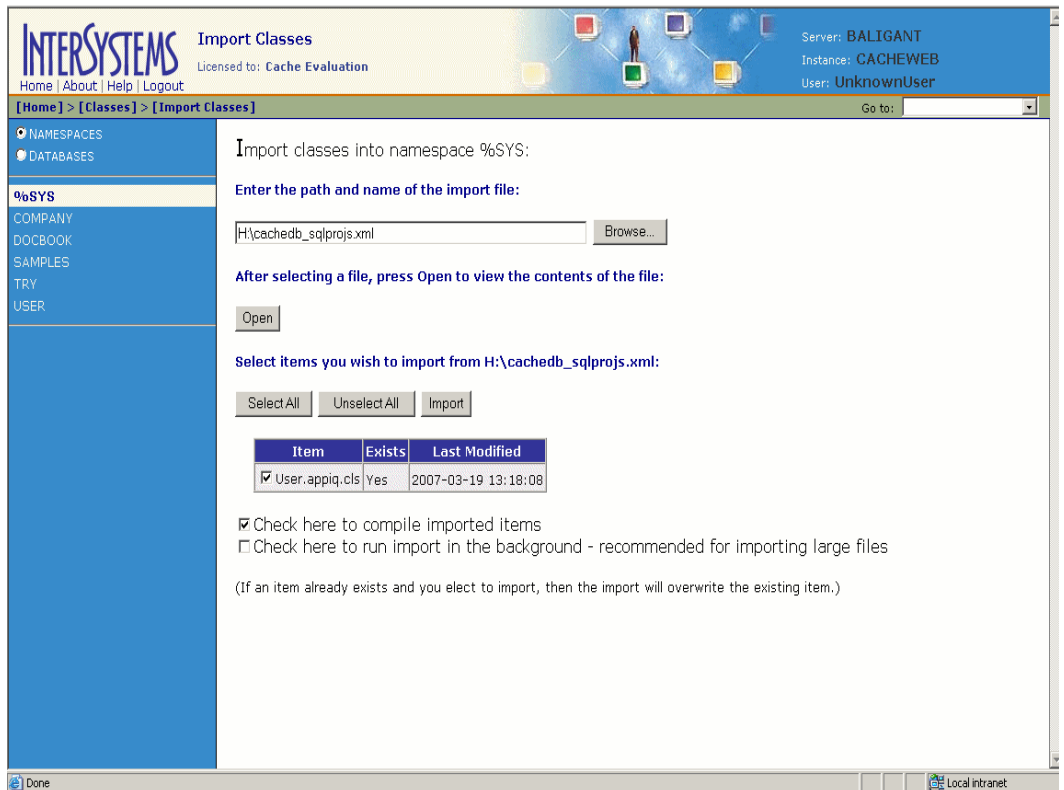
For example, copy `$DQB0:[OVMS.DBIQ.CACHE]SQLPROJS.XML`  
`$DKA0:[000000]SQLPROJS.XML`

where `DKA0` is a local drive on the OpenVMS host.

- c. Browse to `$DKA0` and specify `SQLPROJS.XML` within `$DKA0` as the import file.
6. After the file is opened, click **Select All**.
  7. Select **Check here to compile imported items**, and click **Import**.

The wrapper class definitions are imported into the Caché %SYS namespace.

The following image shows an example of importing the wrapper class definitions:



**FIGURE 19-4** Importing Wrapper Class Definitions

## Step B — Create APPIQ\_USER Account on the Caché Instance

The management server accesses Caché through the APPIQ\_USER account. This account is created when you run the appropriate script (described below) on the computer running the Caché database you want to monitor. You can execute these scripts from the management server also.

This script creates APPIQROLE with execute permissions for the SQL projections imported into the Caché managed instance, creates an APPIQ\_USER account, and assigns APPIQROLE to APPIQ\_USER.

The script must run as the \_SYSTEM user. You should enter the Caché server name, the Super Server port number, and the password of the \_SYSTEM user account as arguments for the script.

---

**Note** – If you are running Caché 5.2 or later, and the Caché instance was installed using “Locked Down” security mode, see “Locked Down Security Mode” on page 387 before creating the APPIQ\_USER account.

---

To create APPIQ\_USER for the Caché instance:

1. Do one of the following:

**To create APPIQ\_USER on the host:**

- To run the script on IBM AIX, HP\_UX, or Linux, log into an account that has administrative privileges, mount the CD-ROM (if not auto-mounted), and go to the  
/DBIQ/cachedb/unix directory by entering the following:

```
cd /cdrom/DBIQ/cachedb/unix
```

where /cdrom is the name of the directory where you mounted the CD-ROM .

- To run the script on Microsoft Windows, go to the DBIQ\cachedb\win directory on the CD-ROM.
- To run the script on OpenVMS, log in as system, mount the CD-ROM drive, and go to the [OVMS.DBIQ.CACHE] directory by entering the following:  
SET DEF DQB0:[OVMS.DBIQ.CACHE]

Where DQB0 is the name of the CD-ROM drive.

**To remotely create APPIQ\_USER on the Caché instance from the management server:**

- To run the script on Linux or Solaris, go to the /opt/<product name>/install/cachedb/unix directory by entering the following:  
# cd opt/<product name>/install/cachedb/unix
- To run the script on Windows, go to the %MGR\_DIST%\install\cachedb\win directory

2. Verify you have the password to the \_SYSTEM user account.
3. For Caché 5.0: run createCacheDB50User.bat (on Windows) or createCacheDB50User.sh (on UNIX platforms) on the computer with the CacheDatabase. To specify a custom password for the APPIQ\_USER account, run createCacheDB50UserCustomPwd.bat (on Windows) or createCacheDB50UserCustomPwd.sh (on UNIX platforms) on the computer with the CacheDatabase.

For later versions of Caché: run createCacheDBUser.bat (on Windows) or createCacheDBUser.sh (on UNIX platforms) or CRUSER.COM (on OpenVMS) on the computer with the CacheDatabase. To specify a custom password for the

APPIQ\_USER account, run createCacheDBUserCustomPwd.bat (on Windows) or createCacheDBUserCustomPwd.sh (on UNIX platforms) or CUSTUSER.COM (on OpenVMS) on the computer with the CacheDatabase.

4. Enter the Caché server name, the Super Server port number and the password of the \_SYSTEM user account as arguments for the script. If you are running the custom password creation script, enter the custom password as the fourth argument.

When invoking the scripts on OpenVMS, enclose the arguments in double quotes:

```
$ @CRUSER.COM "<host name>" "<super server port>" "<password for
_SYSTEM user>"
```

5. Repeat the previous step for each Caché instance you want to manage.

### *Locked Down Security Mode*

For Caché 5.2 and later versions, if the Caché instance was installed using “Locked Down” security mode, the following steps must be carried out before creating the APPIQ\_USER account:

1. Launch the System Management Portal.
2. Click the **Security Management** link under System Administration.
3. On the Security Management page, click **Services**.
4. Click **%Service\_Bindings** on the Services page.
5. On the Edit definition for Service %Service\_Bindings page:
  - a. Under Allowed Incoming Connections, click **Add** and enter the IP address of the management server in the Explorer User Prompt window.
  - b. If the create APPIQ\_USER scripts are being executed from the host on which Caché instance is running, add the IP address of the host.
  - c. Click the **Service Enabled** checkbox on the Edit definition for Service %Service\_Bindings page.
  - d. Click **Save**.
6. Click the **Security Management** link under System Administration in the System Management portal.
7. On the Security Management page, click the **Users** link .
8. Click the **Edit** link for \_SYSTEM user.



9. On the Edit Definition for User \_SYSTEM page, click the **User Enabled** checkbox and enter a password for the \_SYSTEM user in the Password and Confirm Password boxes.
10. Click the **Save** button.

Once the APPIQ\_USER has been created, the \_SYSTEM user can be disabled from the System Management portal.

## Removing the APPIQ\_USER Account from the Caché Instance

If you no longer want the management server to monitor a Caché instance, you can remove the APPIQ\_USER account and APPIQROLE for that Caché instance by running `dropCacheDBUser.bat` (on Windows) or `dropCacheDBUser.sh` (on UNIX platforms) or `DROPUSER.COM` (on OpenVMS).

Before you remove the APPIQ\_USER account from the Caché instances on a host, make sure no processes are running APPIQ\_USER for that Caché instance. The management server uses APPIQ\_USER to obtain information about a Caché instance. One of the ways to make sure APPIQ\_USER is not being used is to temporarily remove the host running Caché (**Discovery > Topology**). After you remove the APPIQ\_USER account for Caché, discover and perform Get Details for the host if you want to continue monitoring it.

For Caché 5.2 and later versions, if the Caché instance was installed using “Locked Down” security mode, ensure that the \_SYSTEM user has been enabled before trying to remove the APPIQ\_USER account. To ensure that the \_SYSTEM user has been enabled:

1. Launch the System Management Portal
2. Click the **Security Management** link under System Administration.
3. On the Security Management page, click the **Users** link.
4. Click the **Edit** link for \_SYSTEM user.
5. On the Edit Definition for User \_SYSTEM page, click the **User Enabled** checkbox and enter a password for the \_SYSTEM user in the Password and Confirm Password fields.
6. Click **Save**.

Once the APPIQ\_USER has been removed, the \_SYSTEM user can be disabled from the System Management portal. The %Service\_Bindings service that was enabled before creating the APPIQ\_USER can also be disabled.

To remove the APPIQ\_USER account:

1. Do one of the following:

**To remove the APPIQ\_USER account from the host:**

- To run the script on IBM AIX, HP\_UX, or Linux, log into an account that has administrative privileges, mount the CD-ROM (if not auto-mounted), and go to the  
/DBIQ/cachedb/unix directory by entering the following:

```
cd /cdrom/DBIQ/cachedb/unix
```

where /cdrom is the name of the directory where you mounted the CD-ROM

- To run the script on Microsoft Windows, go to the DBIQ\cachedb\win directory on the CD-ROM.
- To run the script on OpenVMS, log in as system, mount the CD-ROM drive, and go to the [OVMS.DBIQ.CACHE] directory by entering the following :  
SET DEF DQB0:[OVMS.DBIQ.CACHE]

Where DQB0 is the name of the CD-ROM drive.

**To remotely remove the APPIQ\_USER account from the Caché instance from the management server:**

- To run the script on or Solaris, go to the /opt/<product name>/install/cachedb/unix directory by entering the following:  
# cd opt/<product name>/install/cachedb/unix
- To run the script on Windows, go to the %MGR\_DIST%\install\cachedb\win directory

2. Verify you have the password to the \_SYSTEM user account.
3. For Caché 5.0, run dropCachedB50User.bat (on Windows) or dropCachedB50User.sh (on UNIX platforms) on the computer with the CacheDatabase. For later versions of Caché, run dropCachedBUser.bat (on Windows) or dropCachedBUser.sh (on UNIX platforms), or DROPUSER.COM (on OpenVMS) on the computer with the CacheDatabase.
4. Enter the Caché server name, the Super Server port number and the password of the \_SYSTEM user account as arguments for the script.

When invoking the scripts on OpenVMS, enclose the arguments in double quotes:

```
$ @DROPUSER.COM "<host name>" "<super server port>" "<password for _SYSTEM user>"
```

5. Repeat the previous step for each Caché instance you want to manage.

After deleting the APPIQ\_USER account from the Caché instance, you can also delete the wrapper class definitions.

### For Caché 5.0 (5.0.20 onwards)

1. Launch the Caché Explorer.
2. Click the Classes folder located at **Namespaces > “%SYS” > Classes**. Right-click the `User.appiq` class, and select **Delete**.
3. The Confirm Deletion window displays. Click **Yes**.

### For Caché 5.2 and Caché 2007.1

1. Launch the Caché System Management Portal.
2. Click the **Classes** link under Data Management.
3. On the Classes page, select the Namespaces radio button, and then click **%SYS**.
4. Click **Delete**.
5. Enter `User.appiq.cls` in the Enter search mask box, and click **Search**.
6. Select `User.appiq.cls`, and click **Delete**.

## Step C — Provide the Caché Instance Name and Port Number

To provide the Caché instance name and SuperServer port number for managing the Caché instance:

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 box, enter the IP address or DNS name of the host running Caché.
4. You can leave the Management IP/DNS Name box blank. This box is for clusters. When you leave the Management IP/DNS Name box 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 box, enter the Caché instance name you want to monitor.
6. In the Port Number box, enter the SuperServer port that Caché is using.
7. Select **Cache** from the Database Type menu.
8. Click **OK**.


---

**Caution** – Perform Get Details for your inputs to take effect. See “Step 3 — Discovering Applications” on page 391.

---

## Deleting Caché Information

If you do not want the management server to monitor a Caché 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 Caché instance you do not want the management server to monitor.
3. Perform Get Details to make the management server aware of your changes.

---

## 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 392)
- Obtain topology information about the application (“Step B — Obtain the Topology” on page 392)
- Perform Get Details (“Step C — Run Get Details” on page 393)

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 353.
- If you used a custom password for the APPIQ\_USER account, you must change the password on the management server before performing Get Details. See “Creating Custom Passwords on Managed Database Instances” on page 353.
- 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 **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.
- The Log Messages page is displayed. To view the status of discovery, click **Discovery > View Logs**.

The DISCOVERY COMPLETED message is displayed in the Log Messages box when Discovery is complete.

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 466.

## 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 187.

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 478.

If the topology for an element in your network changes, select the element and click **Get Topology** in **Discovery > Topology** to update 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 — Run 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 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, three SCSI errors (2 FSCSI error and 1 FCS error) per IBM adapter port are displayed in the system log. You can ignore these errors.

- You can quarantine elements to exclude them from Get Details. See “Placing an Element in Quarantine” on page 197 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 is unable to obtain information from an element during Get Details as a result of a CIM extension failure, 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 197 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 187.

3. Click **Get Details**.

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**.

The DISCOVERY COMPLETED message is displayed in the Log Messages box when Discovery is complete.

---

**Caution** – 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. See “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 447.

---

## 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.

---

**Caution** – 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** button for the **Oracle Information** table.
  3. Enter 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 466 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** boxes.

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. Enter a new password in the **Password** box.

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. Re-enter the password in the **Verify Password** box.
6. Click **OK**.
7. Verify that the management server can access the database applications by clicking the **Test** button for each database application.
- 8.



# Host and Application Clustering

---

This chapter contains the following topics:

- “About Clustering” on page 399
- “Discovering Clusters” on page 399
- “Clustering in System Explorer” on page 403
- “Clustering in Topology” on page 405
- “Clustering in Capacity Manager” on page 406

---

## About Clustering

The management server provides full support for managing clusters. Cluster support includes the following features:

- Clusters are recognized as managed elements.
- System Explorer supports clusters in all areas.
- The element topology shows which shared resources an application instance uses.
- Cluster capacity utilization is accurately reported.
- Capacity utilization trending is provided for applications running on clusters.

The management server supports automatic discovery of several popular cluster servers, and allows management of other clusters through Cluster Manager.

---

## Discovering Clusters

The following cluster services support automatic discovery:

- Microsoft Cluster Services (MSCS) on Windows 2003
- Veritas Clusters on Solaris

Cluster services that don't support automatic discovery can be discovered manually by using Cluster Manager. See "Manual Discovery of Host Clusters" on page 401.

The following application clusters are supported:

- Oracle Real Application Clusters (RAC)
- Microsoft Exchange 2000/2003 FailOver Clusters and 2007 Single Copy Cluster (SCC)
- Microsoft SQL Server 2000 and 2005

For information about discovering application clusters, see "Discovering Applications, Backup Hosts and Hosts" on page 345.

Refer to the support matrix for a complete list of supported configurations. The support matrix is accessible from the Documentation Center (**Help > Documentation Center**).

## Automatic Discovery of Host Clusters

MSCS on Windows 2003 and Veritas Clusters on Solaris support automatic discovery. To discover hosts using either of these cluster services:

9. Discover your hosts and applications as described in "Discovering Applications, Backup Hosts and Hosts" on page 345. The clusters are automatically recognized by the management server.

---

**Note** – The following optional steps describe how to select a preferred host from which shared resource capacity data will be collected.

---

10. *Optional:* Access Cluster Manager by right-clicking a cluster in System Explorer and selecting Edit Cluster. The Cluster Manager Overview page is displayed. Click **Next**.
11. *Optional:* Cluster Manager Step 2 (Select Preferred Host for Cluster Shared Resources) is displayed. Select a preferred host for each of the cluster shared resources. Keeping the default selection of "None" will result in shared resource capacity data being collected from an available active host that shares the resource. Choosing a particular active host results in the specified host being used for data collection. If the specified host becomes unavailable, an available active host is used for data collection.

Specify the preferred host for individual cluster shared resources. If a resource is not shared by the preferred host selection, the preferred host menu for that shared resource will continue to display the previous selection.

When you have finished specifying preferred hosts, click **Finish**.

# Manual Discovery of Host Clusters

If you are using a cluster service that doesn't support automatic discovery, you must manually create your clusters. For the list of cluster services that support automatic discovery, see "Discovering Clusters" on page 399.

---

**Note** – In some environments, using Cluster Manager to manually create a cluster with NetApp hosts may result in unsuccessful or incomplete cluster creation.

---

To manually discover clusters:

1. Discover your hosts and applications as described in "Discovering Applications, Backup Hosts and Hosts" on page 345.
2. Access Cluster Manager by right-clicking a host in System Explorer and selecting **Build Cluster**. The Cluster Manager Overview page is displayed. Click **Next**.
3. Cluster Manager Step 2 (Specify Cluster Properties and Cluster Members) is displayed. Follow these steps to specify the cluster properties and cluster members:
  - a. In the Cluster Properties section, specify the cluster name, cluster server, and cluster virtual IP.
  - b. In the Available Hosts section, select the hosts to add to the Cluster Members table. If desired, use the filter to assist in the selection of hosts. For details about the filtering functionality, see "Filtering Hosts" on page 402.

You may also use the Select Related Hosts button to facilitate the selection of hosts. Select a host in the table, and click **Select Related Hosts** to automatically select any related hosts.
  - c. After you have selected the hosts that you would like to add to the cluster, click **Add Selected Hosts to Cluster**. The selected hosts are added to the Cluster Members table.
  - d. Click **Next**.
4. Cluster Manager Step 3 (Specify Cluster Shared Resources) is displayed. Select **Automatic** or **Manual**. If you select Automatic, click **Display Cluster Shared Resources**, and the table at the bottom of the page is automatically populated.

If you select Manual discovery, follow these steps:

- a. Enter a name in the Cluster Shared Resource Name box.
- b. Select a resource type from the Resource Type menu. The menu includes the following resource types:

**Logical Disk**  
**Disk Partition**  
**Volume Manager Volume**  
**Disk Drive**

- c. Select the relevant resource for each cluster host, and click **Save Selections as Cluster Shared Resource**. The selections are added to the Cluster Shared Resources table.
  - d. Repeat steps a through c for each shared resource in the cluster.
  - e. Click **Next**.
5. Cluster Manager Step 4 (Select Preferred Hosts for Cluster Shared Resources) is displayed. Select a preferred host for each of the cluster shared resources. Shared resource capacity data will be collected from the specified node. Selecting "None" will result in no information being collected about the cluster shared resource.

Specify the preferred host for individual cluster shared resources. If a resource is not shared by the preferred host selection, the preferred host menu for that shared resource will continue to display the previous selection.

When you have finished specifying preferred hosts, click **Finish**.

## Filtering Hosts

The Available Hosts table on Cluster Manager Step 2 (Specify Cluster Properties and Cluster Members) allows you to filter the list of hosts displayed. To filter the list of hosts:

1. Click the **+ Filter** link to display the filtering options.  
If the volume filter is already displayed, the **- Filter** link is shown instead, which will collapse the filtering options.
2. Enter all or part of a volume name in the Name Contains box.
3. Select an operating system from the Operating System menu.
4. Enter all or part of a vendor name in the Vendor Contains box.
5. Enter a number in the Processors ( $\geq$ ) box.  
Hosts with at least as many processors as specified will display in the table.
6. Enter a number in the HBAs ( $\geq$ ) box.  
Hosts with at least as many HBAs as specified will display in the table.

7. Enter a number in the Ports ( $\geq$ ) box.

Hosts with at least as many ports as specified will display in the table.

8. Click **Filter**.

The table is updated to display only the elements that meet the filter criteria.

---

**Note** – To reset the filter criteria, click **Reset**.

---

## File Servers and Clusters

If you have marked a host as a file server and you move it into or out of a cluster, you must remove the file server data from the host and then re-mark it as a file server. To remove the file server data from the host and re-mark it as a file server:

1. Select **Configuration > File SRM**.

2. Verify that the **File Servers** tab is displayed.

3. Select the file servers you want to remove, and then click **Delete**.

4. Click **Add File Server**.

5. Click the check boxes for the hosts that you would like to mark as file servers.

6. Click **OK**.

The hosts are marked as file servers, and you are returned to the **File Servers** tab.

7. After removing the file server data from the host and then re-marking it as a file server, you must rescan the cluster member nodes and the cluster nodes. If a rescan is not completed, incorrect data may be displayed.

---

## Clustering in System Explorer

System Explorer has been enhanced to seamlessly support clusters in all areas. You can view connectivity information from all levels on a single canvas — from applications running on clusters, to the storage array spindles that share volumes for all the nodes of a cluster.

For detailed information about System Explorer, see “Viewing Element Topology and Properties” on page 354.





---

# Clustering in Topology

Element topology expands System Explorer's view to show exactly which shared resources a particular application instance uses. Individual paths from application nodes are listed in the path tree as well.

For detailed information about viewing element topology, see "Viewing Element Topology" on page 437.

In the following figure, individual instances of Microsoft Exchange Server 2003 share HP EVA virtual disk array group shared resources:

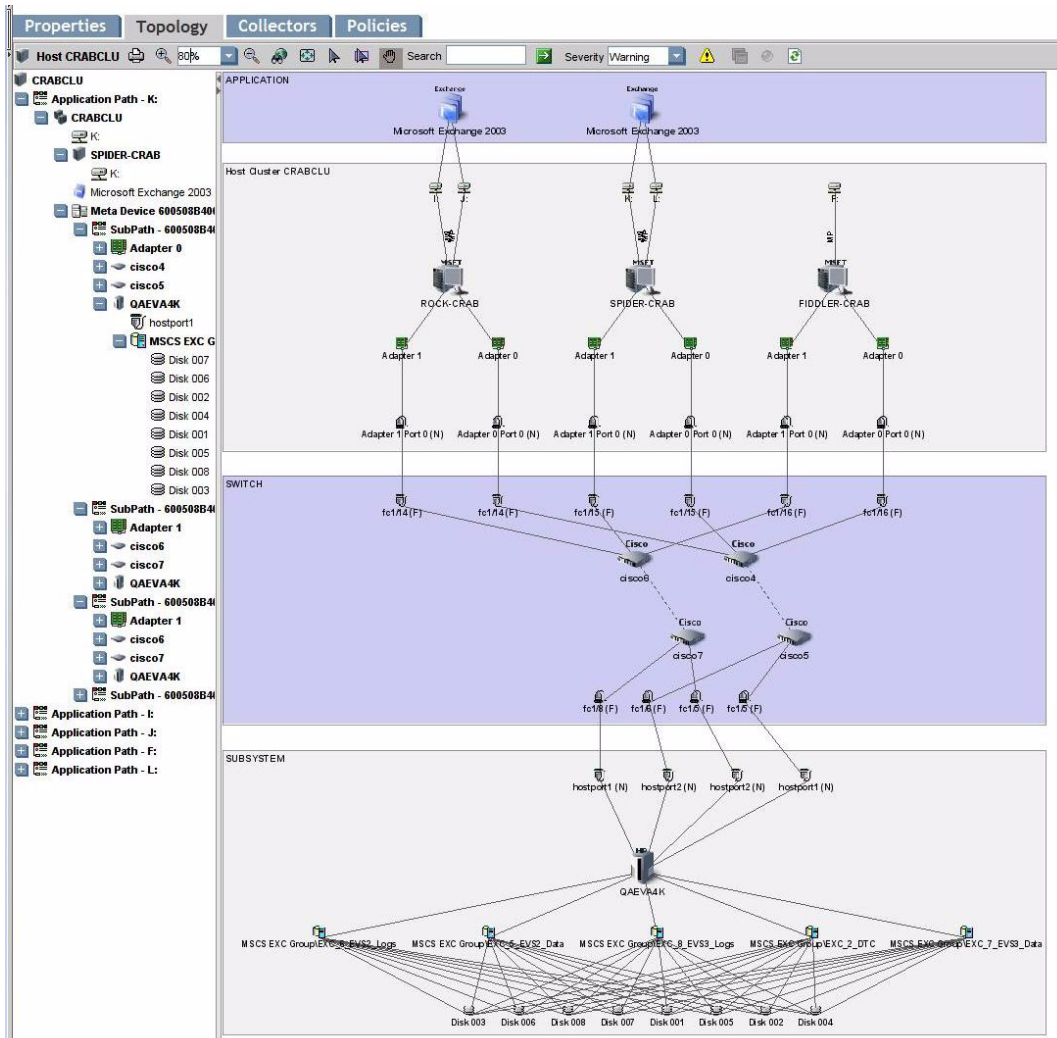


FIGURE 20-2 Cluster Element Topology Representation

---

# Clustering in Capacity Manager

In Capacity Explorer, it is possible to see the whole capacity utilization by the cluster. Clusters are represented as managed elements, and the capacity calculator intelligently avoids double counting of the capacity from individual nodes at the cluster level.

For detailed information about Capacity Explorer, see “Finding an Element’s Storage Capacity” on page 669.

You can drill down to various levels to see the following details of cluster capacity utilization:

- Whole cluster capacity
- Individual application instance capacity
- Individual cluster node capacity
- Capacity trending over a period of time
- Shared resources of individual nodes

The following figure shows an example of how clusters are represented in Capacity Manager:

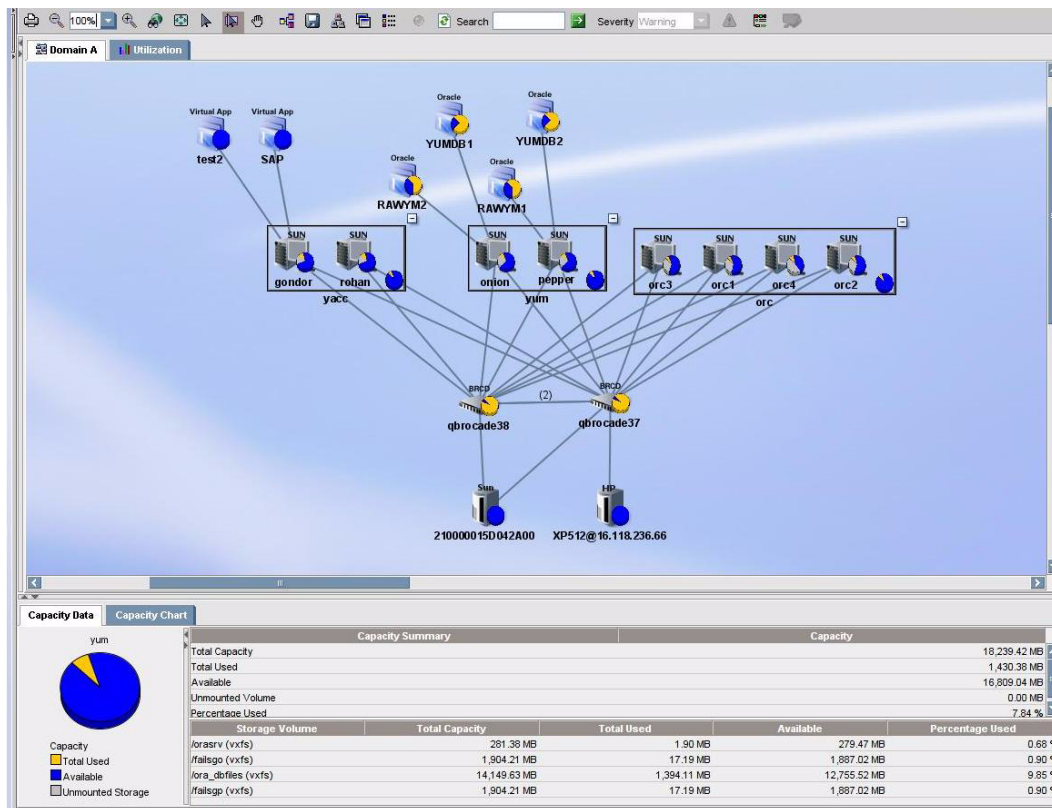


FIGURE 20-3 Capacity Manager Cluster Representation

## Managing Security

---

---

**Caution** – 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 contains the following topics:

- “About Security for the Management Server” on page 409
- “Managing User Accounts” on page 416
- “Managing Roles” on page 423
- “Managing Organizations” on page 426
- “Changing the Password of System Accounts” on page 432
- “Using Active Directory/LDAP for Authentication” on page 434

---

### About Security for the Management Server

The management server offers security based on the assignment of roles and organizations. Role-based security determines access to specific functionality depending on the user account assigned to a role. Organization-based security determines 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 410
- “About Organizations” on page 413
- “Planning Your Hierarchy” on page 415

- “Naming Organizations” on page 416

## About Roles

The management server ships with several predefined roles, which 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, Protection Explorer, and Reporter. Likewise, users assigned to the domain administrator role have access to all of the features, as shown in Table 21-1, “Default Role Privileges,” on page 410.

**TABLE 21-1** Default Role Privileges

| Feature                     | Role |                      |                       |                      |                           |           |
|-----------------------------|------|----------------------|-----------------------|----------------------|---------------------------|-----------|
|                             | CIO  | 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         |
| Protection Explorer         | 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                    |                       |                      |                           |           |

## *Granting Global Reporter Access*

Users with access to Global Reporter can view all 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.

## *Domain Administrator Role Privileges*

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.

## *System Configuration Option*

If the System Configuration option is selected for a role, all users assigned to that role will have the administration capabilities shown in the following list:

- 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

If you do not want users belonging to that role to have those capabilities, do not assign the System Configuration option.

## *Roles Used to Restrict Access*

Roles also restrict access to element properties, element records, and Provisioning, as shown in Table 21-2, "Default Role Privileges by Elements," on page 412.

**TABLE 21-2** Default Role Privileges by Elements

| Role                      | Element      |              |              |                |              |              |
|---------------------------|--------------|--------------|--------------|----------------|--------------|--------------|
|                           | 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         |
| Application Administrator | Full Control | View         | View         | View           | View         | View         |
| Help Desk                 | View         | View         | View         | View           | View         | View         |

### *Options for Restricting a Role*

In addition, you can assign one of the following options within a role to further allow or restrict access for a specific element:

- **Full Control** — Lets you view and modify the record for the element on the Asset Management tab, and perform provisioning if applicable.
- **Element Control** — Lets you view and modify the record for the element on the Asset Management tab. You cannot perform provisioning.
- **View** — Lets you only view element properties.

For example, if users belong to a role that only lets them view the element properties on storage systems, those users 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 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.

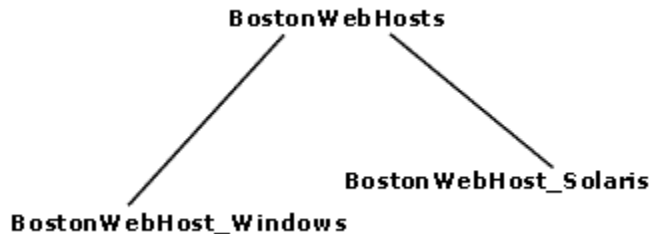


## About Organizations

You can use organizations to 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 assigned to an organization can see only the elements that belong to that 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. A user assigned to OnlyHosts and OnlySwitches 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. The figure below shows a parent-child hierarchy in which BostonWebHosts organization contains two child organizations, BostonWebHost\_Windows and BostonWebHost\_Solaris. BostonWebHosts is a parent because it contains two organizations.



**FIGURE 21-1** Parent-Child Hierarchy for Organizations

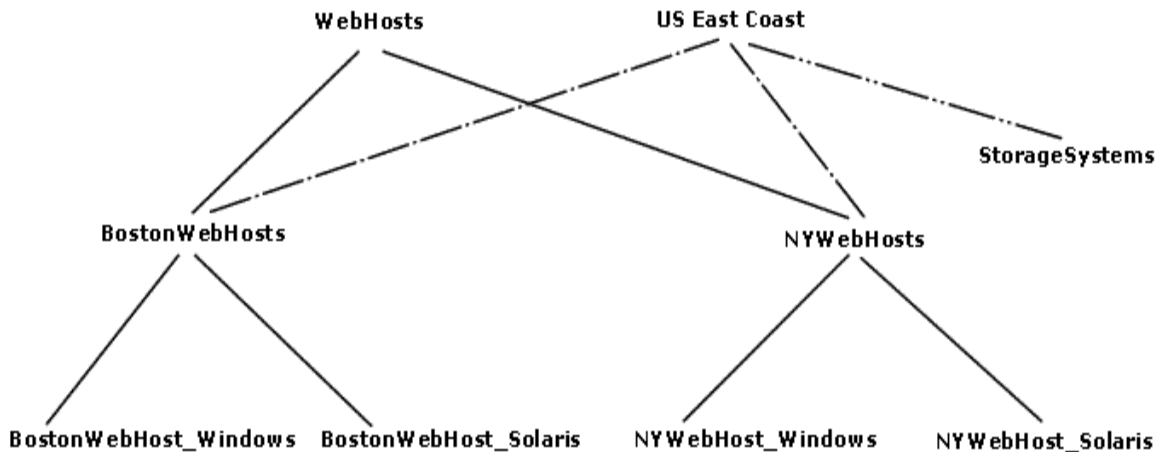
If a child contains organizations, it is also a parent. For example, if you add two organizations called BostonWebMarketing and BostonWebProduction to BostonWebHost\_Windows. BostonWebHost\_Windows would become a parent because it now contains two organizations. It would also be a child because it is 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; for example, when you add a new element, you need to add it only once; the change ripples through the hierarchy. For example, if you add an element to BostonWebHost\_Windows, not only users 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 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. For example, if you have a user that oversees all Web hosts in the company, you could assign that user 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. For example, if 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 21-2** 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 become 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 view all elements only 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.
- Events from all elements regardless of the user's organization are displayed by Event Manager.
- 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 when you email reports. If you do not have permission to access hosts, the reports you email, including the host-specific reports, will not contain information about hosts. 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? Or 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 a graphics illustration program, so you can keep track of which organizations are parents and children.

Create the child organizations first, then their parents. See “Adding an Organization” on page 426 for more information.

## Naming Organizations

When you create an organization, give it a name that reflects its members. 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 which are children. When you name an organization, you might want to include a portion of the name of the dominant parent organization. For example, if 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 contains the following topics:

- “Adding Users” on page 416
- “Editing a User Account” on page 418
- “Changing the Password for a User Account” on page 419
- “Changing Your Password” on page 420
- “Deleting Users” on page 420
- “Modifying Your User Profile” on page 420
- “Modifying Your User Preferences” on page 421
- “Viewing the Properties of a Role” on page 422
- “Viewing the Properties of an Organization” on page 423

## Adding Users

This section contains procedures for adding users and authorizing privileges. Only users belonging to the Domain Administrator role can add or modify users.

Keep in mind the following:

- On Windows and Sun Solaris systems — The user name and password must be alpha-numeric, and cannot exceed 256 characters. The user name cannot begin with a number.
- On Linux systems — The user name and password cannot exceed 256 characters.

To create an account:

1. Click **Security > Users**.
2. Click the **New User** button.
3. In the **Login Name** box, enter a name for the user account, for example: jsmith  
This name becomes the user name for the account.
4. (Optional) In the **Full Name** box, enter 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** menu. See “About Security for the Management Server” on page 409 for more information about roles.
6. (Optional) In the **E-mail** box, enter the user's e-mail address.
7. (Optional) In the **Phone** box, enter the user's phone number.
8. (Optional) In the **Notes** box, provide additional information about the user.
9. (Optional) In the **Password** box, enter 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 box blank.

---

10. (Optional) In the **Verify Password** box, enter 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 Security for the Management Server” on page 409 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.
- See “Domain Administrator Role Privileges” on page 411.
- User modifications take 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 444.

If you want to change your password, follow the steps in “Changing Your Password” on page 420.

To modify a user account:

1. Click **Security > Users**.
2. Click the **Edit** () button for the user account you want to modify.
3. To change the account name, enter a new name for the user account in the **Name** box; for example: jsmith  
This name becomes the user name for the account.
4. To change the name assigned to the user account, enter a new name for the account in the Full Name box.  
This information is used to provide a correlation between an account name and a user.
5. To change the role assigned to the user account, select a new role from the Role menu.
6. To change the e-mail address listed, enter a new e-mail address in the **E-mail** box.
7. To change the phone number listed, enter the user's new phone number in the **Phone** box.
8. Change or remove information from the **Notes** box if necessary.
9. To change the password:

- a. Click **Change Password**.
  - b. Enter a new password in the **Password** box.
  - c. Enter the password again In the **Verify Password** box.
  - 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.

---

**Note** – The Everything organization is the default organization that lets users access all current and future elements.

---

11. Click **OK**. The user account is updated.


## 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 menu.
3. Click the **Edit** button () corresponding to the user account you want to modify.
4. Click **Change Password**.
5. Enter a new password in the **New Password** box.
6. Enter the password again in the **Verify Password** box.
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 444 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. Enter a new password in the **New Password** box.
4. Enter the password again in the **Verify Password** box.
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, ask your Domain Administrator to make the changes.

To modify your user profile (other than name, role, and organization affiliation):

1. Click the name of your account in the upper-left corner.



**FIGURE 21-3** Clicking the Name of Your User Account

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 420. 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 **Save Changes**.

## Modifying Your User Preferences

Use the User Preference tab to modify your user preferences for System Explorer and Element Topology. 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.
2. Click the **User Preferences** tab.

## System, Capacity and Performance Manager Preferences

Select one of the following:

- **Load-on-Demand:** Does not populate the tree nodes or display elements in the topology when the page opens (Faster). Use this option for medium to large environments.
- **(Default) Automatic Loading:** Populate fabric tree nodes and display all elements in the topology when the page opens (Slower).

## 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 menu.

If you want events refreshed within a time period, select the **Refresh events automatically** box 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.

## Warnings for Slow Systems Operations

By default, the management server warns you when it encounters issues occurring when 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 421 for information on how to access the User Preferences tab.

## Viewing the Properties of a Role

If you are assigned the Domain Administrator role, you can determine which components a user can access by viewing the properties of the user's role.

To view the properties of a role:

1. Click **Security > Users**.
2. In the Role column, click the name of the role.

The following information for the selected role is displayed:

- 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** — How much access the user has to a type of element, such as hosts, storage systems, switches, and applications. See “About Security for the Management Server” on page 409 for more information.
- **Access to the <product name>** — 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 “Editing Roles” on page 424.

## Viewing the Properties of an Organization

If you are assigned the Domain Administrator role, you can determine which elements a user can access by viewing the properties of the user's organization

To view the properties of an organization:

1. Click **Security > Users**.
2. In the Organization column, click the name of a organization.
3. Take one of the following actions:
  - To determine which elements are in a child organization, click the link of the child organization.
  - To learn more about an element, click the element's link to display 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 Security for the Management Server” on page 409 for more information.

To learn how to edit an organization, see “Editing an Organization” on page 429.

---

## Managing Roles

This section contains the following topics:

- “Adding Roles” on page 424
- “Editing Roles” on page 424
- “Deleting Roles” on page 425

## 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 “About Security for the Management Server” on page 409 for more information about roles and organizations.

Keep in mind the following:

- The Role Name and Description boxes 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. Click **Security > Roles**.
2. Click **New Role**.
3. In the Role Name box, enter 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 box, enter a description for the role; for example: Role for those in quality assurance.  
The description cannot be more than 1024 characters.
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.  
See “Options for Restricting a Role” on page 412.
6. Select the features you want a user to be able to access.
7. Click **OK**.

## Editing Roles


The software lets you modify the default roles and/or the roles you have created. See “About Security for the Management Server” on page 409 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.
- After you click **OK** 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 box does not accept special characters, except spaces and the following characters: \$, -, ^, ., and \_

To edit a role:

1. Click **Security > Roles**.
2. Click the **Edit** () button.
3. Make the desired changes:
  - To edit the name of the role, change the name in the Role Name box. The name can contain spaces, but it cannot be longer than 256 characters.
  - To edit the description of the role, change the description in the Description box. The description cannot be more than 1024 characters.
  - 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.

See “Options for Restricting a Role” on page 412.
4. Select the features you want a user to be able to access.
 

See “Management Server Components” on page 9 for more information about these features.
5. 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. Click **Security > Roles**.
2. Select **Roles** from the menu.

3. Click the corresponding **Delete** button (.

The role is deleted.

---

## Managing Organizations

This section contains the following topics:

- “Adding an Organization” on page 426
- “Viewing Organizations” on page 428
- “Editing an Organization” on page 429
- “Removing an Organization” on page 430
- “Removing Members from an Organization” on page 430
- “Filtering Organizations” on page 431

## Adding an Organization

You can create new organizations to restrict access to certain elements. For example, if 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 will only be able to access the elements you specified.

See “About Security for the Management Server” on page 409 for more information about roles and organizations.

Keep in mind the following:

- Create child organizations first, then their parents.
- Events from all elements regardless of the user’s organization are displayed by Event Manager.
- 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.
- Moving a cluster from one organization to another moves all of the cluster’s nodes to the target organization.

To add an organization:

1. Click **Security > Organizations**.

2. Click the **New Organizations** button.

3. In the **Name** box, enter 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 caret (^) symbol—currently the system allows the caret symbol to be entered, but the caret symbol should not be included in an organization's name.

4. In the **Description** box, enter a description for the organization.

The Description box cannot have more than 1024 characters.

5. Click **Add or Remove Members** to determine which elements the user will see.

6. To add elements:

- a. Expand the Element Types node in the tree, and select the element type that you would like to add.
- b. In the right-hand pane, select the elements you would like to add by clicking the appropriate check boxes.
- c. Click **Add**.
- d. The selected elements are added to the Organization Members pane. To add storage volumes to the organization, see "Adding Storage Volumes to an Organization" on page 427.

7. To add organizations:

- a. Click the **Organizations** node.
- b. In the right-hand pane, select the elements you would like to add by clicking the appropriate check boxes.
- c. Click **Add**. 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 "About Security for the Management Server" on page 409 for more information.

8. Click **OK** when you are done adding the elements and organizations.

## 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 **Add or Remove Members**.
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 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 **Submit Query**.
5. Select the storage volumes you want to add to the organization. Click the **+Ports** link in the Ports column 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.
7. Click **OK**. The selected volumes are added to the Organization Members pane.

## Viewing Organizations

The Setup Organizations page lists the organizations with their descriptions. The page also shows 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 directly to an organization. This number does not include those within the child organization. A zero (0) in the Elements column indicates that the organization contains only child organizations; 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**.

To access information about a child organization, click its link in the Child Organization column.



# Editing an Organization

When elements are removed from an organization, users belonging only to that organization are no longer able to access the removed elements.

See “About Security for the Management Server” on page 409 for more information about roles and organizations.

Keep in mind the following:

- Depending on your license, role-based security may not be available. See the List of Features accessible from the Documentation Center.
- Only users belonging to the Domain Administrator role can edit organizations.
- Only active organizations can be edited.
- You cannot edit the Everything organization.

To edit an organization:

1. Click **Security > Organizations**.

2. Click the Edit () button.

3. To change the name of the organization, enter a new name in the Name box.

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 include special characters, except spaces and the following characters: \$, -, ., and \_
- Cannot contain the carot (^) symbol.

4. To change the description of the organization, enter a new description in the **Description** box.

You cannot enter more than 1024 characters in the **Description** box.

5. Click **Add or Remove Members**.

6. Add or remove elements as described in “Adding an Organization” on page 426 and “Removing Members from an Organization” on page 430.

7. Once you are done adding or removing elements, click **OK** in the Add Organization or Remove Organization page.

8. In the Edit Organization page, click **OK**.


## Removing an Organization

When an organization is removed, users assigned only to that organization are no longer able to access its elements. 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.
- Only users belonging to the Domain Administrator role can delete organizations.
- 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.

To delete an organization:


1. Click **Security > Organizations**.
2. Click the Delete () 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 become 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.

Use one of the following methods to remove an element from an organization:

- In the Edit Organization window, click the Delete () 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, and then click **Remove**.

- Only users belonging to the Domain Administrator role can remove members from an organization.


## Filtering Organizations

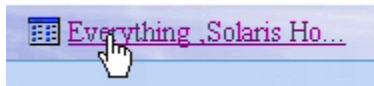
The management server provides a filtering feature that lets you designate which organizations are active in your view. For example, assume you belong to an organization name Hosts and this organization contains two organizations: WindowsHosts and SolarisHosts. If you want to view elements only in WindowsHosts and not in SolarisHosts organizations, you could use the filtering feature to activate only the WindowsHosts 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 the filtering feature for organizations.
- If you do not want to view an element, deselect all child organizations containing that 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 SolarisHosts organization. The SolarisHosts organization is contained in the Hosts organization. You must deselect the SolarisHosts organization and the Hosts organization if you do not want to see the Solaris hosts.
- The filter for organizations does not appear in Event Manager. Events from all elements regardless of the user's organization are displayed by Event Manager.
- 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 21-4** Clicking the Organization Link

2. Deselect the organizations that contain the elements you do not want to obtain information about. For example, if you want to view only the elements in the WindowsHosts organization, you would select only WindowsHosts. If you have a parent organization named Hosts that contains SolarisHosts and WindowsHosts, you would need to deselect SolarisHosts and Hosts. You would need to deselect Hosts because it contains organizations other than WindowsHosts.

If you belong to the Domain Administrator role, links are displayed for the organizations. To learn more about the contents of an organization, click its link.

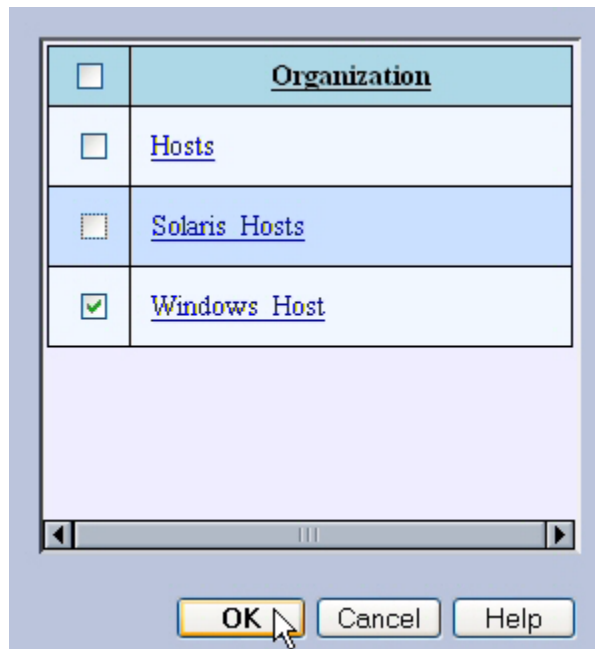


FIGURE 21-5 Filtering Organizations

3. Click **OK**.

You can now only obtain information about elements in the active organizations. These active organizations are listed in the link next to the filter button, as shown in the following figure.



FIGURE 21-6 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 to create and update the management server database. Default password: `change_on_install`
- SYSTEM — Used to create and upgrade, import, export and re-initialize the management server database. 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`

To change the passwords of the SYS, SYSTEM, RMAN\_USER, and DB\_SYSTEM\_USER accounts, you must use the Database Admin Utility, so the management server is aware of the changes. Do not change the password for any 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 password requirements for the management server are:

- Must have a minimum of three characters
- Must start with a letter
- May contain only letters, numbers and underscores (`_`)
- May not start or end with an underscore (`_`)

To change the password of a system account:

1. Access the Database Admin Utility as described in “Accessing the Database Admin Utility” on page 277.
2. Click **Change Passwords** in the left pane.
3. Select an account name from the User Name box.
4. Enter the current password in the Old Password box.
5. Enter the new password in the New Password box.
6. Re-enter the password in the Confirm Password box.
7. 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 that 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 both AD and LDAP. It is important to enable either AD 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`.
- Business Tools do not work when the management server is configured for AD/LDAP authentication.

To use AD/LDAP to authenticate your users, complete the following procedures:

- “Step 1 — Configure the Management Server to Use AD or LDAP” on page 434
- “Step 2 — Restart the AppStorManager Service and Login as the Designated Admin Account” on page 443
- “Step 3 — Add Users to the Management Server” on page 444
- “Step 4 — Provide Login Information to Your Users” on page 444

## Step 1 — Configure the Management Server to Use AD or LDAP

If you want to use AD/LDAP, you must modify the `login-handler.xml` file. How you modify the `login-handler.xml` file depends on whether you plan to use AD or LDAP.

To configure the management server:

- To use AD, see “Configuring the Management Server to Use Active Directory” on page 435
- To use LDAP, see “Configuring the Management Server to Use LDAP” on page 439

## Configuring the Management Server to Use Active Directory

By default, AD allows connections with `domain\username`, instead of with the distinguished name (DN) used by a generic LDAP server. However, you can use the generic LDAP server setup to authenticate with AD, as described in “Configuring the Management Server to Use LDAP” on page 439.

To specify the management server to use AD:

1. Before switching to AD authentication mode, the management server needs to be configured with a designated AD user and other AD-specific credentials. At startup, the designated AD user is mapped to the built-in Admin user and overrides it with the AD user information.

---

**Caution** – Make sure the administrator account has already been created in AD 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`

**UNIX systems:** `$MGR_DIST/Data/Configuration`

- b. In the `login-handler.xml` file, change the value of the `<AdminAccountName>` tag to the name of a user account in AD, 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 AD.

For security reasons, it is recommended that the designated user not be the AD Domain Administrator

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.ActiveDirectoryLoginHandler</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 AD.
- 389 is the port on which AD 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 AD.

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 allows a user to also 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 AD 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.



---

**Caution** – 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 AD and one for LDAP. Make sure you also change the value of the <CaseSensitiveUserName> tags that are children of the <ActiveDirectory> tag.

9. Provide the AD 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</LDAP
Env>
-->
<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>

```

## Configuring the Management Server to Use 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.

---

**Caution** – 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`

**UNIX systems:** `$MGR_DIST/Data/Configuration`

- 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</Logi
nHandlerClass-->

```

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 allows a user to also 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 AD 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. For example, the management server sees `MyUserName` and `myusername` as different users.

The `login-handler.xml` file contains two sets of `<CaseSensitiveUserName>` tags: one for AD and one for LDAP. Make sure you also 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).

---

**Caution** – Different LDAP implementations may be using different keynames for CN. The appropriate keyname should be named 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>PreferredUser\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</Logi
nHandlerClass>
<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</LDA
PEnv>
-->
<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.

---

**Caution** – 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 menu.
- d. To start the management server, right-click **AppStorManager** and select **Start** from the menu.

On UNIX systems:

- 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 AD or LDAP” on page 434.

For example, the user name would be the following:

- AD — domain\PrimaryUser
- LDAP — PrimaryUser

where `PrimaryUser` is the name of the user account in LDAP or is the designated primary user in AD.

The password would be the following: `[NTdomainpassword]`.

## Step 3 — Add Users to the Management Server

Once the management server is configured for Active Directory/LDAP, the users can be added to the management server. This is required to prevent accidental access to the management server from other AD/LDAP users. Until the user is authenticated against AD/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 AD/LDAP, the user is tagged as an external user and the user’s password must be managed through AD/LDAP.

To add a user to the management server:

1. Log onto the management server by using the designated Admin account specified in “Step 1 — Configure the Management Server to Use AD or LDAP” on page 434.
2. Create the users as described in “Adding Users” on page 416 observing the following rules:
  - AD: 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 AD/LDAP.
  - It is not necessary to create a password, since the passwords used for login are those already configured on either the AD or LDAP server.

## Step 4 — Provide Login Information to Your Users

Notify your users that they are now able to log into the management server, and provide them with the user name and password you have specified in Active Directory/LDAP



---

**Caution** – Remind your users not to give the password they use to access the management server to anyone. Since user credentials are now stored in AD/LDAP, the password used to access the management server may also be used to access other accounts. In some instances, it may even be their network user name and password.

---



## Troubleshooting

---

This chapter contains the following topics:

- “Troubleshooting Installation/Upgrade” on page 447
- “Configuring the Java Console” on page 452
- ““Data is late or an error occurred” Message” on page 453
- “appstorm.<timestamp>.log Filled with Connection Exceptions” on page 453
- “Receiving HTTP ERROR: 503 When Accessing the Management Server” on page 454
- “Permanently Changing the Port a CIM Extension Uses (UNIX Only)” on page 456
- “Configuring UNIX CIM Extensions to Run Behind Firewalls” on page 458
- “Volume Names from Ambiguous Automounts Are Not Displayed” on page 461
- “Solaris Management Server Suddenly Restarts” on page 462
- “Installing the Software Security Certificate” on page 462
- “Troubleshooting Discovery and Get Details” on page 465
- “Troubleshooting Topology Issues” on page 477
- “Troubleshooting Provisioning” on page 492
- “Troubleshooting Hardware” on page 493

---

## Troubleshooting Installation/Upgrade

This section provides help with troubleshooting installations and upgrades.

- “If Your Installation or Upgrade Failed, Capture the Logs” on page 448
- “Checking Installation Log Files” on page 449
- ““The environment variable ‘perl5lib’ is set.” Message” on page 449
- ““SEVERE: OUI-10029...” Message” on page 450
- “Brocade API Switches Displaying Stale Data” on page 450
- “Troubleshooting the Oracle Database (Windows)” on page 450

# If Your Installation or Upgrade Failed, Capture the Logs

(Windows management servers only) You can quickly gather system information and log files for troubleshooting by running the `srmCapture.cmd` program in `<installation directory>/tools`.

---

**Caution** – The `srmCapture.cmd` program requires that `zip.exe` is in the same folder as `srmCapture.cmd`. If you are missing `zip.exe`, you can find it in the `tools` directory of the management server CD.

---

The following information is gathered by `srmCapture.cmd`:

- List of environment variables, look for file `srmListEnvVar.txt`.
- Results from running `ipconfig /all`, look for file `srmListIpconfigAll.txt`.
- Results from running `netstat -noab`, look for file `srmListNetstatNoab.txt`.
- Results from running `netstat -rte`, look for file `srmListNetstatRte.txt`.
- Results from running `netsh diag show test`, look for file `srmListNetshDiagShowTest.txt`.
- Install wizard log files (all files are found in `%systemdrive%\srmInstallLogs`).
- `srmwiz.ini`.
- Oracle export log file.
- File SRM log files.
- File SRM configuration files.
- Oracle log files
- Zero G registry content

If you see a message resembling the following, “Current location, `d:\Tools`, is not writable,” the current working subdirectory is not writable. The `srmCapture.cmd` program will go through the following directories in order until it finds one that is writeable:

1. `%temp%`
2. `%tmp%`
3. `%systemdrive%`

## Checking Installation Log Files

The following log files are generated by the installer and can be found on the management server in the following directories:

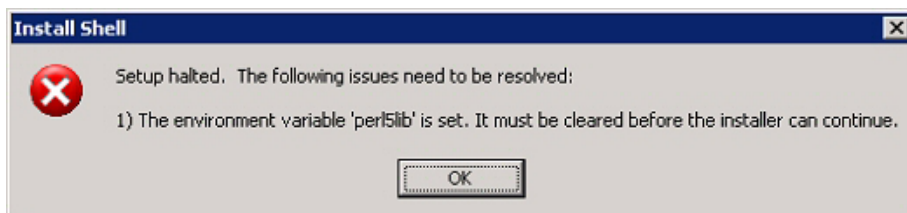
- **C:\srmlInstallLogs** includes these log files:
  - **srmlInstall.log** — This is the master log file of the installation wizard session. It provides information for troubleshooting installation of the management server and related components.
  - **srmlInstallOracle10g.log** — Log file that provides information about the Oracle 10g database installation.
  - **srmlInstallSrm.log** — Log file that provides information about the management server installation.
  - **srmOracle<monthyear>Patch.log** — Log file that provides information about the installation of the specified Oracle patch.

Where <monthyear> is the date of release of the specified Oracle patch.

See the Troubleshooting chapter in the installation guide for more information about installations and upgrades.

## “The environment variable ‘perl5lib’ is set.” Message

(Windows only) If the perl5lib environment variable is set, the installation/upgrade fails with the following message:



**FIGURE 22-1** Perl5lib environment variable message

This variable may have been set by another application. The environment variable may have also been set if your upgrade of Oracle was suddenly stopped, for example, as a result of a power outage. You must remove the perl5lib environment

variable before you can run the installation/upgrade again. For information about removing environment variables, refer to the documentation for the Windows operating system.

## “SEVERE: OUI-10029...” Message

The installation wizard lets you specify an installation location for Oracle 10g. If you specify a location that is being used by another program or if you specify the Oracle DVD drive, Oracle displays the following message:

```
SEVERE: OUI-10029: You have specified a non-empty directory to install
this product. It is recommended to specify either an empty or a non-
existent directory. You may, however, choose to ignore this message
if the directory contains Operating System generated files or
subdirectories like lost+found
```

If you see this message, contact customer support. Engineering has found this message to indicate the installation of your Oracle database may have failed.

## Brocade API Switches Displaying Stale Data

All Brocade API switches are placed in quarantine after you upgrade to Build 6.0. This means previous data is preserved but you can no longer update the data using Get Details. Therefore, data such as topology, zoning information will be stale until you migrate to Brocade SMI-A. See “Discovering Brocade Switches” on page 133.

## Troubleshooting the Oracle Database (Windows)

This section provides Oracle troubleshooting help:

- “Use Only the Installation Wizard (or Unix Scripts) to Install/Upgrade Oracle” on page 450
- “Existing Oracle Database Is Detected” on page 452

### Use Only the Installation Wizard (or Unix Scripts) to Install/Upgrade Oracle

With this release of the product, the Oracle database is automatically installed using the new Installation Wizard (or Unix scripts) developed to install the management server along with the Oracle database used by the management server. Installing Oracle separately is no longer recommended.

---

**Caution** – Do not install the Oracle database separately, the management server Installation Wizard (or Unix scripts) automatically configures the Oracle database for use with the management server. If you install the Oracle database separately, the database will not meet the configuration settings required by the management server.

---

## Cancelling an Installation or Upgrade Before Completion

If you cancel the installation of the management server after the Oracle database is installed, you must use the Oracle scripts to remove the Windows Registry entries and other Oracle changes and files that were partially installed or future installations of the management server will fail. See “Uninstalling Oracle Using the Oracle Scripts” on page 451.

## Uninstalling Oracle Using the Oracle Scripts

With this release of the management server, the Oracle database is automatically installed by the Windows installation wizard installer and the Linux and Solaris installation scripts along with various Oracle files and some Windows Registry changes. If you cancel the installation, you must use the Oracle removal scripts included on the CD-ROM set for the management server to completely remove all of the Oracle files. If the Linux and Solaris installation scripts or the Windows installer wizard detects any Oracle files during a re-installation, the installation will fail. If you need to uninstall Oracle for any reason, you must follow these steps:

### Windows:

1. Put the Oracle DVD in the DVD drive of the management server for Windows.
2. Locate the following scripts on the DVD:
  - `removeOracle9i.vbs`
  - `removeOracle10g.vbs`
3. Open a Command window and enter a script name as follows:

```
cscript d:\removeOracle10g.vbs
removeOracle10g.vbs
```

The script runs in the command window and removes the Oracle files from the server.

### Linux:

1. Put the Oracle DVD in the DVD drive of the management server for Linux.

2. Log on to the management server as root.
3. Run either of the scripts by entering the following at the command line:

```
<ORACLEDVD>/uninstallOracle9i.sh
```

```
<ORACLEDVD>/UninstallDatabase.sh
```

The remaining Oracle files are uninstalled from the management server for Linux.

### **Solaris:**

1. Put the Oracle DVD in the DVD drive of the management server for Solaris.
2. Log on to the management server as root.
3. Run either of the scripts by entering the following at the command line:

```
<ORACLEDVD>/uninstallOracle9i.sh
```

```
<ORACLEDVD>/uninstallOracle10g.sh
```

The remaining Oracle files are uninstalled from the management server for Solaris.

## Re-installing the Management Server

See “Cancelling an Installation or Upgrade Before Completion” on page 451.

## Existing Oracle Database Is Detected

If the Windows installation wizard installer (or the Unix installation scripts) detects an existing Oracle database, the following message is displayed: Existing Oracle Database is Detected. See “Uninstalling Oracle Using the Oracle Scripts” on page 451.

---

# Configuring the Java Console

It is recommended you configure your Java Console as follows for optimal performance. Please refer to the documentation for your Java Console for more information on how to make these changes.

To increase:

- The Memory, add -Xmx128m to the Java console
- The heap size, add -Xms128m to the Java console



---

## “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.

---

## appstorm.<timestamp>.log Filled with Connection Exceptions

When an Oracle redo log becomes corrupt, the management server is unable to connect to the database. Whenever this occurs, the management server writes to the `appstorm.<timestamp>.log` file.

To correct this problem, stop the management server and Oracle, and 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_appstorm.<timestamp>.log` file, which can be found in one of the following locations:
  - **Windows:** `\oracle\admin\APPIQ\bdump`.
  - **Unix systems:** `$ORACLE_BASE/admin/APPIQ/bdump`

You can verify if the redo log listed in the `alert_appstorm.<timestamp>.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;
```

The following sections describe how to start the database for the management server.

## Windows

In the Services window, make sure the OracleOraHome92TNSListener service has started and is set to automatic. See 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.

## Unix systems

To verify the Oracle service has started, enter the following at the command prompt:

```
ps -ef | grep ora
```

If the service has started, 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 ?	

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
```

---

**Caution** – 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. To save space, the text has been shortened:

```
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
```

---

**Caution** – 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 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.

---

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 box in the Add Address for Discovery page (**Discovery > Setup > Add Address**), enter 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 add it again. 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 456.
- 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 22-1** Troubleshooting Firewalls

<b>Configur- ation</b>	<b>Manual Start Parameters for CIM Extension</b>	<b>If Mentioned in cim.extension.parameters</b>	<b>Step 1 Discovery and RMI Registry Port</b>
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.	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
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 192.168.250.10:9012 Communication Port: 1234, 5678, 9012

**TABLE 22-1** Troubleshooting Firewalls (*Continued*)

<b>Configur- ation</b>	<b>Manual Start Parameters for CIM Extension</b>	<b>If Mentioned in cim.extension.parameters</b>	<b>Step 1 Discovery and RMI Registry Port</b>
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
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	172.16.10.10:1234OR 172.16.20.20:5678OR 172.16.30.30:9012 Communication Port: 1234, 5678, 9012



**TABLE 22-1** 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, cimom.Dcxws.agency.firstwai t=200000 cimom.Dcxws.agency.timeou t=200000	Any IP that is reachable Communication Port: 4673
No DNS, never resolve.		jboss.properties cimom.Dcxws.agency.firstwai t=200000 cimom.Dcxws.agency.timeou t=200000	Any IP that is reachable Communication Port: 4673
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 -on 10.250.250.10:1234 -on 172.31.250.10:5678 -on 192.168.250.10:9012 -credentials abcuser:passwd	-on 10.250.250.10:1234 -on 172.31.250.10:5678 -on 192.168.250.10:9012 -credentials abcuser:passwd	10.250.250.10:1234 OR 172.31.250.10:5678 OR 192.168.250.10:9012. 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 or 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-separated 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-separated 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.

---

**Caution** – 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.

---

This section contains the following topics:

- “Installing the Certificate by Using Microsoft Internet Explorer 6.0” on page 462
- “Changing the Security Certificate to Match the Name of the Server” on page 463

## Installing the Certificate by Using Microsoft Internet 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**.
3. When you are told there is a problem with the site's security certificate, click **View Certificate**.
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**.

# 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 program to delete the original certificate, and then use the generateAppiqKeystore program to create a new certificate and to copy the new certificate to the management server.

## Windows

To change the certificate on Windows:

1. Go to the %MGR\_DIST%\Tools directory.
2. To delete the original certificate, enter the following at the command prompt:  

```
%MGR_DIST%\Tools> generateAppiqKeystore.bat del
```

The original certificate is deleted.
3. To create a new certificate containing the DNS name of the management server, enter the following at the command prompt:  

```
%MGR_DIST%\Tools> generateAppiqKeystore.bat
```
4. If the program is unable to detect a DNS name, enter the following at the command prompt:  

```
%MGR_DIST%\Tools> generateAppiqKeystore.bat mycomputername
```

where mycomputername is the DNS name of the computer
5. To copy the new certificate to the management server, enter the following at the command prompt:  

```
%MGR_DIST%\Tools> generateAppiqKeystore.bat copy
```

The new certificate is copied to the correct location.

## Sun Solaris and Linux

To change the certificate on Sun Solaris and Linux:

1. Go to the [Install\_Dir] directory and run the following command:

```
eval `./usersvars.sh`
```

---

**Caution** – The quotes in the example must be entered as left single quotes as shown.

---

2. Go to the following directory:

```
[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 Discovery and Get Details

This section contains the following topics:

- "Troubleshooting Mode" on page 466
- "Unable to discover Emulex host bus adapters" on page 467
- "CIMOM Service Not Starting After Trying to Discover Sybase or SQL Server Applications" on page 467
- "Configuring E-mail Notification for Get Details" on page 468
- "Increasing the Time-out Period and Number of Retries for Switches in Progress" on page 469
- "'Connection to the Database Server Failed" Error" on page 470
- "Using the Test Button to Troubleshoot Discovery" on page 471
- "DCOM Unable to Communicate with Computer" on page 473
- "Duplicate Listings/Logs for Brocade Switches in Same Fabric" on page 473
- "Element Logs Authentication Errors During Discovery" on page 475
- "EMC Device Masking Database Does Not Appear in Topology (AIX Only)" on page 475
- "Management Server Does Not Discover Another Management Server's Database" on page 475
- "Microsoft Exchange Drive Shown as a Local Drive" on page 475
- "Unable to Discover Microsoft Exchange Servers" on page 476
- "Nonexistent Oracle Instance Is Displayed" on page 476
- "Requirements for Discovering Oracle" on page 476
- "Do Not Run Overlapping Discovery Schedules" on page 476
- "'This storage system uses unsupported firmware. ManagementClassName: class\_name" Message" on page 477
- "Troubleshooting Topology Issues" on page 477
- "Incorrect Topology Sometimes Displayed for CNT Switches" on page 482
- "Unable to Find Elements on the Network" on page 483
- "Device Locking Mechanism for Brocade Element Manager Query/Reconfiguration" on page 483
- "A Discovered Sun StorEdge A5000 JBOD Does Not Display Its WWN Properly" on page 483
- "Unable to Monitor McDATA Switches" on page 484
- "Unable to Detect a Host Bus Adapter" on page 485
- "Navigation Tab Displays Removed Drives as Disk Drives" on page 485
- "Unable to Obtain Information from a CLARiiON Storage System" on page 485
- "Discovery Fails Too Slowly for a Nonexistent IP Address" on page 486
- "'CIM\_ERR\_FAILED" Message" on page 487
- "CIM\_ERR\_FAILED When Trying to Activate a Zone Set Using McDATA SWAPI" on page 489
- "Communicating with HiCommand Device Manager Over SSL" on page 489

- “Unable to Discover a UNIX Host Because of DNS or Routing Issues” on page 490
- “ERROR replicating APPIQ\_EVAStorageVolume during Get Details for an EVA array” on page 491

## 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.

When Troubleshooting Mode is enabled during Get Details, the following additional information is provided to assist in the identification of configuration issues:

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

## Unable to discover Emulex host bus adapters

The Emulex driver does not contain the required library that is required by the management server. You must install Emulex HBAnywhere software so that the management server can discover hosts configured with HBAnywhere and hbatest can detect the Emulex host bus adapter.

## CIMOM Service Not Starting After Trying to Discover Sybase or SQL Server Applications

If your management server is running on Linux, you will not be able to discover Sybase or SQL Server applications. If you already added a Sybase or SQL Server entry to be managed in the Discovery setup page and performed a Get All Element Details operation, entries for the Sybase or SQL server will be added to the oracle listener configuration file. On the next system reboot, or on the next restart of the Oracle service, the Oracle listener will error out, and the CIMOM service will not start.

To correct the issue:

1. Edit `ORA_HOME/network/admin/listener.ora` and remove the `SID_DESC` text blocks containing the `PROGRAM=hsodbc` string.

where `ORA_HOME` is the Oracle home

For example: `. /opt/oracle/product/9.2.0.4`

If you have a `SID_DESC` block similar to the text block below, remove this entire block.

```
(SID_DESC =
(SID_NAME = SQLSERVERSID)
(ORACLE_HOME = /opt/oracle/product/9.2.0.4)
(PROGRAM = hsodbc)
```

2. Restart Oracle with the following command:

```
/etc/init.d/dbora restart
```

3. Restart the appstormanager service.

4. After the service has started, delete any Sybase or SQL entries from the Application tab in the discovery setup page. This is necessary to prevent them from being re-added to the `listener.ora` on further discoveries.

## 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. See the User Guide for more information.

2. Add or edit the e-mail address for the Admin account.

The status reports for Get Details are sent as follows:

- `gaedemail` property is empty - The e-mail is sent to users whose roles have System Configuration selected.
- `gaedemail` property is populated - The e-mail is sent only to users whose e-mail is assigned to the `gaedemail` property.

3. If you want additional users to receive the status reports for Get Details, do the following:

- a. Select **Configuration > Product Health**, and then click **Advanced** in the **Disk Space** tree.

- b. Click **Show Default Properties** at the bottom of the page.

- c. Copy the `gaedemail` property.

- d. Return to the Advanced page.

- e. Paste the copied text into the Custom Properties box.

- f. Assign the e-mail accounts you want to receive the report to the `gaedemail` property. For example, if you want `user1@mycompany.com` and `user2@mycompany.com` to receive these status reports, modify the `gaedemail` property in the Custom Properties box as follows:

```
gaedemail=user1@mycompany.com;user2@mycompany.com
```

---

**Note** – Make sure the hash (#) symbol is removed from the `gaedmail` property.

---

- g. When you are done, click **Save**.

## 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 switch 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. If it does not receive a response from the switch a second time, the management server says it cannot contact the switch.

To change the time-out period and number of retries for switches, modify the properties as described in the following steps:

1. Access the management server.
2. Select **Configuration > Product Health**, and 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 22-2, "Time-out Properties," on page 469.
5. Return to the Advanced page.
6. Paste the copied text into the Custom Properties box.
7. 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 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 22-2** Time-out Properties

Switch	Property
McDATA/Connectrix discovered through SNMP	<code>cimom.McData.Snmp.Timeout</code>
Cisco	<code>cimom.Cisco.Snmp.Timeout</code>
Other switches discovered through SNMP: • Sun StorEdge • QLogic	<code>cimom.snmp.switch.timeout</code>

9. To modify the number of retries, repeat steps 4 through 6 by copying and pasting the property specified in the table below. 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 22-3** Retry Properties

Switch	Property
McDATA/Connectrix discovered through SNMP	<code>cimom.McData.Snmp.Retries</code>
Cisco	<code>cimom.Cisco.Snmp.Retries</code>
Other switches discovered through SNMP: <ul style="list-style-type: none"> <li>• Sun StorEdge</li> <li>• QLogic</li> </ul>	<code>cimom.snmp.switch.retries</code>

10. When you are done, click **Save**.

## “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 these items, 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, and 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 Win32 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
HDLN 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/Logs for Brocade Switches in Same Fabric

### Duplicate listings: Targets tab

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
```

### Duplicate Logs

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
```

## Duplicate entries for the same element on the Get Details page

If an element is discovered through two different protocols, it may be listed twice on the Get Details page.

If you want to change the protocol used to discover an element that has already been discovered, delete the element before attempting to rediscover it. See “Deleting Elements from the Product” on page 194.

For some elements, duplicate entries may result if a second protocol is available. For example, you could choose to discover an element through a supported API, but if the element supports SMI-S, and the SMI-S provider is also available, the element could be discovered again. In this example, you could fix the issue by disabling the SMI-S provider.

## 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.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. See 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, see 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 the 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 rescheduled 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 `appstorm.<timestamp>.log` file in the following directory:

```
[Install_Dir]\jbossandjetty\server\appiq\logs
```

## "This storage system uses unsupported firmware. ManagementClassName: class\_name" Message

The following message is displayed when an LSI storage system is discovered, and is running unsupported firmware:

```
This storage system uses unsupported firmware. ManagementClassName:
class_name
```

Where `class_name` is the management class name for the unsupported array.

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

This section contains the following topics:

- “About the Topology” on page 478
- “Undiscovered Hosts Display as Storage Systems” on page 481
- “Solaris Machines Appear to Have Extra QLogic HBAs” on page 482
- “No Stitching for Brocade Switches with Firmware 3.2.0” on page 482
- “Link Between a Brocade Switch and a Host Disappears from the Topology” on page 482
- “Incorrect Topology Sometimes Displayed for CNT Switches” on page 482
- “Unable to Find Elements on the Network” on page 483
- “Device Locking Mechanism for Brocade Element Manager Query/Reconfiguration” on page 483
- “A Discovered Sun StorEdge A5000 JBOD Does Not Display Its WWN Properly” on page 483
- “Sun 6920 Storage Systems: “ReplicatorSQLException: Database create error” During Get Details” on page 484
- “Mirrored Volumes Cannot Be Provisioned on Sun 6920 Storage Systems” on page 484
- “Unable to Monitor McDATA Switches” on page 484
- “Unable to Detect a Host Bus Adapter” on page 485
- “Navigation Tab Displays Removed Drives as Disk Drives” on page 485
- “Unable to Obtain Information from a CLARiiON Storage System” on page 485
- “Discovery Fails Too Slowly for a Nonexistent IP Address” on page 486
- ““CIM\_ERR\_FAILED” Message” on page 487
- “Communicating with HiCommand Device Manager Over SSL” on page 489
- “Unable to Discover a UNIX Host Because of DNS or Routing Issues” on page 490

### About the Topology


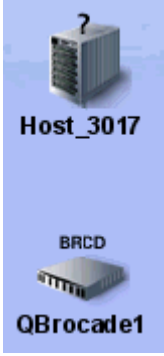
The software determines the topology by looking at the following:

- **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. LSI 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 22-4, “Troubleshooting Discovery and Get Details,” on page 479 provides details about how to correct problems that might occur during discovery and data collection.

**TABLE 22-4** Troubleshooting Discovery and Get Details

Scenario	Description	What to do
 <p>The host appears discovered and it is connected to the switch.</p>	<p>The software is aware of the host, but it cannot obtain additional information about it.</p>	<p>Verify that a CIM extension is installed on the host.</p> <p>Try discovering the element again, and then run Get Details.</p>
 <p>Host appears discovered and it is not connected to the switch.</p>	<p>The switch was previously made aware of the host, but it can no longer contact it.</p> <p>If the steps provided do not work, see “Link Between a Brocade Switch and a Host Disappears from the Topology” on page 482.</p>	<p>Verify that the host is on and the network cables are connected to it.</p> <p>Try discovering the element again, and then run Get Details.</p>

**TABLE 22-4** Troubleshooting Discovery and Get Details (*Continued*)

Scenario	Description	What to do
 <p>The host appears managed, but it is not connected to the switch.</p>	<p>There is a problem with Get Details from the host.</p> <p>If the steps provided do not work, see “Link Between a Brocade Switch and a Host Disappears from the Topology” on page 482.</p>	<p>Try getting the topology again:</p> <ol style="list-style-type: none"> <li>1. Click the <b>Discovery</b> menu, and then click the <b>Topology</b> tab.</li> <li>2. Verify the element is selected and click <b>Get Topology</b>.</li> </ol>
 <p>The element appears discovered, but a connected switch does not appear.</p>	<p>The switch has not been discovered.</p>	<p>Try discovering the switch again.</p> <ol style="list-style-type: none"> <li>1. Click the <b>Discovery</b> menu.</li> <li>2. Click the <b>Setup</b> tab and the <b>Add Address</b> button on the IP Addresses tab.</li> <li>3. Enter the IP address or DNS Name of the switch, and then enter its user name and password. Click <b>OK</b>.</li> <li>4. Verify the element is selected.</li> <li>5. Click <b>Start Discovery</b>.</li> <li>6. After discovery has completed, click the <b>Topology</b> tab.</li> <li>7. Verify the element is selected and click <b>Get Topology</b>.</li> </ol>
<p>When discovering a Windows-based host, the correct IP address is entered, but the host does not appear in the topology.</p> <p>The following can be seen on the host:</p> <ul style="list-style-type: none"> <li>• In Windows Event Manager the WinMgmt.exe process is not running. This process starts WMI.*</li> <li>• In the Windows Event Log, DCOM error messages are shown.</li> </ul>	<p>An invalid user account was entered</p>	<p>Enter a valid user account that has administrative privileges so it can start WMI.</p>

\*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 the management server.

---

**Caution** – 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 200 for more information.

---

## Undiscovered Hosts Display as Storage Systems

On rare occasions, the management server displays undiscovered hosts as storage systems in System Explorer. To resolve this issue, provide the host’s world wide name (WWN) as described in the following steps:

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. Select **Configuration > Product Health**, and then click **Advanced** in the **Disk Space** tree.
3. Click **Show Default Properties** at the bottom of the page.
4. Copy the following property:  
`#hostPortWWNs=`
5. Return to the Advanced page.
6. Paste the copied text into the Custom Properties box.
7. Uncomment the `hostPortWWNs` property by removing the hash mark (#) in front of `hostPortWWNs`.
8. Enter the host’s WWN in hexadecimal format. Multiple WWNs can be entered as a comma-separated list. For example:  
`hostPortWWNs=00-01-C9,00-01-C8`
9. Click **Save**.

## 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.
- 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.

## Sun 6920 Storage Systems: “ReplicatorSQLException: Database create error” During Get Details

While performing a Get Details, the Sun 6920 provider will return the error “ReplicatorSQLException: Database create error” under certain circumstances. This error appears in the management server logs but can be safely ignored. Sun Microsystems is aware of this issue.

## Mirrored Volumes Cannot Be Provisioned on Sun 6920 Storage Systems

Mirrored volumes are not represented properly by the management server. You cannot use the management server to provision mirrored volumes on Sun 6920 storage system.

## 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 “Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries” on page 119.



---

**Caution** – 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, if 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. See 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 because the service processor is 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 IOs per second.

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 or three minutes and 45 seconds on Unix systems. 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 the `cimom.CimXmlClientHttpConnectTimeout` property to more than 20 seconds on Windows or three minutes and 45 seconds on Unix systems, 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. Select **Configuration > Product Health**, and 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.
5. Return to the Advanced page.
6. Paste the copied text into the Custom Properties box.
7. Make your changes in the Custom Properties box. 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 milliseconds 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**.

## “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 tries 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 Get Details operation the management server performs 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. Select **Configuration > Product Health**, and 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`.
4. Return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Make your changes in the Custom Properties box by changing the value of `cimom.mcData.swapIThrottle`. For example, the default is 200 ms. To change the value to 800 ms, 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. Verify if you can re-establish communication with EFCM by following the steps in “Re-establishing Communication with EFCM” on page 488. 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 to EFCM fails, there is a network problem that must be resolved. Once network connectivity is restored, click 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 indicate that it still cannot communicate with EFCM, wait approximately three minutes for the lost SWAPI connection to time out, and then click the **Test** button again. If this 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. Note that 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, see the support matrix to determine if the EFCM and switch versions are all supported. Contact technical support for further information.

## 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.

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, run Get Details for this element to update the zoning information. See “Get Details” on page 188 for more 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 that you want to communicate through a secure connection (SSL) and another that 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 following steps. 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. Select **Configuration > Product Health**, and 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.
4. Return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Make your changes in the Custom Properties box. 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.

## 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 to 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**, and then click **Advanced** in the **Disk Space** tree.

2. Paste the following text into the Custom Properties box.

```
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 200,000 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 starts to question whether its partner is still alive. If one entity (management server or extension) does not receive a message from the other during the interval set by the `timeout` property, it sends an "are you there" message. If that message is not acknowledged during the interval set by the `timeout` property, the entity concludes that the connection is no longer functioning. The CIM extension stops attempting to make a connection. When this occurs on the side of the management server, the management server attempts to re-connect (and continues the attempt until the host becomes available). The default value is 1,000 ms. You are modifying it to wait 200,000 ms or 3.33 minutes.

3. Click **Save**.

## ERROR replicating APPIQ\_EVAStorageVolume during Get Details for an EVA array

Errors similar to `ERROR replicating APPIQ_EVAStorageVolume` might occur when an EVA-specific data cache is updated during a Get Details operation. For example, when Data Protector creates a snapshot, a new virtual disk is automatically created on the EVA array, and the EVA database used by the management server is updated to reflect this change.

If the EVA database is changed during a Get Details operation, small replication errors may be seen as a result. The array information will be updated with the correct information next time Get Details runs.

## Recalculating the Topology

When Recalculating the topology or running Get Details, other tasks using the management server can be delayed because the management server must recalculate the topology, which is a resource intensive operation. Recalculation occurs after a Get Details when provisioning is done, and when you choose to recalculate the topology manually.

During the recalculation period, you may not be able to log into the application. If you are already logged into the application, navigation may not be possible until the topology recalculation is complete.

## 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 contains the following topics:

- “Cannot Access a Resource Owned by Another Controller” on page 492
- “Error -56” on page 493
- ““Can't delete this zone” Message” on page 493
- “Changes in EFC Manager Requiring Get Details” on page 493

### Cannot Access a Resource Owned by Another Controller

If you receive a message about not being able to access a resource owned by another controller, it is because you tried to access a controller that has not been discovered. You should discover all controllers on the LSI storage system.



For example, assume you discovered only one of the controllers on an LSI 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 “Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries” on page 119 for more information on how to discover a controller.

## Error -56

If you see `error -56`, the switch has network connection failures or problems. To solve the problem, make sure the switch is physically connected to the network, and 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 see the following message when you try to delete a zone, move the zone to an inactive zone set, and 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 contains the following topics:

- “About Swapping Host Bus Adapters” on page 494
- ““Fork Function Failed” Message on AIX Hosts” on page 494
- “Known Driver Issues” on page 494
- “Known Device Issues” on page 494
- ““mailbox command 17 failure status FFF7” Message” on page 498
- ““Process Has an Exclusive Lock” Message” on page 498

## 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 are 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 Table 22-5, “Known Device Issues,” on page 495 provides a description of the known device issues. You can find the latest information about device issues in the release notes.

**TABLE 22-5** Known Device Issues

Device	Software	Description
AIX host	NA	<p>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 occurs, you see a message containing the following when you start the CIM extension:</p> <pre>CXWS 3.1.0.144 on 0.0.0.0/0.0.0.0 now accepting connections</pre> <p>To fix this situation, add the following line to the /opt/APPQcime/tools/start file on the AIX host:</p> <pre>export NSORDER=local,bind</pre>
AIX host using an IBM Storage System	NA	<p>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.</p>
Hosts running SGI IRIX version 6.5.22 or 6.5.24	NA	<p>If a host is 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.</p>

**TABLE 22-5** Known Device Issues (*Continued*)

Device	Software	Description
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/output into the metadata server into <code>/folder</code> , 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 <code>/folder</code> on the metadata client.
Solaris host	Sun SAN Foundation Suite driver (Leadville driver)	The bindings page reports a SCSI number that comes from the HBA API. 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 reports 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."
Solaris host	HDLM	If you do a Get Details for the host by itself, on the bindings page, the controller number begins with c-1, for example, <code>c-1t0d58</code> . Perform Get Details on the host with storage and switches. The controller numbers are displayed correctly.

**TABLE 22-5** Known Device Issues (*Continued*)

Device	Software	Description
Solaris host	VxVM	<p>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.</p> <p>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 fiber are shown as external.</p>
Windows host	VxVM	<p>When a Windows host with VxVM is used, the SCSI bus number is always reported to be 1 in the SCSI bus column of the Disk Drives page.</p>
Any host	NA	<p>The Unmounted Volume box 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, or if your license does not allow you to discover a particular storage system. See the support matrix to determine which storage systems you can discover. The List of Features is accessible from the Documentation Center (<b>Help &gt; Documentation Center</b>).</p>

**TABLE 22-5** Known Device Issues (*Continued*)

Device	Software	Description
IBM Storage Systems	Subsystem Device Driver (SDD) or MPIO (multipath I/O)	If you discover 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.

```
SYMAPI routine SymDevMaskSessionStart failed with error code 188: The operation failed because another process has an exclusive lock on the local Symmetrix.
```

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.

After the management server has detected the lock on the Symmetrix storage system, it tries to access the storage system for 15 minutes and then 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 before you remove the lock manually. Be sure that no other processes are occurring on the storage system. To learn how to remove the lock, see 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, 157

## A

about

- AIX CIM Extension, 215
- Altix CIM Extension, 227
- HP-UX CIM Extension, 249
- IRIX CIM Extension, 239
- management server, 2
- NonStop CIM Extension, 273
- OpenVMS CIM Extension, 287
- security, 409
- Solaris CIM Extension, 301, 313
- SUSE and Red Hat Linux CIM Extension, 262
- Windows CIM Extension, 327

accessing

- domain controller, 353

account

- password, 418

accounts

- users, 416

Active Directory, 476

adding

- domain controller, 353, 396
- elements, 426, 429
- IP address, 127
- IP range, 125
- new elements, 199
- organizations, 426
- roles, 424
- switches, 153

TNS Listener Port, 396

user accounts, 416

AIX, 476

AIX CIM Extension

- installing, 215
- prerequisites, 215
- removing, 215
- starting, 215
- stopping, 215

Altix CIM Extension

- installing, 227
- prerequisites, 227
- removing, 227
- starting, 227
- stopping, 227

API data

- Brocade switches, 450

APPIQ\_OWNER account, 353

APPIQ\_USER, 396

Application Administrator role, 409

applications

- discovering, 353

authentication errors

- SNMP, 475

## B

benefits, 2

Bridge Agent, 142

Brocade Rapid program, 186

Brocade switches, 186

- API data, 450

- discovering, 133

- stale data, 450
- building
  - topology, 186

## C

- certificate
  - installing, 34, 66
- changing
  - domain controller, 353, 396
  - e-mail address, 420
  - full name, 420
  - license, 117
  - login name, 420
  - number of retries, 156, 469
  - organizations, 429
  - password, 187, 396, 419, 420
  - phone number, 420
  - roles, 424
  - SNMP trap listener, 155
  - time-out period, 156, 469
  - TNS Listener Port, 396
  - user account, 418
  - user name, 187
  - user preferences, 421
  - user profile, 420
- child organizations, 409
- CIM, 2
- CIM Extension
  - installing, 249, 301, 313, 327
  - port, 457
  - Solaris, 249, 301, 313
  - Windows, 327
- CIM Extensions
  - about, 215, 227, 239, 249, 262, 273, 287, 301, 313, 327
  - AIX, 215
  - Altix, 227
  - HP-UX, 249
  - IRIX, 239
  - NonStop, 273
  - OpenVMS, 287
  - Solaris, 301, 313
  - SUSE and Red Hat Linux, 261
  - Windows, 327
- cimom.CimXmlClientHttpConnectTimeout, 486
- cimom.emc.skipRefresh, 160
- cimom.hds.exclude, 164

- cimom.symmetrix.exclude, 159
- CIO role, 409
- clearing
  - elements, 129
- CNT
  - switches, 138
- Command View EVA
  - SNMP traps, 169
- configuring
  - Java Console, 452
- controller
  - removing, 353
- cookies
  - JavaScript, 2
- creating
  - new password, 420
  - organizations, 426
  - roles, 424
  - topology, 119
  - user accounts, 416

## D

- data
  - outdated (Brocade switches), 450
- database
  - AIX, 476
  - management server, 49, 85
- database connection failed
  - error, 471
- DCOM
  - unable to communicate, 474
- deleting
  - domain controller, 353
  - elements, 129, 194
  - organizations, 430
  - roles, 425
  - switches, 153
  - TNS Listener Port, 396
  - user accounts, 420
  - zone sets, 493
  - zones, 493
- details
  - obtaining, 188
- detecting
  - IP range, 125
  - McDATA switches, 153
  - switches, 153

- device issues, 494
- devices
  - deleting, 194
- discovered address
  - modifying, 187
- discovered elements
  - deleting elements, 194
- discovering
  - applications, 353
  - Brocade switches, 133, 186
  - CNT switches, 138
  - DNS Name, 127
  - EMC Solutions Enabler, 158
  - HDS storage systems, 163
  - HDS systems, 164
  - HP XP storage systems, 168, 171
  - IBM storage systems, 174
  - IP address, 127
  - McDATA switches, 142
  - Microsoft Exchange, 353, 378, 476
  - NetApp filers, 183
  - new elements, 199
  - Oracle, 353, 355
  - Oracle clusters, 355
  - passwords, 122
  - SQL servers, 363
  - storage system, 119
  - storage systems, 161, 176
  - Sun StorEdge storage systems, 176, 178, 179
  - Sun StorEdge switches, 140
  - switches, 119, 133
  - Sybase, 353, 374
  - Symmetrix systems, 159
  - troubleshooting, 476, 477, 478, 483, 498
  - user names, 122
- discovering the host, 279
- discovery
  - authentication errors, 475
  - Emulex host bus adapters, 467
  - quarantine, 197
  - time-out, 486
  - troubleshooting, 471
  - Windows proxy, 342
- discovery groups, 187
- discovery requirements
  - Oracle, 477
- discovery settings
  - importing, 129

- saving, 131
- disk drive, 485
- displaying
  - deleted Oracle instances, 476
- DNS, 476
- Domain Administrator role, 409
- domain controller
  - access, 396
  - accessing, 353, 396
  - removing, 353
- domain controller access, 353, 396
- drivers
  - fixing, 494
- drives
  - Microsoft Exchange, 476
  - uninitialized, 485

## E

- editing
  - e-mail address, 420
  - full name, 420
  - login name, 420
  - organizations, 429, 430
  - password, 419, 420
  - phone number, 420
  - roles, 424
  - user account, 418
  - user preferences, 421
  - user profile, 420
- EFC Manager, 142, 493
- element details
  - obtaining, 188
- elements
  - adding, 426, 429
  - deleting, 129, 194
  - managing, 429
  - modifying, 187
  - organization, 429
  - removing, 430
  - topology, 186
  - unable to find, 478, 483
- e-mail address
  - changing, 420
- EMC CLARiiON, 161
- EMC Solutions Enabler, 158
- Emulex host bus adapters, 467

- error
  - database connection failed, 471
  - error -56, 493
- Error 503, 454
- error message
  - exclusive lock, 498
- errors
  - authentication, 475
- excluding
  - HDS systems, 164
  - switches, 151
  - Symmetrix systems, 159
- exclusive lock
  - error message, 498
- Extension
  - CIM, 249, 301, 313

## F

- features
  - key, 2
- filtering
  - organizations, 431
- finding
  - applications, 353
  - hosts, 353
  - IP address, 127
  - IP range, 125
  - new elements, 199
  - storage systems, 119
  - switches, 119
- fixing
  - drivers, 494
- full name
  - changing, 420

## G

- Get Details
  - email notification, 468
- getting
  - element details, 188
- getting details, 188
  - applications, 353
  - hosts, 353

## H

- HBAs

- swapping, 494
- HDS storage systems
  - discovering, 163
- HdsSkipRefresh, 166
- Help Desk role, 409
- hierarchy
  - organizations, 409
- host
  - not in topology, 478, 483
- host bus adapter
  - unable to detect, 485
- hosts
  - discovering, 353
  - removing, 129
- hot-swapped
  - drives, 485
- HP XP storage systems, 168, 171
- HP-UX CIM Extension
  - installing, 249
  - prerequisites, 249
  - removing, 249
  - starting, 249
  - stopping, 249
- HTTP Error 503, 454
- HTTPS, 34, 49, 66, 85

## I

- IBM storage systems
  - discovering, 174
- importing
  - discovery settings, 129
- inaccessible
  - device, 492
- increasing
  - Java heap size, 452
- information
  - obtaining element, 188
- installing
  - AIX CIM Extension, 215
  - Altix CIM Extension, 227
  - CIM Extension, 249, 301, 313, 327
  - HP-UX CIM Extension, 249
  - IRIX CIM Extension, 239
  - Java plug-in, 32, 64, 69, 110
  - management server, 49, 85
  - NonStop CIM Extension, 275

- OpenVMS CIM Extension, 289
- security certificate, 34, 49, 66, 85
- Solaris CIM Extension, 301, 313
- SUSE and Red Hat Linux CIM Extension, 264
- Windows CIM Extension, 327
- internal
  - drives, 485
- IP range, 125
- IRIX CIM Extension
  - installing, 239
  - prerequisites, 239
  - removing, 239
  - starting, 239
  - stopping, 239
- issues
  - devices, 494

## J

- Java, 2
- Java Console
  - increasing heap size
  - increasing
    - Java memory, 452
  - increasing memory, 452
- Java plug-in
  - installing, 32, 64, 69, 110

## K

- key benefits, 2
- key features, 2

## L

- license
  - modifying, 117
- local drives, 476
- locating
  - storage systems, 119
  - switches, 119
- log messages
  - viewing, 156
- login name
  - modifying, 420

## M

- management server
  - about, 2

- database, 49, 85
  - installing, 49, 85
  - porting across operating systems, 69, 79
  - security, 409
- managing
  - elements, 426, 429, 430
  - switches, 152
- McDATA switches, 484
  - adding, 153
  - discovering, 142
- messages
  - data is late, 453
- Microsoft Exchange
  - Adding domain controllers, 378
  - deleting domain controllers, 380
  - discovering, 353, 378, 476
  - drive M, 476
  - failover clusters, 380
- mixed mode authentication, 364
- modifying
  - discovered address, 187
  - discovery IP address, 128
  - DNS name for discovery, 128
  - domain controller, 353, 396
  - elements, 187
  - e-mail address, 420
  - full name, 420
  - license, 117
  - login name, 420
  - organizations, 429
  - password, 187, 396, 419, 420
  - phone number, 420
  - roles, 424
  - SNMP trap listener, 155
  - TNS Listener Port, 396
  - user account, 418
  - user name, 187
  - user preferences, 421
  - user profile, 420
- moving
  - management server, 69

## N

- naming organizations, 409
- NetApp filers
  - discovering, 183
- netcnfg, 158

- nethost, 158
- new elements
  - adding, 199
- new password, 420
- nonexistent IP addresses, 486
- nonexistent Oracle instances, 476
- NonStop CIM Extension
  - installing, 275
  - prerequisites, 274
  - removing, 284
  - starting, 277
  - stopping, 283
- number of retries
  - changing, 156, 469

## O

- obtaining
  - security certificate, 34, 66
  - topology information, 186
- OpenVMS CIM Extension
  - installing, 289
  - prerequisites, 288
  - removing, 299
  - starting, 291
  - stopping, 298
- Oracle
  - deleted instances, 476
  - discovering, 353, 355
  - discovery requirements, 477
- Oracle TNS Listener Port, 396
- organizations
  - about, 409
  - adding, 426
  - deleting, 430
  - editing, 429, 430
  - elements, 426, 429, 430
  - filtering, 431
  - properties, 423
  - users, 423
  - viewing, 428

## P

- parent organizations, 409
- password
  - changing, 187, 396, 418, 419, 420
- Performance Explorer
  - Java plug-in, 32, 64, 69

- phone number
  - editing, 420
- planning organizations, 409
- port
  - CIM Extension, 457
- porting
  - management server, 69
- prerequisites
  - AIX CIM Extension, 215
  - Altix CIM Extension, 227
  - HP-UX CIM Extension, 249
  - IRIX CIM Extension, 239
  - NonStop, 274
  - OpenVMS, 288
  - Solaris CIM Extension, 301, 313
  - SUSE and Red Hat Linux, 262
  - Windows CIM Extension, 327
- privileges
  - roles, 409
- problems
  - drivers, 494
- process
  - exclusive lock, 498
- profile
  - user, 420
- properties
  - organizations, 423
  - roles, 422
- provisioning
  - troubleshooting, 492, 493, 498

## Q

- quarantine
  - adding elements, 197
  - clearing elements, 197

## R

- Rapid program, 186
- Re, 79
- refreshing
  - Symmetrix systems, 160
- remote drives, 476
- removing
  - AIX CIM Extension, 215
  - Altix CIM Extension, 227
  - domain controller, 353

- elements, 129, 194, 429, 430
- HP-UX CIM Extension, 249
- IRIX CIM Extension, 239
- NonStop CIM Extension, 284
- OpenVMS CIM Extension, 299
- organizations, 430
- roles, 425
- Solaris CIM Extension, 301, 313
- SUSE and Red Hat Linux CIM Extension, 272
- switches, 153
- TNS Listener Port, 396
- user accounts, 420
- Windows CIM Extension, 327
- zone sets, 493
- zones, 493
- requirements, 2
  - software, 2
- restricting NonStop CIM Extension users, 279
- roles
  - about, 409
  - adding, 424
  - Application Administrator, 409
  - CIO, 409
  - deleting, 425
  - Domain Administrator, 409
  - editing, 424
  - Element Control privilege, 409
  - Full Control privilege, 409
  - Help Desk, 409
  - privileges, 409
  - properties, 422
  - Server Administrator, 409
  - Storage Administrator, 409
  - users, 422
  - View privilege, 409

## S

- saving
  - discovery settings, 131
  - settings to a file, 131
- scanning
  - IP range, 125
- security
  - Management server, 409
  - roles, 424
- security certificate
  - installing, 34, 49, 66, 85
- Server Administrator role, 409

- setting
  - discovery passwords, 122
  - discovery user name, 122
- silent installation
  - Windows, 331
- SNMP
  - authentication errors, 475
- SNMP trap listener
  - changing, 155
- software requirements, 2
- Solaris
  - porting management server, 69
- Solaris CIM Extension
  - installing, 301, 313
  - prerequisites, 301, 313
  - removing, 301, 313
  - starting, 301, 313
  - stopping, 301, 313
- SQL Server
  - authentication modes, 364
- SQL servers
  - discovering, 363
- starting
  - AIX CIM Extension, 215
  - Altix CIM Extension, 227
  - HP-UX CIM Extension, 249
  - NonStop CIM Extension, 277
  - OpenVMS CIM Extension, 291
  - Solaris CIM Extension, 301, 313
  - SUSE and Red Hat Linux CIM Extension, 267
  - Windows CIM Extension, 327
- stopping
  - AIX CIM Extension, 215
  - Altix CIM Extension, 227
  - HP-UX CIM Extension, 249
  - IRIX CIM Extension, 239
  - NonStop CIM Extension, 283
  - OpenVMS CIM Extension, 298
  - SAN details, 190
  - Solaris CIM Extension, 301, 313
  - SUSE and Red Hat Linux CIM Extension, 271
  - Windows CIM Extension, 327
- Storage Administrator role, 409
- storage systems, 176
  - discovering, 119, 176
  - removing, 129
- storage terms, 2

- Sun StorEdge
  - SNMP trap listener, 155
- Sun StorEdge storage systems, 176, 178, 179
- Sun StorEdge switches, 140
- SUSE and Red Hat Linux CIM Extension
  - installing, 264
  - prerequisites, 262
  - removing, 272
  - starting, 267
  - stopping, 271
- swapped
  - drives, 485
- swapping HBAs, 494
- switches
  - adding, 153
  - discovering, 119, 133
  - excluding, 151
  - managing, 152
  - McDATA, 142, 153, 484
  - number of retries, 156, 469
  - removing, 129, 153
  - time-out period, 156, 469
  - unable to monitor, 484
- Sybase
  - discovering, 353, 374
- System Explorer
  - can't access, 492
  - deleting elements, 194
  - Java plug-in, 32, 64, 69

**T**

- terms
  - storage, 2
- time-out period
  - changing, 156
- TNS Listener Port
  - changing, 396
- topology
  - AIX, 476
  - building, 186
  - host not appearing, 478, 483
- topology issues, 478
- troubleshooting
  - discovery, 471
  - discovery and getting element details, 471, 474, 476, 477, 478, 483, 498
  - Microsoft Exchange, 476

- provisioning, 492, 493, 498

## U

- unable to
  - discover, 471
- Unable to access resource, 492
- unable to detect
  - host bus adapter, 485
- unable to find
  - elements, 483
- unable to retrieve data, 494
- uninitialized
  - drives, 485
- uring, 452
- user accounts
  - creating, 416
  - deleting, 420
- user name
  - changing, 187
- user profile
  - modifying, 420
- users
  - about, 409
  - adding, 416
  - organizations, 423
  - roles, 422, 424

## V

- viewing
  - log messages, 156
  - organization properties, 423
  - organizations, 428
  - security certificate, 34, 66
  - topology, 119

## W

- Web browsers, 2
- WEBEM, 2
- Windows
  - porting management server, 69
  - silent installation, 331
- Windows CIM Extension
  - installing, 327
  - removing, 327
  - starting, 327
  - stopping, 327



- Windows proxy
  - discovery, 342
- WinMgmt.exe, 478

## **X**

- Xiotech storage systems, 179

## **Z**

- zone sets
  - deleting, 493
- zones
  - deleting, 493

