

EMC ControlCenter
5.2 Service Pack 4

PLANNING AND INSTALLATION GUIDE

VOLUME 1

P/N 300-002-648
REV A02

Note: This document has been updated to reflect the new ControlCenter features provided in Service Packs 1-4 since the original ControlCenter 5.2 release. Use this document to plan and install the base ControlCenter 5.2 software. Use the *EMC ControlCenter 5.2 Service Pack 4 Release Notes* for instructions to apply SP4 to a base 5.2 installation or a base 5.2 installation with previous Service Packs installed applied. The latest version of the *EMC ControlCenter 5.2 Service Pack 4 Release Notes* can be found on the EMC Powerlink website: <http://powerlink.emc.com>.

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748-9103
1-508-435-1000
www.emc.com

Copyright © 2002 - 2006 EMC Corporation. All rights reserved.

Published March 2006

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

Trademark Information

EMC², EMC, EMC ControlCenter, AlphaStor, ApplicationXtender, Catalog Solution, Celerra, CentraStar, CLARAlert, CLARiiON, ClientPak, Connectrix, Co-StandbyServer, Dantz, Direct Matrix Architecture, DiskXtender, Documentum, EmailXtender, EmailXtract, HighRoad, Legato, Legato NetWorker, Navisphere, OpenScale, PowerPath, RepliStor, ResourcePak, Retrospect, Smarts, SnapShotServer, SnapView /IP, SRDF, Symmetrix, TimeFinder, VisualSAN, VSAM Assist, Xtender, Xtender Solutions, and where information lives are registered trademarks and EMC Developers Program, EMC OnCourse, EMC Proven, EMC Snap, EMC Storage Administrator, Access Logix, ArchiveXtender, Authentic Problems, Automated Resource Manager, AutoStart, AutoSwap, AVALONidm, C-Clip, Celerra Replicator, Centra, CLARevent, Codebook Correlation Technology, Common Information Model, CopyCross, CopyPoint, DatabaseXtender, Direct Matrix, DiskXtender 2000, EDM, E-Lab, EmailXaminer, Enginuity, eRoom, FarPoint, FLARE, FullTime, Global File Virtualization, Graphic Visualization, InfoMover, Invista, MirrorView, NetWin, NetWorker, OnAlert, Powerlink, PowerSnap, Rainfinity, RecoverPoint, RepliCare, SafeLine, SAN Advisor, SAN Copy, SAN Manager, SDMS, SnapImage, SnapSure, SnapView, StorageScope, SupportMate, SymmAPI, SymmEnabler, Symmetrix DMX, UltraPoint, Viewlets, VisualSRM, and WebXtender are trademarks of EMC Corporation. All other trademarks used herein are the property of their respective owners.

Preface	xi
Document Your Storage Environment.....	1
Step 1 Document Your Storage Environment.....	2
Step 2 Determine the Installation Size	5
Plan the Infrastructure	7
Step 3 Know the ControlCenter Architecture.....	8
Step 4 Determine the Configuration Type.....	12
Step 5 Plan for ControlCenter Multihoming (Optional)	17
Step 6 Plan for Cluster Support (Optional)	24
Plan for Business Functions.....	29
Step 7 Plan for Open Integration Components (OIC)	30
Step 8 Plan for Licensed Features and Applications	32
Step 9 Plan for Console Interfaces	40
Step 10 Plan for PowerPath Volume Manager.....	45
Step 11 Plan for Console Views	46
Plan for Agents.....	49
Step 12 Perform General Agent Planning	50
Step 13 Plan for Master Agents.....	54
Step 14 Plan for Common Agents	57
Step 15 Plan for Backup Agents.....	61
Step 16 Plan for Common Mapping Agent.....	67
Step 17 Plan for Connectivity Agents	70
Step 18 Plan for Database Agent for Oracle.....	74
Step 19 Plan for Host Agents	76
Step 20 Plan for Storage Agents.....	80
Step 21 Plan for EMC Solutions Enabler	97

Plan for Security and Remote Access	99
Step 22 Plan for User Authentication	100
Step 23 Consider Services for Remote Access	105
Prepare to Install ControlCenter.....	109
Step 24 Prepare the Network and Hosts	110
Step 25 Create the eccadmin Account.....	114
Step 26 Install the Installation Tools on the Target Host.....	116
Step 27 Set Up Shared Folder Installation (Recommended)	120
Step 28 Create Native Installable Images for UNIX Master and Host Agents	125
Install and Start the Infrastructure.....	129
Step 29 Be Sure You are Ready to Install ControlCenter.....	130
Step 30 Install the Infrastructure	131
Step 31 Install the WebConsole Server (Optional)	145
Step 32 Configure SSL for Web Applications (Optional)	147
Step 33 Configure Agent Load Balancing (Optional).....	154
Step 34 Start Infrastructure Components.....	160
Implement Business Functions	163
Step 35 Install the ControlCenter Console	164
Step 36 Launch the ControlCenter Console and Log In.....	168
Step 37 License the Desired Applications	171
Step 38 Launch the Web Console and Log In (Optional).....	172
Step 39 Install the Integration Packages (Optional).....	175
Step 40 Install Performance Manager (Optional).....	177
Step 41 Install StorageScope (Optional)	182
Step 42 Install StorageScope API (Optional)	185
Step 43 Install the SupportTools (Optional).....	187
Step 44 Install the EACLI Client (Optional).....	189
Deploy Agents and Perform Initial Discovery	191
Step 45 Deploy and Start Master Agents	192
Step 46 Deploy Open Systems Agents.....	210
Step 47 Finish Setting Up Agents.....	223
Step 48 Enable Access to Symmetrix Arrays	224
Step 49 Allow Automatic Discovery to Complete	227
Step 50 Perform Assisted Discovery.....	228
Step 51 Discover connectivity devices.....	237
Step 52 Back Up ControlCenter (Optional).....	238

Set Up Cluster Support (Optional)	243
Step 53 Install the ControlCenter Infrastructure in a Clustered Environment	244
Step 54 Install ControlCenter Agents in an Application Clustered Environment	261
Step 55 Troubleshoot Problems with Clusters	266
Uninstall ControlCenter	271
Step 1 Removing Service Pack 4	272
Step 2 Uninstall Agents	274
Step 3 Uninstall ControlCenter Console(s)	276
Step 4 Uninstall Integration Packages	278
Step 5 Uninstall Other Components and Products	279
Step 6 Uninstall ControlCenter Cluster Support	284
Appendix A Installing FibreZoneBridge and FibreZone CLI	287
About FibreZoneBridge	288
Install the FibreZoneBridge Software	290
Uninstalling the FibreZoneBridge Software	291
Installing the FibreZone CLI Software	292
Uninstalling the FibreZone CLI Software	294
FibreZone CLI Support Matrix	295
Appendix B Port Usage and Firewall Configuration	297
Understanding ControlCenter NAT Firewall Support with Multihome	298
Configure Communications over a NAT Firewall with Multihome	299
Fibre Channel Connectivity Agent Port Usage	307
Controlling Port 162 Usage for SNMP	310
ControlCenter Infrastructure Port Usage	313
ControlCenter Console Port Usage	316
Agent-to-Infrastructure Communication Ports	318
Workload Analyzer Archiver Port Usage	323
StorageScope Port Usage	324

Appendix C Alternate Methods for Installing the Master Agent	325
Install the Master Agent with the Push Utility	326
Install the Master Agent with UNIX Package Tools	330
Appendix D AccessInfoChange Utility	335
Running the Utility	336
Update Template File	338
Output File	339
Appendix E ConnectEMC	341
Overview of ConnectEMC Process	342
Installation and Configuration	343
Index	347

1	Sample Data Center Diagram	2
2	Architecture for a Single-Host Infrastructure Configuration	9
3	Architecture for a Distributed Infrastructure Configuration	10
4	Example Single-Host Infrastructure Configuration (Proxy Mode)	11
5	Single-Host Infrastructure with Remote Console and Agents	13
6	Distributed Infrastructure with Separate Stores	14
7	Sample Single-Host Infrastructure Multihoming Configuration	21
8	Sample Distributed Infrastructure (Integrated) Configuration	22
9	Sample Distributed Infrastructure (Segmented) Configuration	23
10	Sample Single-Host Infrastructure Cluster Configuration	26
11	Storage Agent for Symmetrix in a Proxy Configuration	95
12	Example Cross-Section of an LDAP Directory	102
13	Sample NAT Firewall Configuration	299
14	Sample Code from listener.ora file	303
15	SNMP Communications between FCC Agent and Switch or SP	308
16	ControlCenter Console-to-Server Communication	315
17	Accessing the ControlCenter Console across a Firewall	316
18	ControlCenter Infrastructure and Agents	319
19	StorageScope Port Usage	324

1	Sample Storage Array Notes	3
2	Sample Switch Notes	3
3	Sample Host Notes	3
4	Sample Database Notes	4
5	Managed Object Sizes	5
6	Required Agents for Topology View Functions	46
7	Required Agents for Relationship View Functions	47
8	Required Agents and Licenses for Free Space View	48
9	Summary of Agents and Associated Managed Objects	50
10	Agent Planning Data Center Example	52
11	Master Agent Installation Notes	55
12	Master Agent Data Center Example	56
13	Integration Gateway Quick Summary	57
14	Integration Gateway Deployment Field	58
15	Workload Analyzer Archiver Quick Summary	58
16	Workload Analyzer Archiver Deployment Field	59
17	Managed Objects per WLA Archiver	60
18	BackupAgent Data Center Example	61
19	Backup Agent for EDM Quick Summary	62
20	Backup Agent for EDM Deployment Field	62
21	Backup Agent for Legato NetWorker Quick Summary	63
22	Backup Agent for Legato NetWorker Deployment Field	63
23	Backup Agent for TSM Quick Summary	64
24	Backup Agent for TSM Deployment Field	65
25	Backup Agent for VERITAS NetBackup Quick Summary	65
26	Backup Agent for VERITAS NetBackup Deployment Field	66
27	Common Mapping Agent Quick Summary	67
28	Managed Objects per Common Mapping Agent	69
29	Fibre Channel Connectivity Agent Quick Summary	70
30	Symmetrix SDM Agent Quick Summary	73

31	Database Agent for Oracle Quick Summary	74
32	Host Agents for AIX, HP-UX, Linux, and Solaris Quick Summary	76
33	Host Agent for Novell Quick Summary	77
34	Host Agent for Novell Deployment Requirement	78
35	Host Agent for Windows Quick Summary	78
36	Storage Agent Data Center Example	80
37	Storage Agent for Centera Quick Summary	81
38	Storage Agent for ESS Quick Summary	81
39	Storage Agent for CLARiiON Quick Summary	82
40	Storage Agent for HDS Quick Summary	83
41	Storage Agent for HP StorageWorks Quick Summary	85
42	Storage Agent for NAS Quick Summary	86
43	Storage Agent for SMI Quick Summary	91
44	Storage Agent for Symmetrix Quick Summary	92
45	Storage Agent for Invista Quick Summary	93
46	Interface Software for Proxy Agents	95
47	Suggested WLA Revolving Policy for Proxy Symmetrix Agent	96
48	LDAP Installation Notes	103
49	Tools Installation Notes	118
50	Repository Installation Notes	133
51	ECC Server Installation Notes	136
52	Store Installation Notes (for a Multihomed Host Only)	141
53	Components Optionally Installed on Infrastructure Hosts	143
54	Console Installation Notes	166
55	StorageScope Installation Notes	183
56	License Key Requirements for ControlCenter Agents	211
57	ControlCenter Agent Disk Space Requirements	212
58	Agent Administration Wizard Buttons	217
59	Objects and Agents Participating in Assisted Discovery	230
60	Switch Ports for FCC Agent Firewall Communication	307
61	Ports for ECC Server Communications	314
62	Agent Acronyms, Listening Ports, Processes, Filenames	320
63	Database Accessibility Alert Indicators	337
64	Contents of the ConnectEmc_service.ini File	343
65	Contents of the ConnectEMC Input XML File	344

As part of an effort to improve and enhance the performance and capabilities of its product line, EMC from time to time releases revisions of its hardware and software. Therefore, some functions described in this guide may not be supported by all revisions of the software or hardware currently in use. For the most up-to-date information on product features, refer to your product release notes.

If a product does not function properly or does not function as described in this guide, please contact your EMC representative.

Audience

This guide is part of the EMC ControlCenter documentation set, and is intended for use by system and data storage administrators.

Readers of this guide are expected to be familiar with the following topics:

- ◆ Storage array operation
- ◆ Host operating environments

Organization

The major sections of this guide are:

- ◆ *Document Your Storage Environment*, explains how to document and classify your storage environment, so you can select the optimal ControlCenter configuration for that environment.
- ◆ *Plan the Infrastructure*, describes how to plan for the ControlCenter infrastructure components (the ECC Server, Repository, and one or more Stores).
- ◆ *Plan for Business Functions*, describes how to plan for ControlCenter products and features.

- ◆ *Plan for Agents*, explains how to plan for the ControlCenter programs that collect data about resources in your environment, monitor the health of those resources, and run user commands.
- ◆ *Plan for Security and Remote Access*, describes how to plan for user authentication and access through a firewall.
- ◆ *Prepare to Install ControlCenter*, describes how to install ControlCenter infrastructure components.
- ◆ *Install and Start the Infrastructure*, describes how to install and start the ControlCenter infrastructure components (ECC Server, Repository, and one or more Stores).
- ◆ *Implement Business Functions*, describes how to install the ControlCenter user interfaces (the ControlCenter Console and WebConsole) and enable the various ControlCenter applications such as Integration Packages, Performance Manager, and StorageScope.
- ◆ *Deploy Agents and Perform Initial Discovery*, explains how to deploy the ControlCenter components that collect data about resources such as storage arrays, hosts, and switches.
- ◆ *Set Up Cluster Support (Optional)*, describes how to set up failover support for ControlCenter components and products.
- ◆ *Uninstall ControlCenter*, describes how to uninstall ControlCenter.
- ◆ *Appendix A, Installing FibreZoneBridge and FibreZone CLI*, describes how to install the listed products.
- ◆ *Appendix B, Port Usage and Firewall Configuration*, describes EMC ControlCenter TCP Port Usage requirements for ControlCenter.
- ◆ *Appendix C, Alternate Methods for Installing the Master Agent*, describes how to use utilities to distribute the Master Agent to several different hosts at one time.
- ◆ *Appendix D, AccessInfoChange Utility*, describes how to perform batch updates of access information required by the Common Mapping Agent and the Database Agent for Oracle.
- ◆ *Appendix E, ConnectEMC*, describes the EMC ControlCenter support for ConnectEMC.

An *Index* is located at the back of this document.

Related Documentation

You can access ControlCenter publications from the:

- ◆ *Documentation /Help* CD (provided with your EMC ControlCenter installation kit)

- ◆ ControlCenter Documentation Library (available from the ControlCenter Console Help menu)
- ◆ EMC Powerlink Documentation Library (<http://powerlink.emc.com>)

Conventions Used in This Guide

This book uses the following convention for notes.

A note presents information that is important, but not hazard-related.

Typographical Conventions

EMC uses the following type style conventions in this guide.

AVANT GARDE	Keystrokes
Palatino, bold	◆ Dialog box, button, icon, and menu items in text ◆ Selections from the user interface, including buttons, icons, options, and field names
<i>Palatino, italic</i>	◆ New terms or unique word usage in text ◆ Command line arguments when used in text ◆ Book titles
<i>Courier, italic</i>	Arguments used in examples of command line syntax.
Courier	System prompts and displays and specific filenames or complete paths. Examples: working root directory [/usr/ecc]: c:\Program Files\ecc\console
Courier, bold	◆ User entry. For example: sympoll -p ◆ Options in command line syntax.

Where to Get Help

For questions about technical support, call your local sales office or service provider. For service call one of the following and ask for Customer Support.

- United States: (800) 782-4362 (SVC-4EMC)
- Canada: (800) 543-4782 (543-4SVC)
- Worldwide: (508) 497-7901

**Sales and Customer
Service Contacts**

For a list of EMC sales locations, refer to the EMC home page.

<http://www.emc.com/contact/>

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink site at: <http://powerlink.emc.com>

Your Comments

Your suggestions help us improve the accuracy, organization, and overall quality of the user publications. Please send a message to **techpub_comments@emc.com** with your opinions of this guide.

Before you begin to install EMC ControlCenter, follow the steps in this section to document and classify your storage environment, so you can select the optimal ControlCenter configuration for that environment.

This guide does not include information about installing EMC ControlCenter 5.2 SP4 agents and applications. For information about installing and configuring EMC ControlCenter 5.2 SP4, refer to *EMC ControlCenter 5.2 Service Pack 4 Release Notes*.

If you are installing Service Packs, refer to the installation instructions located in the release notes for each specific Service Pack release.

Important: Be sure to follow these steps before continuing on to other sections of this book. Thorough planning can greatly simplify ControlCenter installation and ensure that the ControlCenter configuration is optimized for your installation.

- ◆ Step 1: Document Your Storage Environment 2
- ◆ Step 2: Determine the Installation Size 5

Step 1 Document Your Storage Environment

Before installing EMC® ControlCenter®, list the assets (arrays, hosts, switches, databases, file systems, etc.) that you will be tracking.

A *managed object* is a named physical and logical element, of a type known to ControlCenter (for example, database, volume manager, zone set, port, physical device) that ControlCenter manages. List the number and size of objects that you want ControlCenter to manage, using the tables in this section as a guideline.

Follow these steps:

- Using a network diagram package (or a similar tool), diagram your storage network, showing the type and location of equipment (a sample is shown in Figure 1).

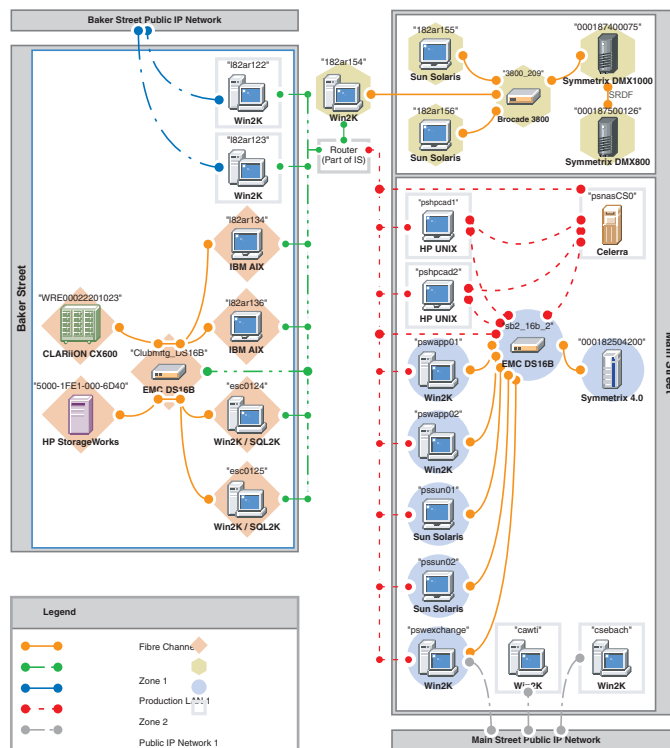


Figure 1 Sample Data Center Diagram

- b. Record information about storage arrays you want ControlCenter to manage in a matrix like the one shown in Table 1.

Table 1 Sample Storage Array Notes

Storage	Array Model	IP Addresses	Firmware Revision
WRE00022201023	CLARiiON [®] CX600	172.23.142.182 172.23.142.183	2.04.1.60.4.004
5000-1FE1-0005-E090	HP StorageWorks	None	V86F
000187400075	Symmetrix DMX [™] 1000	None	5669.42.19
psnasCS0	Celerra [®]	10.15.64.27	5.1.9-4

- c. Record information about the switches, hubs, and ports to be managed in a matrix like the one shown in Table 2.

Table 2 Sample Switch Notes

Switch	Switch Type	IP Addresses (Nodes)	Firmware Revision
3800_209	Brocade 3800	172.23.172.209	3.0.2m_rc4
Clubmftg_DS16B	EMC DS16B	172.23.174.170	2.6.0d

- d. Record information about the hosts to be managed in a table like the one shown in Table 3. Refer to *EMC ControlCenter Support Matrix* on Powerlink[™] to ensure that each host identified in your worksheet has the required hardware and software.

Table 3 Sample Host Notes

System Administrator	Host	IP Address	Host Purpose	Server Make and Model	OS Version, Patch Level	Fibre Channel HBA	HBA Driver
Mary Baker	pshpcw3	168.159.90.63	Payroll	Dell	Windows 2003	-----	-----
James Nasium	cawti	168.159.90.60	Web Server	Compaq	Windows 2000, SP3	-----	-----
Mark Dawson	l82ar134	172.23.172.134	Database	IBM F80	AIX 4.4.3, 10	6227	-----
David Hoffmann	pshpcad1	10.15.64.23	CAD	HP	HP-UX 11	-----	-----
Gary Schilling	cawyi	168.159.90.65	Build	Dell	Linux	-----	-----

Table 3 Sample Host Notes (continued)

System Administrator	Host	IP Address	Host Purpose	Server Make and Model	OS Version, Patch Level	Fibre Channel HBA	HBA Driver
Hilary Johnson	pssun01	10.15.64.22	Oracle Database	Sun 220R	Solaris 8, 108528-08	Emulex LP8000	5.01b
Tom Wilkerson	pswap01	10.15.64.18	Transaction Engine	Dell	Windows 2003	Emulex LP8000	2.13
Leslie Uggams	pswxchg	10.15.64.20	Exchange Server	Dell	Windows 2000, SP3	Emulex LP8000	2.13

- e. Record information about the databases to be managed in a table like the one shown in Table 4. Refer to *EMC ControlCenter Support Matrix* on Powerlink to ensure that each database identified in your worksheet meets the prerequisites.

Table 4 Sample Database Notes

Database	Host	IP Address	Tablespaces	Data Files	Schemas
salesprod	pssun01	10.15.64.22	100	250	50
hrprod	l82ar134	172.23.172.134	25	75	20

Step 2 Determine the Installation Size

Determine your installation size by classifying managed objects (hosts, arrays, databases, etc.) as small, medium, or large, counting the managed objects of each size, and using the sizing tables in *EMC ControlCenter Performance and Scalability Guidelines* on Powerlink as a guide in determining your overall installation size.

- ◆ 2.1 *Classify managed objects as small, medium, or large* on page 5.
- ◆ 2.2 *Count the number of managed objects of each size* on page 6.
- ◆ 2.3 *Determine the installation size* on page 6.

2.1 Classify managed objects as small, medium, or large

Using Table 5, classify managed objects in your data center as small, medium, or large. When using the table, keep in mind that managed object size is determined by the number of objects (not total capacity). For example, a host that has 1 TB of storage spread over 10 devices (10 metavolumes) is considered *small*.

Important: When using Table 5, keep the following in mind.

- ◆ A *host device* is a physical device, such as `/dev/rdisk/cXtXyd`
- ◆ A *Symmetrix[®] logical volume* is a virtual disk drive within a Symmetrix array (it is the same as a Symmetrix *logical device* or *hypervolume*).
- ◆ An *agent host logical volume* is a logical device with multiple host devices, created by a logical volume manager such as VERITAS.
- ◆ If the size of a managed object exceeds the large classification, contact EMC Customer Support for assistance.

Table 5 **Managed Object Sizes**

Managed Object	Resource	Small	Medium	Large
Symmetrix	Logical volumes	1-800	801-2000	2001-8192
	Front-end mappings	Up to 1600	Up to 4000	Up to 16000
CLARiiON	Logical devices	1-32	33-256	257-1024
NAS	Logical devices	1-150	151-500	501-1200
	Data movers	2	4	10

Table 5 Managed Object Sizes (continued)

Managed Object	Resource	Small	Medium	Large
<i>Switch</i>	Ports	1-16	17-64	65-256
<i>Oracle database</i>	Sum of data files and tablespaces	1-800	801-1600	1601-2048
<i>SQL Server or Sybase</i>	Sum of databases, data files, log files, file groups	1-100	101-200	201-400
<i>MVS LPAR</i>	DASD devices	1-600	601-1500	1501-3000
<i>DB2</i>	Sum of data files and tablespaces	1-800	801-1600	1601-2048
<i>Agent host</i>	Host devices	1-16	17-128	129-512
	Logical volumes	1-16	17-64	65-128
	File systems (NTFS, UFS, VVFX)	1-16	17-64	65-128
	Redundant paths	1-2	3-4	5-32

2.2 Count the number of managed objects of each size

Count the number of managed objects of each size in your data center. The totals will be used in the next step.

2.3 Determine the installation size

Using the number and size of managed objects obtained in the previous steps, determine the installation size, using the sizing tables in *EMC ControlCenter Performance and Scalability Guidelines* on Powerlink as a guide. If you need assistance with the performance and scalability guidelines for installation size, contact Customer Support.

The most important part of planning your ControlCenter configuration is determining how to install the ControlCenter *infrastructure* components (the ECC Server, Repository, and one or more Stores).

If you plan to install ControlCenter on a host that has multiple IP addresses connected to networks, you must also plan for ControlCenter *multihoming*. If you want to provide failover capability for the ControlCenter infrastructure and other components, you must also plan for ControlCenter *cluster support*.

Important: Follow these steps before continuing to other sections of this book. Careful planning of the infrastructure can greatly simplify ControlCenter installation and ensure that ControlCenter is optimized for your installation.

- ◆ Step 3: Know the ControlCenter Architecture 8
- ◆ Step 4: Determine the Configuration Type 12
- ◆ Step 5: Plan for ControlCenter Multihoming (Optional) 17
- ◆ Step 6: Plan for Cluster Support (Optional) 24

Step 3 Know the ControlCenter Architecture

ControlCenter architecture has the following major components:

- ◆ **ControlCenter interfaces** allow you to monitor, manage, and report on your ControlCenter environment. The interfaces include the ControlCenter Console and the Web Console, which allow you monitor and control the storage infrastructure from a central point, and related applications like StorageScope[™] and Performance Manager Automated Reports, which allow you to view reports through Web interfaces.
- ◆ The **Infrastructure** contains:
 - One *ECC Server* that processes requests from the Console and controls all managed objects.
 - One *Repository*, a relational database that contains data about ControlCenter and the storage environment.
 - One or more *Stores*, which write persistent data (collected by agents) to the Repository.
 - One *WebConsole Server*, which controls communications for the Web Console, a Web-based interface to ControlCenter.
- ◆ **Agents** manage specific objects (such as storage arrays, Fibre Channel switches, and hosts), monitor those objects for alert conditions, gather information about object performance and configuration, and perform active commands. ControlCenter uses the following types of agents.
 - *Master Agent*: Runs on each agent host to manage the application agents.
 - *Application agents*: Run on agent hosts to manage specific storage resources.
 - *Proxy agents*: Provide indirect access to resources. Examples are Storage Agent for Symmetrix and Common Mapping Agent, which can communicate with EMC Solutions Enabler, located on a remote host, to monitor and manage storage resources.

Figure 2 (a *single-host infrastructure* configuration) shows how the ControlCenter architecture might appear when the ControlCenter infrastructure components are installed on one host machine.

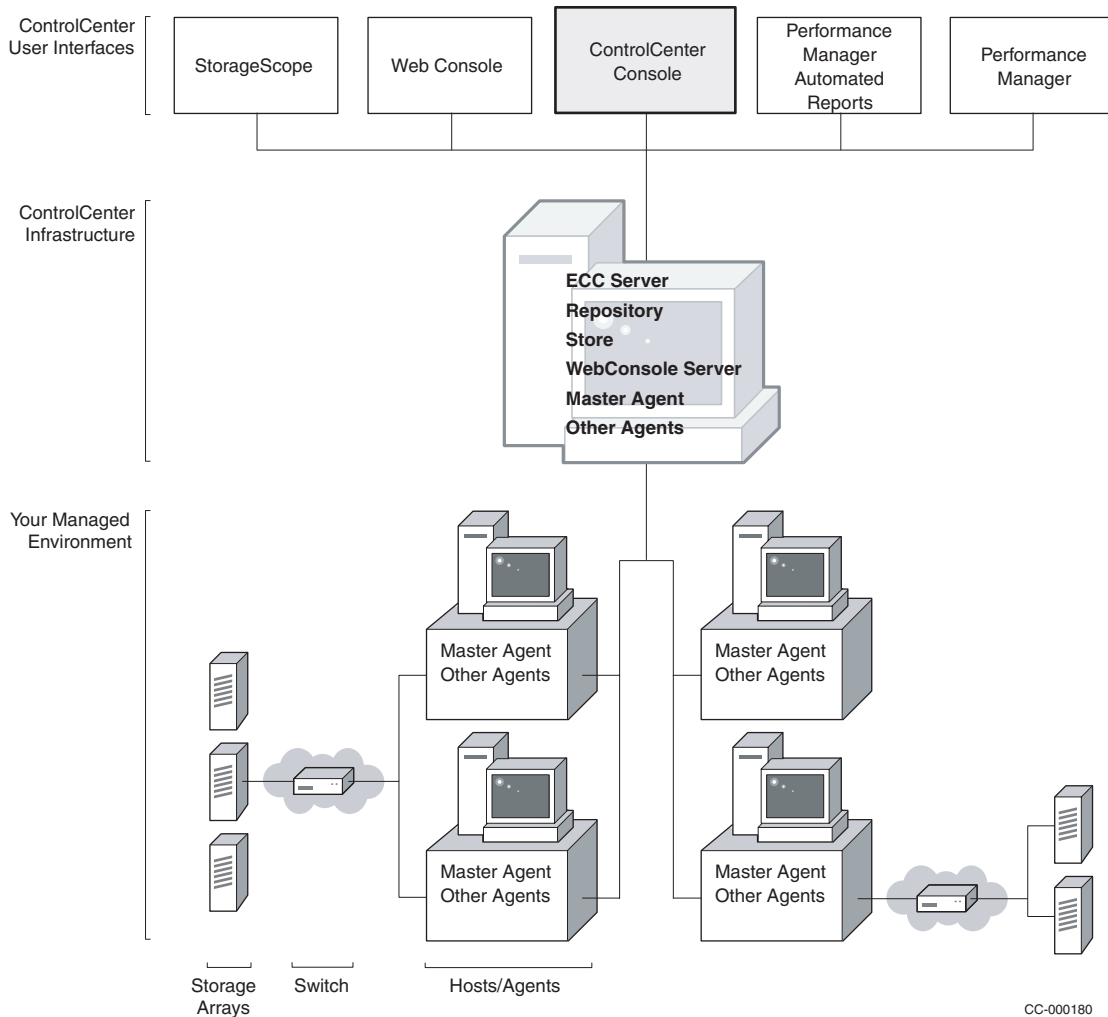


Figure 2 **Architecture for a Single-Host Infrastructure Configuration**

Figure 3 (a *distributed infrastructure* configuration) shows how the ControlCenter architecture might appear when the ControlCenter infrastructure components are installed on two or more machines.

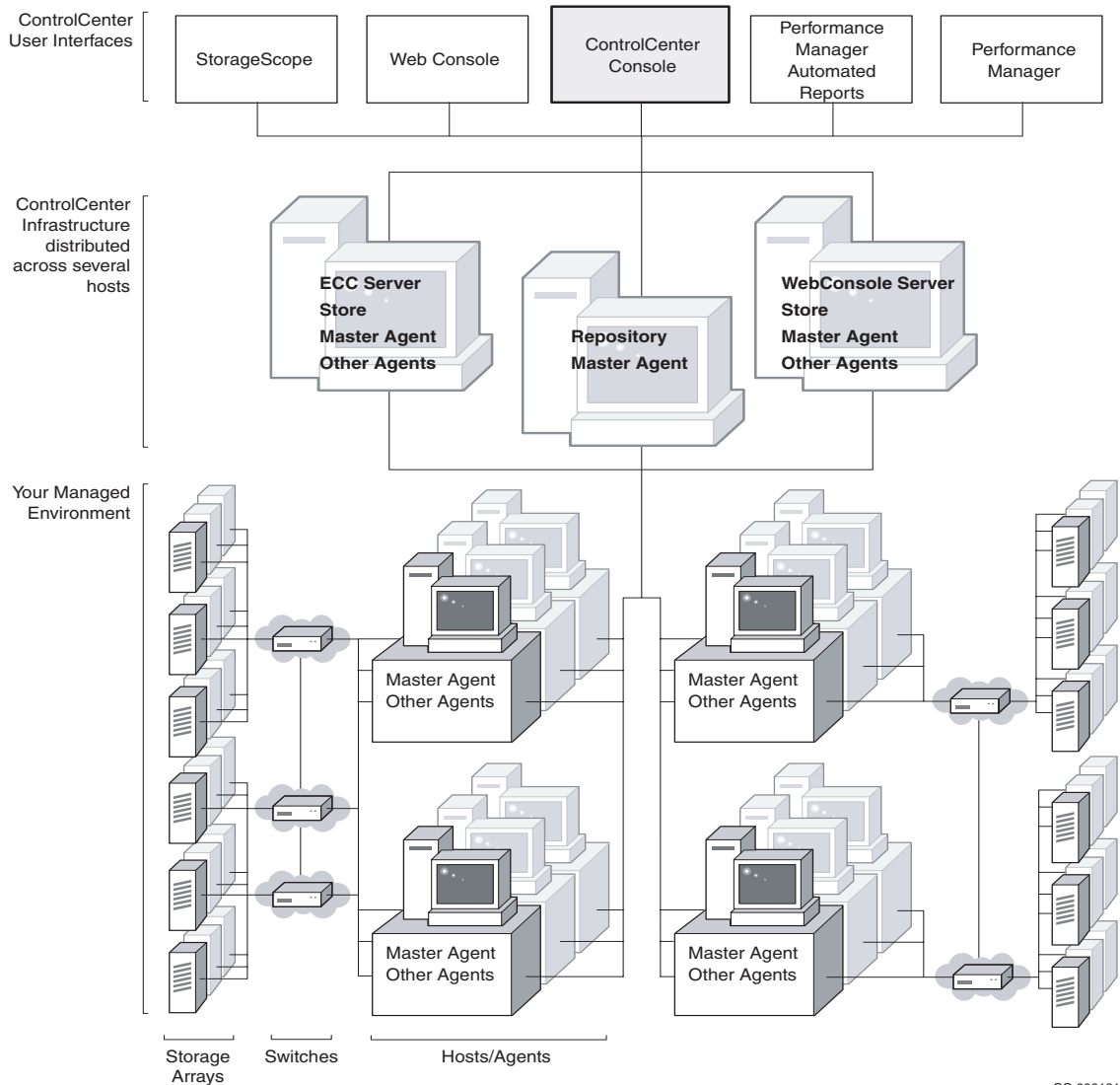
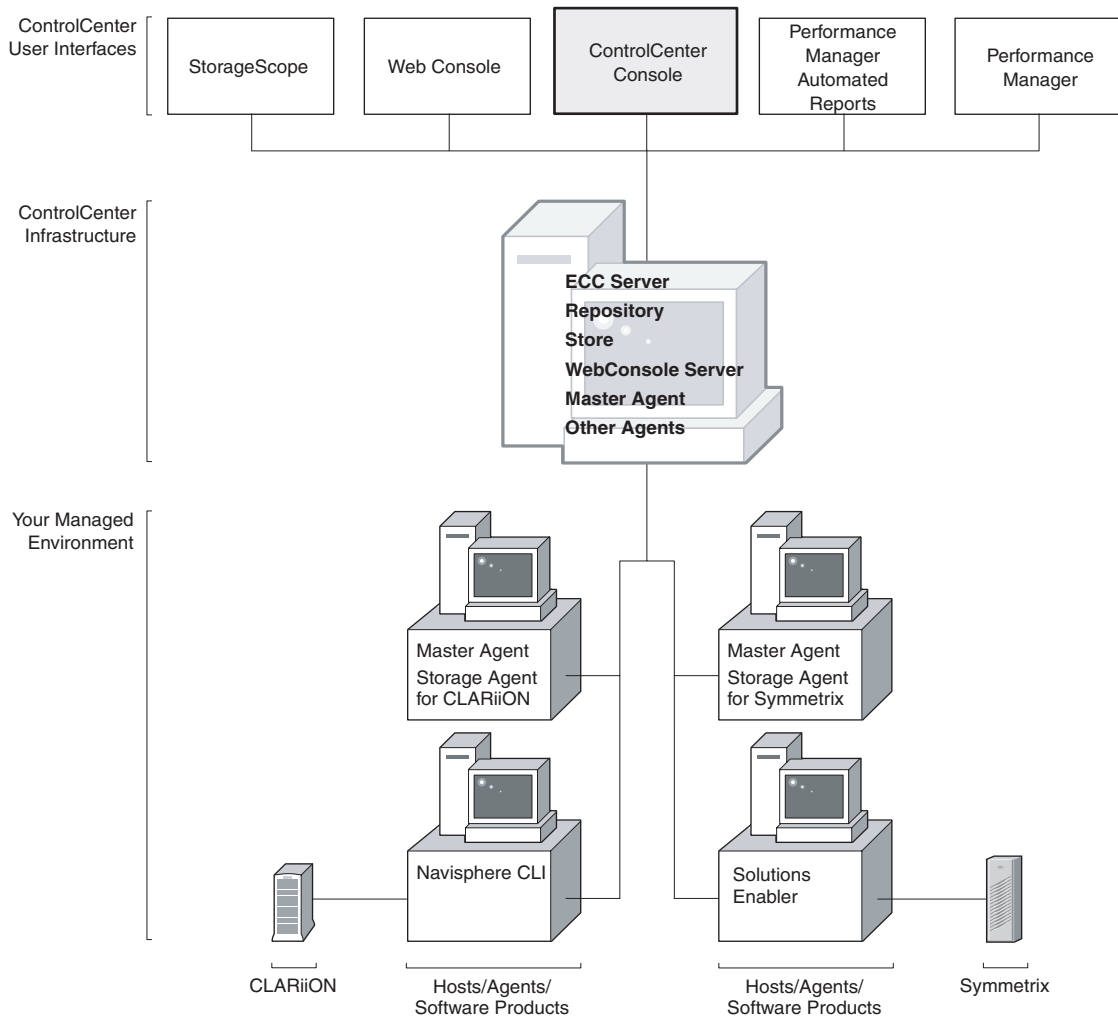


Figure 3 Architecture for a Distributed Infrastructure Configuration

Some ControlCenter agents can communicate in *proxy mode* to manage resources that are not directly connected to the host where the agent is installed. For example, Figure 4 shows Storage Agent for Symmetrix and Storage Agent for CLARiiON running in proxy mode to manage Symmetrix and CLARiiON arrays.



CC-000182

Figure 4 Example Single-Host Infrastructure Configuration (Proxy Mode)

Step 4 Determine the Configuration Type

One of the major steps toward implementing ControlCenter is determining how the ECC Server, Store(s), and Repository—the three *infrastructure components*—are to be configured. Consider the following:

- ◆ Should the ECC Server, Store(s), and Repository be installed on *one* machine (a ***single-host infrastructure*** configuration)?

This is often the best practice for small- to medium-sized installations (refer to *Step 2: Determine the Installation Size* on page 5) that do not anticipate significant growth in the near future (for example, over the next two to four years). This setup can minimize costs and simplify management of the ControlCenter infrastructure, but does not offer the best environment for future performance and scalability enhancements.

- ◆ Should the ECC Server, Store(s), and Repository be installed on *different* machines (a ***distributed infrastructure*** configuration)?

This is often the best practice for medium- to large-sized installations (refer to *Step 2: Determine the Installation Size* on page 5) or smaller installations that anticipate a large amount of growth in the near future. The distribution of components across several machines allows for optimal performance and scalability.

Follow these steps to determine the optimal ControlCenter configuration type:

- ◆ 4.1 *Identify the optimal configuration type* below.
- ◆ 4.2 *Select one or more hosts for the ECC Server, Repository, and Store(s)* on page 15.

4.1 Identify the optimal configuration type

Using the installation size obtained from *Step 2: Determine the Installation Size* on page 5, determine the ControlCenter configuration type, which is one of the following:

- ◆ Single-host infrastructure
- ◆ Distributed infrastructure

Single-Host Infrastructure

The ECC Server, Store, and Repository reside on one host. In most cases, this configuration is recommended for small- to medium-sized installations that do not anticipate significant growth in the near future (for example, over the next two to four years).

Figure 5 shows a typical single-host infrastructure configuration. Note that the ECC Server, Store, and Repository are installed on the Windows host in the center. Consoles are installed on other hosts connected to the ECC Server host through TCP/IP, and agents are installed on hosts where they can monitor storage elements.

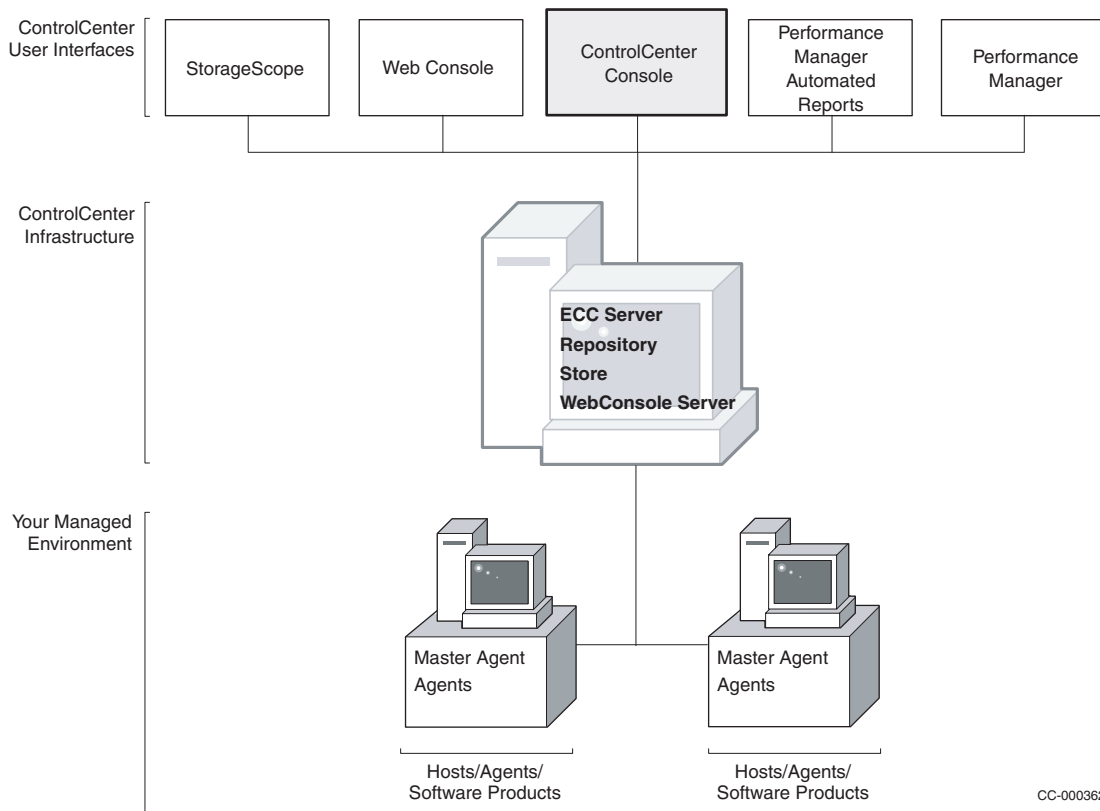
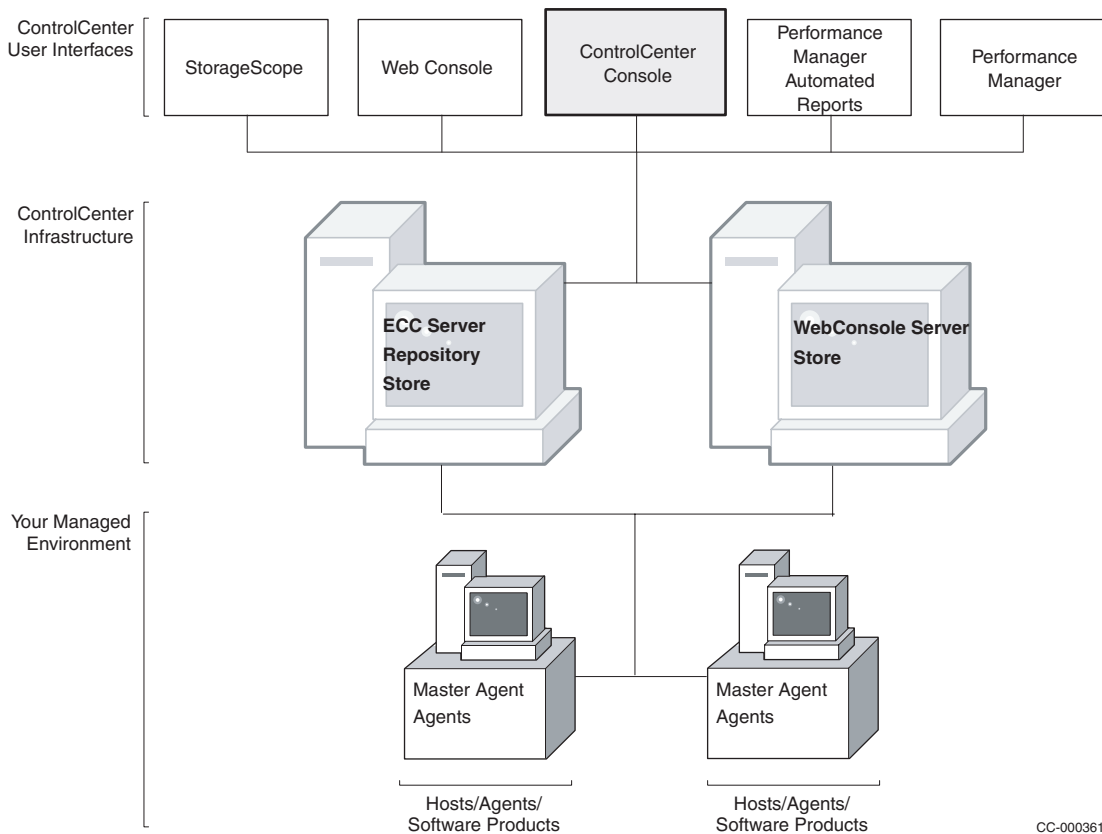


Figure 5 Single-Host Infrastructure with Remote Console and Agents

Distributed infrastructure

The ECC Server, Store, and Repository are distributed among two or more hosts. In most cases, this configuration is recommended for medium- to large-sized installations or smaller installations that anticipate a large amount of growth in the near future.

For example, your initial configuration could have the ECC Server and Repository on separate hosts, with one Store installed on the ECC Server host and a second Store installed on another host, as shown in Figure 6. As your installation grows, you can install additional Stores.



CC-000361

Figure 6 Distributed Infrastructure with Separate Stores

When considering separate hosts for infrastructure components, keep the following in mind:

- ◆ In a distributed infrastructure configuration, EMC recommends that you install the Repository on a dedicated host.
- ◆ The activity of the Store corresponds to when each agent runs its data collection policies (refer to *EMC ControlCenter 5.2 Administration/User Guide* for details on data collection policies). It is important to evenly distribute the schedule for data collection and rediscovery, particularly for the largest managed objects.
- ◆ If more than one Store is installed, the allocation of a Store to an agent happens dynamically, based on the current load on the Store. In addition to load balancing, this mechanism also provides redundancy—if a Store goes down, the agent traffic is routed to a different Store.

4.2 Select one or more hosts for the ECC Server, Repository, and Store(s)

Do one of the following:

- ◆ If a *single-host infrastructure* setup is appropriate, install the Repository, ECC Server, and Store on *one host* that meets or exceeds the minimum requirements for memory, processing power, and disk space, as described in *EMC ControlCenter Performance and Scalability Guidelines* on Powerlink.
- ◆ If a *distributed infrastructure* setup is appropriate, select hosts for the Repository, ECC Server, and Store(s) that meet or exceed the minimum requirements for memory, processing power, and disk space for the desired components, as described in *EMC ControlCenter Performance and Scalability Guidelines* on Powerlink.

Important: Be aware that some issues have been reported with installing or upgrading the ControlCenter Repository on Windows hosts that are configured with Terminal Services. EMC suggests that you disable Terminal Services (which requires a reboot) before installing or upgrading the Repository on hosts where Terminal Services is configured. You can restart Terminal Services after the install or upgrade is complete. Refer to *Step 23: Consider Services for Remote Access* on page 105 for details.

Performance and Scalability Guidelines Infrastructure Hosts

Follow these recommendations when providing disk high availability for infrastructure hosts.

When allocating disk space on infrastructure hosts:

- ◆ For disk high availability, use a mirrored (RAID 1) disk (This requires additional physical hard drives).
- ◆ For system performance, at a minimum, use a RAID controller for disk mirroring. To increase performance, use disk arrays such as Symmetrix (metavolume) or CLARiiON (RAID-10 LUN).

Host-based mirroring is strongly discouraged.

When a Store is overloaded or the configuration size increases to the next classification, consider adding another Store or distributing DCPs.

When the `Store Load` alert displays in the Console Alert view and does not reset for about an hour, a Store is overloaded. That alert triggers when the workload of a Store exceeds a threshold value, indicating that you might need to add a Store.

To determine the cause of overloading:

- ◆ Investigate whether DCPs are properly distributed. If they are scheduled to start concurrently, reschedule them accordingly.

Note: Be aware that DCPs run based on the system time of the agent host. The agent host system time and the Store system time may be different.

- ◆ Determine if managed objects were added to ControlCenter over time without proper redistribution or consideration of the existing, associated DCPs.

After determining which DCPs caused the overload, address the overload conditions by doing one or all of the following:

- ◆ Distribute DCPs evenly over longer periods of time so bottlenecks are not created.
- ◆ Decrease the frequency of the DCPs (for example, change the frequency from one minute to five minutes).
- ◆ Move from a single-host configuration to distributed configuration by uninstalling Store component in single-host configuration and installing Store on a new host, or adding more Stores on new hosts.

Step 5 Plan for ControlCenter Multihoming (Optional)

Multihomed describes a host machine that has multiple IP addresses connected to networks. A multihomed host is physically connected to multiple data links that can be on the same or different networks.

When you install ControlCenter on a host that has multiple network interface cards (NICs) or one NIC with multiple interface connections or port connections, the ControlCenter installation program automatically detects the host cards and follows an installation path for multihoming.

This section describes how to plan for ControlCenter multihoming support at your installation, using these steps:

- ◆ 5.1 *Know when multihoming is required* below.
- ◆ 5.2 *Understand networking issues for multihoming* on page 18.
- ◆ 5.3 *Recommended: Organize your network traffic* on page 19.
- ◆ 5.4 *Recommended: Verify network topology and routing* on page 19.
- ◆ 5.5 *Ensure proper name resolution on your network* on page 20.
- ◆ 5.6 *Understand the supported configurations* on page 21.

5.1 Know when multihoming is required

Multihoming is required when implementing the following for ControlCenter:

- ◆ **Traffic management:** Routing ControlCenter data traffic through different networks can increase the performance and scalability of an entire system. For example, your installation could handle traffic that is specific to ControlCenter on one network, other production traffic on a second network, and perform nightly backups on a third network.
- ◆ **Cluster support:** To provide continuous availability and backup in the event of a host failure, your installation might want to set up cluster support for ControlCenter. Refer to *Step 6: Plan for Cluster Support (Optional)* on page 24 for more information.

When you install ControlCenter on a multihomed host (one with multiple NICs or a NIC with multiple interface connections or port connections), the ControlCenter installation program automatically detects the NICs and prompts you for the required installation fields to set up multihoming support for ControlCenter.

5.2 Understand networking issues for multihoming

When setting up multihoming for ControlCenter, keep the following in mind:

- ◆ The following are *not supported*:
 - Dynamic host addressing (DHCP) for any ControlCenter host with an infrastructure component or host agent. The only exception is a host on which only the Console (no other ControlCenter component) is installed.

If you mistakenly install the ControlCenter infrastructure on a host with a DHCP-configured network interface card (NIC), refer to the *EMC ControlCenter 5.2 Troubleshooting Help* (available in the Documentation Library in the ControlCenter Console help menu, or the Troubleshooting button in the ControlCenter installation wizard) for information about how to correct your configuration.

- Adapter Teaming (which groups network adapter ports for a connection to a single physical segment—if connectivity through one port is not working, another port is activated automatically) on hosts where infrastructure components reside.
- ◆ Windows Resource Kits provides an in-depth discussion of issues in configuring multihoming. Some points include:
 - NetBIOS over TCP/IP binds to the first IP address for each network adapter only.
 - DNS configuration settings are global.
 - WINS configuration settings are defined for each adapter.
 - Only one active default gateway is used at a time.

5.3 Recommended: Organize your network traffic

One of the main goals of multihoming is to route ControlCenter data over management networks so production networks can be reserved for other applications. The following guidelines are recommended for organizing the network traffic at your installation:

- ◆ Install ControlCenter infrastructure components on one or more hosts that are part of your management network, unless ControlCenter Consoles reside on the production network (if so, refer to the next guideline).
- ◆ ControlCenter Consoles *can* reside on hosts in production networks, but *should* reside on hosts in management networks. If Consoles reside on a production network, the ECC Server and Repository should also reside on that network because the amount and frequency of data transfer between those components is typically high.
- ◆ Configure production (agent) hosts so they reside on both production and management networks, including any cyclical (midnight) backup network.
- ◆ If your networks are isolated, install ControlCenter components so they can be accessed on each network. For example, install Performance Manager once on each isolated subnet. Be aware that if multiple Stores exist in your configuration, the Stores will automatically perform load balancing.

5.4 Recommended: Verify network topology and routing

Once the network topology is finalized, configure routing to enable communication between ControlCenter components.

- ◆ Ensure that ControlCenter management traffic follows the desired route by adjusting the routing configurations on the Console, Store, and agent hosts and their intermediate routers. The ECC Server and Repository should serve each management network for ECC Server, Store, Console, and StorageScope access.
- ◆ Some ControlCenter features, such as Store load balancing and data archival, require the ECC Server to dynamically assign the network addresses of Stores to agents. For agents on a remote management network (one that is not directly attached to the server host) to support this feature, routing on the ECC Server host needs appropriate configuration.

- ◆ For a single-host infrastructure ControlCenter configuration, ensure that all ControlCenter Console hosts and agent hosts can reach one of the listening network addresses on the ECC Server. Agents should also be able to reach at least one Store in your ControlCenter configuration.

Distributed infrastructure

If the Repository and ECC Server are installed on different hosts, ensure that the ControlCenter Console and Stores can reach at least one listening network address for both the ECC Server and Repository.

5.5 Ensure proper name resolution on your network

During installation, use network names instead of IP addresses whenever possible. Use of network names avoids the need to reconfigure ControlCenter if IP address assignments change (a common security practice).

- ◆ Use the fully-qualified domain name (FQDN) to avoid ambiguity.
- ◆ Map each of the ECC Server and Repository management IP addresses to a unique network name.
- ◆ Ensure that hostnames are added to DNS. Contact the network administrator to ensure that the IP addresses for each NIC on the ECC Server host are registered with DNS.
- ◆ Ensure that the ECC Server, Store, ControlCenter Console, Web Console, Performance Manager, and StorageScope can resolve the Repository's network names.
- ◆ If you specify IP addresses instead of hostnames (be sure to verify the hostname/IP relationship in DNS), replace the IP addresses with their corresponding hostnames in the following file.

```
%RAMBOH%\network\admin\listener.ora
```

Then, in a command window, enter the following two commands:

```
lsnrctl stop
lsnrctl start
```

Important: You cannot specify IP addresses when setting up ControlCenter in a cluster environment—you must use hostnames. Refer to *Step 53: Install the ControlCenter Infrastructure in a Clustered Environment* on page 244 for details.

5.6 Understand the supported configurations

The example *single-host infrastructure* configuration shown in Figure 7 has a multihomed infrastructure host that can reach the production network, the management network, and the storage configuration.

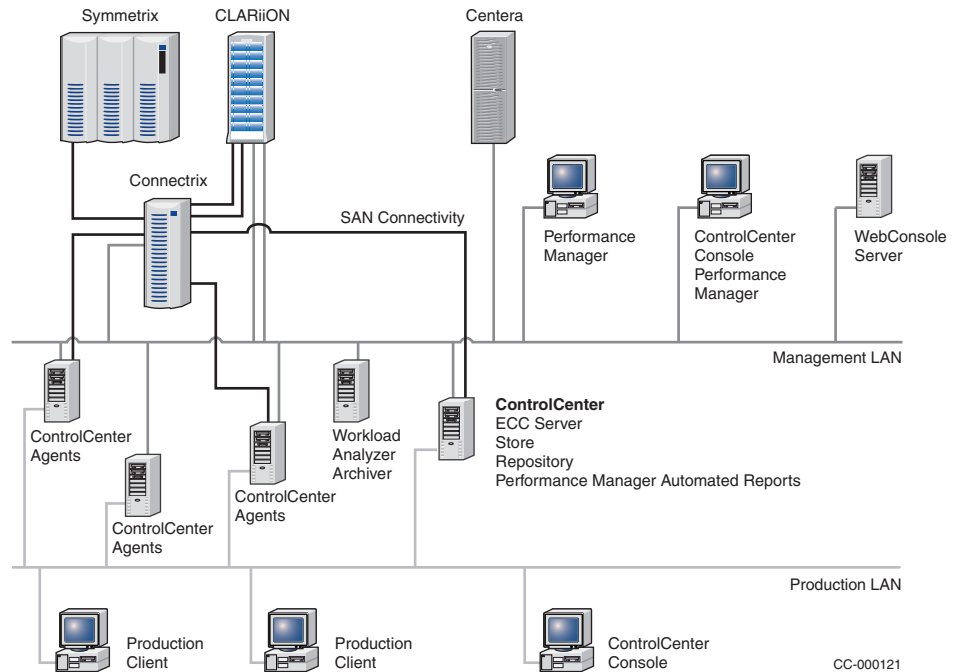


Figure 7 Sample Single-Host Infrastructure Multihoming Configuration

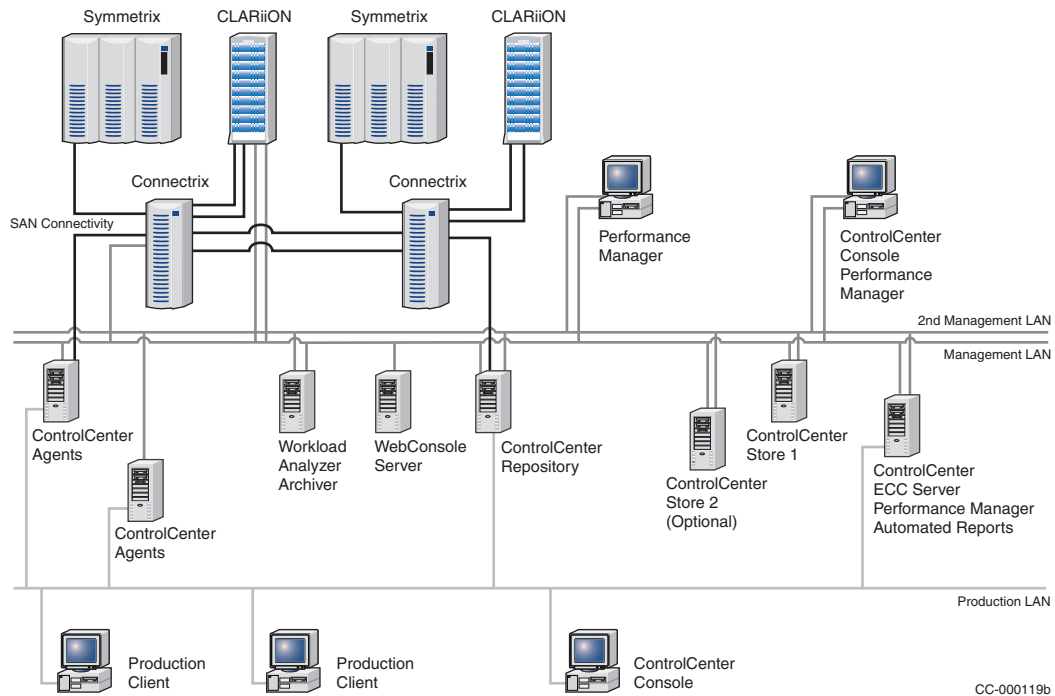


Figure 8 Sample Distributed Infrastructure (Integrated) Configuration

Distributed Infrastructure

In an *integrated configuration* (refer to Figure 8), ideally each infrastructure host is multihomed and connected to each network that supports ControlCenter.

- ◆ The Repository and ECC Server hosts are connected to both management LANs.
- ◆ Store hosts and Workload Analyzer Archiver agent hosts are connected to both management LANs.
- ◆ Agent hosts are connected to one or both management LANs and the production LAN.
- ◆ Each agent can communicate only with Workload Analyzer Archiver agents on the same LAN as the agent host.

Distributed Infrastructure

When multihoming is used as part of a *segmented configuration*, Store hosts are connected only to isolated subnets that support ControlCenter, as shown in Figure 9.

- ◆ The Repository, StorageScope server, ECC Server (and Performance Manager Automated Reports service) hosts are connected to the management LANs.
- ◆ Each Store host and Workload Analyzer Archiver agent host is connected to its own management LAN.
- ◆ Each agent host is connected to one or both management LANs and the production LAN.
- ◆ Each agent can communicate only with Workload Analyzer Archiver instances on the same LAN as the agent host.

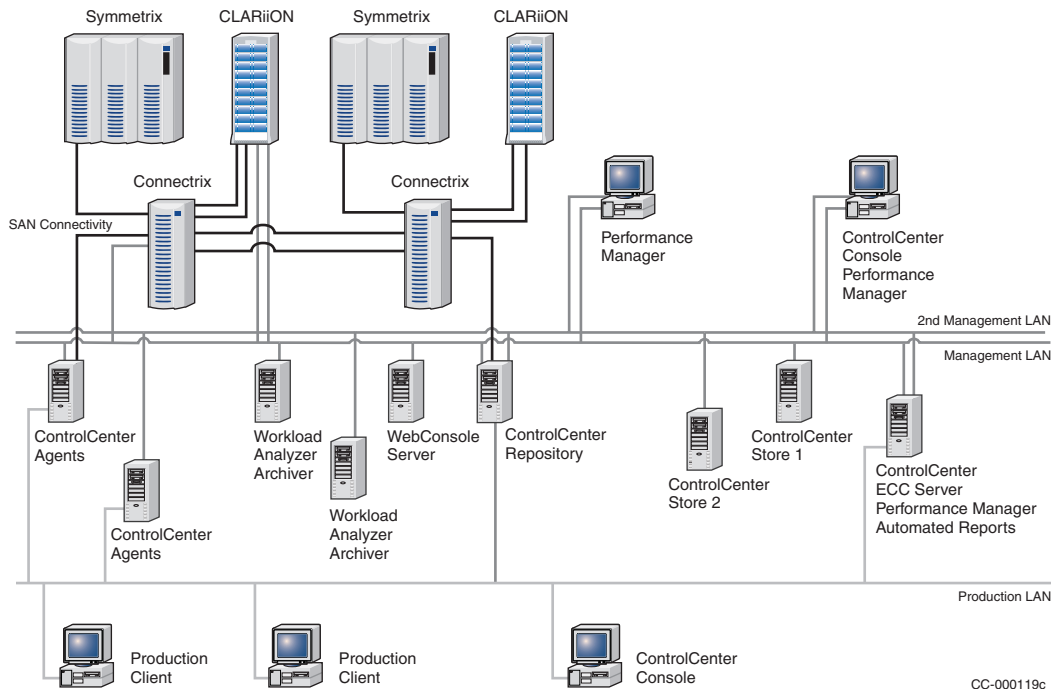


Figure 9 Sample Distributed Infrastructure (Segmented) Configuration

Step 6 Plan for Cluster Support (Optional)

A *cluster* is a set of hosts that can perform failover operations to reduce downtime in the event of a host failure. When a system-level failure requiring failover occurs on the active primary host, a backup standby takes over. When the primary host is back online, you can manually perform failback to the primary host.

This section describes how to plan for cluster support for ControlCenter, using the following steps:

- ◆ 6.1 *Know the software required for cluster support* on page 24.
- ◆ 6.2 *Understand cluster support for ControlCenter* on page 25.
- ◆ 6.3 *Establish a multihomed environment* on page 25.
- ◆ 6.4 *Understand what happens at cluster failover* on page 27.

6.1 Know the software required for cluster support

ControlCenter cluster support is provided through the following.

- ◆ **Microsoft Windows Advanced Server Cluster Service (MSCS):** Allows hosts running Windows in the same domain to be connected to a shared storage system, to protect against failure of production server hardware or network connections. If one host fails, another host assumes the application workload. To implement ControlCenter cluster support, you must implement MSCS using the guidelines in:
 - *Microsoft Step-by-Step Guide to Installing Cluster Service:*
<http://www.microsoft.com/windows2000/techinfo/planning/server/clustersteps.asp>
 - *Introducing Windows 2000 Clustering Technologies*
<http://www.microsoft.com/windows2000/techinfo/howitworks/cluster/introcluster.asp>
- ◆ **EMC GeoSpan for MSCS:** A software extension that allows Windows hosts running MSCS to operate across SRDF[®]-connected Symmetrix systems in geographically distributed clusters. Two Symmetrix systems, connected through SRDF, provide automatic failover of SRDF-mirrored volumes during host failover, which extends the maximum distance between cluster nodes to 60 km and forms a geographically distributed cluster with disaster-tolerant capabilities.



6.2 Understand cluster support for ControlCenter

ControlCenter works with only certain features of MSCS, and only certain ControlCenter products and components are supported:

- ◆ **Only active/passive clusters are supported.** In this type of cluster, a primary (active) host performs normal processing, and a secondary (passive) host restarts applications with full performance when a failure occurs on the active host. *Active/active* clusters, where both hosts run application software during normal operation and all the work is transferred to one host if a failure occurs, are not supported for ControlCenter.
- ◆ **Only two-node clusters are supported.** Although MSCS and EMC GeoSpan for MSCS support both two-node (one host failing over to another) and four-node (for up to three host failures) clusters, only two-node clusters are supported for ControlCenter.
- ◆ The following ControlCenter infrastructure components and products are supported for clustering on an ControlCenter infrastructure host:
 - ECC Server (includes the Performance Manager Automated Reports and WebApplications Server services)
 - Repository
 - Store(s)
 - WebConsole Server (includes ControlCenter API Server service)
 - Master Agent
 - StorageScope
 - Workload Analyzer Archiver

Refer to *Step 53: Install the ControlCenter Infrastructure in a Clustered Environment* on page 244 for instructions on installing infrastructure components in a cluster.

- ◆ EMC does not support installing host agents and infrastructure components on the same hosts in a cluster. Refer to *Install ControlCenter Agents in an Application Clustered Environment* on page 261 for instructions on installing host agents in a cluster.

6.3 Establish a multihomed environment

You must create a multihomed host environment to implement clustering support for ControlCenter. Refer to *Step 5: Plan for ControlCenter Multihoming (Optional)* on page 17 for details. Figure 10

shows a cluster setup where each physical node is multihomed and the cluster is connected to its heartbeat LAN and external networks.

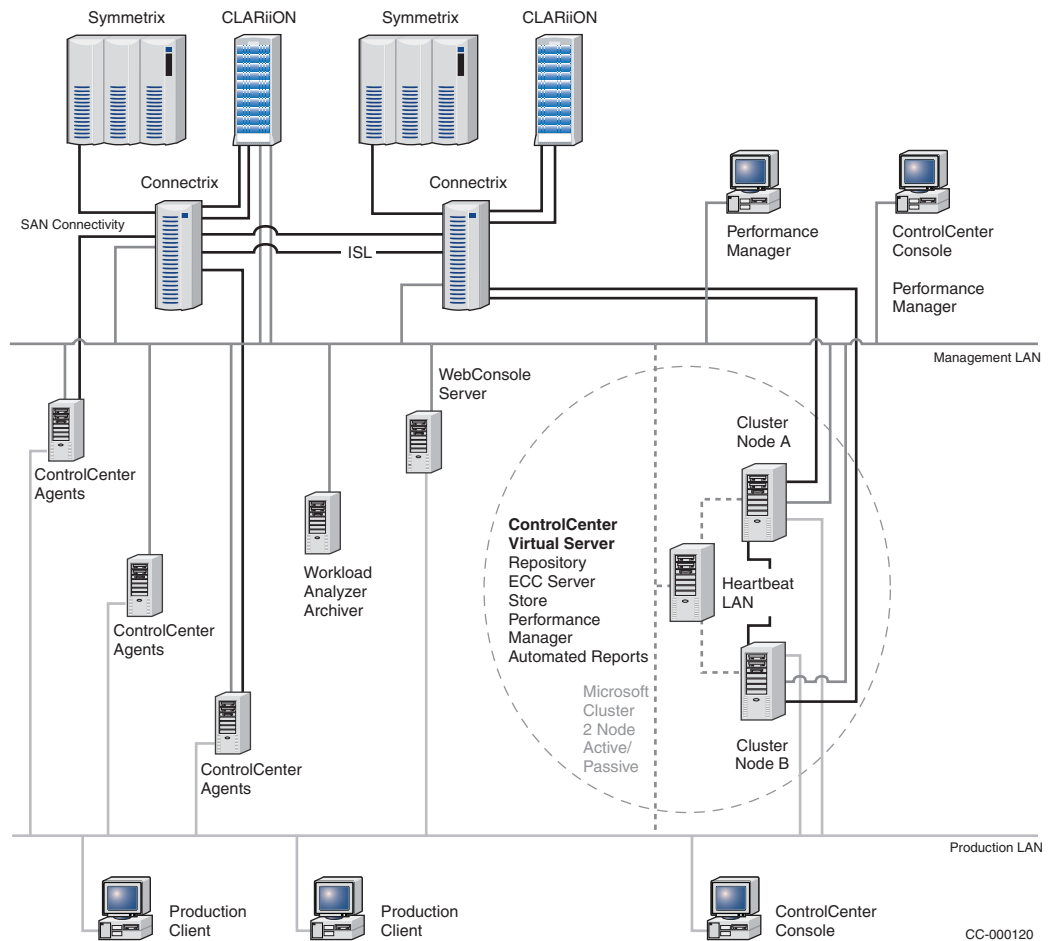


Figure 10 Sample Single-Host Infrastructure Cluster Configuration

Firewall Requirement

If your ControlCenter cluster environment includes a firewall, ensure that the firewall allows access to both the real (physical) and virtual (cluster) IP addresses for the ECC Server.

6.4 Understand what happens at cluster failover

If failover occurs in a ControlCenter cluster environment, ControlCenter services shut down immediately on the failed node, with the exception of the ECC Server and Store services, which can take several minutes to shut down completely.

Do the following if failover occurs:

- ◆ Allow sufficient time for all ControlCenter services to shut down completely on the failed node.
- ◆ **Restart ControlCenter Consoles:** Depending on your infrastructure configuration, you must restart ControlCenter Consoles as follows:
 - *Single-host infrastructure:* If ControlCenter fails over and restarts, you must restart all ControlCenter Consoles.
 - *Distributed infrastructure:* If the Repository fails over and restarts, but failover takes more than 10 minutes to complete, you must restart the Store(s), Consoles, and StorageScope instances. If the ECC Server fails over and restarts, you must restart all Stores and ControlCenter Consoles.
- ◆ **Prevent immediate failback:** If ControlCenter components or products fail over to a primary or secondary host, *you must reboot the failed node*, and then perform manual failback. Because some ControlCenter processes do not shut down completely on the failed node, automatic failback is not allowed.

To prevent automatic failback from occurring, disable “Automatic failback” for the appropriate resource group.

ControlCenter is comprised of several products and features—some are installed automatically with the base product, while others are installed with the ControlCenter installation CDs. Some products and features are automatically enabled for installation and do not require license keys, while others require separate license keys.

This section describes how to plan for implementing ControlCenter applications, which involves the following steps:

1. Verify the main applications and features that your installation has purchased, using the descriptions in this section.
2. Determine which applications and features require license keys, which applications are automatically installed with the base product, and which applications must be installed with the ControlCenter installation CDs.
3. Plan to install the *agents* (refer to *Plan for Agents* on page 49) that are required to enable the functions associated with your enabled applications.

Important: Follow these steps before continuing in this book. Thorough planning can greatly simplify ControlCenter installation and ensure that the ControlCenter configuration is optimized for your installation.

◆ Step 7: Plan for Open Integration Components (OIC).....	30
◆ Step 8: Plan for Licensed Features and Applications.....	32
◆ Step 9: Plan for Console Interfaces	40
◆ Step 10: Plan for PowerPath Volume Manager	45
◆ Step 11: Plan for Console Views	46

Step 7 Plan for Open Integration Components (OIC)

The ControlCenter open integration components (OIC) are a set of common services that are available to all EMC ControlCenter products. The services include centralized installation, agents for all managed resources, login and access control administration, a Repository for storing data, and so on. None of the OIC services require license keys. When you install the ControlCenter base product, you automatically receive access to the open integration components.

Open Integration Components (OIC) Quick Summary	
Source	Automatically installed with the ControlCenter base product.
Required Licenses	None. OIC functions and features do not require license keys.
Allows these agents to be deployed: ◆ Common Mapping Agent (enables full functionality) ◆ Database Agent for Oracle (enables discovery, monitoring, and alerts) ◆ Integration Gateway (enables full functionality) ◆ Master Agent ◆ Host Agents for AIX, HP-UX, Linux, Solaris, and Windows ◆ Storage Agent for SMI	Includes these features and applications: ◆ Alerts (Display, Edit Properties, Edit Source, Edit Conditions) ◆ Command history ◆ Data collection policies (DCPs) ◆ Discovery (refer to <i>Deploy Agents and Perform Initial Discovery</i> on page 191 for details) ◆ Integration Packages ◆ Web Console and Web Console Server (refer to <i>Know when to use the Web Console</i> on page 44 for details) ◆ Performance Manager (installation only) ◆ PowerPath[®] Volume Manager

Integration Packages

Integration Packages is a program included with ControlCenter OIC that allows ControlCenter to be integrated with most of the leading management framework applications such as the following:

- ◆ BMC PATROL Enterprise Manager
- ◆ BMC PATROL
- ◆ CA Unicenter TNG
- ◆ HP OpenView Network Node Manager
- ◆ HP OpenView Operations
- ◆ IBM Tivoli NetView
- ◆ IBM Tivoli Enterprise Console (TEC)
- ◆ MicroMuse Netcool/OMNIBus
- ◆ Microsoft Operations Manager

Frameworks not specifically supported can receive unformatted traps using the FibreAlliance MIB V3.0.

To enable support for the listed applications:

1. Install the Integration Gateway agent (refer to *Plan for the Integration Gateway* on page 57 for details).
2. Download the Integration Packages component installation files to the host that is running your framework application.
3. Install the Integration Packages component on the host.

Refer to *EMC ControlCenter Integration Packages Product Guide* for details about Framework applications.

Integration Packages Quick Summary	
Source	ControlCenter Web installation interface (refer to <i>Step 39: Install the Integration Packages (Optional)</i> on page 175 for details).
Licenses	Integration Packages is available with Open Integration Components (the ControlCenter base package).
Agent	Integration Gateway
Required Installation Field	
<i>Integration packages download location</i>	The directory where you intend to download the Integration Packages installation files. <i>Default: C:/ecc/InstallIntPkg</i>

Step 8 Plan for Licensed Features and Applications

This section describes the functions and agents that are available with ControlCenter licensed features and applications. Your installation can license any number of the listed features and applications. You can plan for licenses that apply to your installation in any order (you do not have to follow steps 8.1 through 8.7 in order).

- ◆ 8.1 *Plan for Automated Resource Manager (ARM).*
- ◆ 8.2 *Plan for SAN Manager on page 33.*
- ◆ 8.3 *Plan for Symmetrix Manager on page 34.*
- ◆ 8.4 *Plan for StorageScope on page 35.*
- ◆ 8.5 *Plan for Symmetrix Optimizer on page 37.*
- ◆ 8.6 *Plan for Performance Manager on page 38.*
- ◆ 8.7 *Plan for Celerra, Centera, and CLARiiON Agents on page 39.*

8.1 Plan for Automated Resource Manager (ARM)

Automated Resource Manager™ provides the storage provisioning, active host configuration, and automated alert fixes you need to respond to changing conditions in the data center. Automated Resource Manager also provides a central view to the free space throughout your storage environment.

Automated Resource Manager (ARM) Quick Summary

Source	Automatically installed with the ControlCenter base product—enabled with a license key.	
Required Licenses	ARM functions are enabled by entering the Automated Resource Manager license key provided in your ControlCenter package. The license allows you to deploy the agents shown below. Refer to <i>Step 37: License the Desired Applications</i> on page 171 for details.	
Provides deployment, discovery, & monitoring for: ◆ Fibre Channel Connectivity Agent ◆ Symmetrix SDM Agent Provides deployment and full functionality for: ◆ Backup Agents for EDM™, Legato® NetWorker, TSM, and VERITAS NetBackup ◆ Database Agent for Oracle ◆ Host Agent for Novell Provides full functionality for: ◆ Host Agents for AIX, HP-UX, Linux, Solaris, and Windows		Enables these features and applications: ◆ Free Space View (refer to <i>Step 11: Plan for Console Views</i> on page 46) ◆ Real-time explore of hosts with Host Agents ◆ Autofixes ◆ Storage Provisioning Services

8.2 Plan for SAN Manager

SAN Manager™ performs SAN discovery, topology representation, monitoring, performance, zoning, and active LUN masking. Key features are:

- ◆ Discovery and monitoring of storage networks and their components to detect and respond to error conditions.
- ◆ Ability to manage and zone McDATA/Connectrix®, Brocade, and CNT switches, as well as mixed fabrics.
- ◆ Limited discovery of Cisco switches that allows you to view the physical topology of these switches, and zoning functionality for Cisco switches.
- ◆ Thresholds for connectivity device and connectivity device port performance monitoring, event notification, policy-based management, and auditing the history of user actions.
- ◆ Can run ControlCenter in a secure fabric for McDATA and Brocade fabrics.
- ◆ Topology view that shows a pictorial view of an SAN, including user-defined objects and groups, zone/zone set highlighting, and toggling on and off links belonging to a selected object.
- ◆ Storage device masking (SDM), a feature that manages host port access privileges to logical devices in storage arrays.

SAN Manager Quick Summary	
Source	Automatically installed with the ControlCenter base product—enabled with a license key.
Required Licenses	SAN Manager functions are enabled by entering the SAN Manager license key provided in your ControlCenter package. This license allows you to deploy the agents and enable the functions shown below. Refer to <i>Step 37: License the Desired Applications</i> on page 171 for details on entering license keys.
Provides deployment, discovery, monitoring for: ◆ Storage Agents for CLARiiON and HP StorageWorks (includes LUN masking) ◆ Storage Agent for Symmetrix Provides deployment and full functionality for: ◆ Fibre Channel Connectivity Agent ◆ Database Agent for Oracle ◆ Storage Agent for HDS ◆ Symmetrix SDM Agent	Enables these features and applications: ◆ Topology View ◆ LUN Masking ◆ Switch Zoning

8.3 Plan for Symmetrix Manager

Symmetrix Manager supports a wide range of configuration and management controls. The controllable areas include:

- ◆ SDR (Symmetrix Disk Reallocation) — Map and unmap devices to Symmetrix front-end ports.
- ◆ Logical Device Configuration — Create additional storage capacity from unused physical disks within a Symmetrix unit.
- ◆ Meta Device Configuration — Create new metadevices and configure existing members of metadevices.
- ◆ Port Flag Settings — Configure flag settings on Symmetrix Fibre Channel and SCSI front-end ports for host communication.
- ◆ Device Type Definition — Convert DRV, BCV, and STD devices.
- ◆ Device Attribute Definition — Specify attributes such as RDB Checksum and Dynamic RDF.
- ◆ Device Protection Definition — Define the level of protection for a logical device.
- ◆ SRDF Device Definition — Define a local device and remote device as an SRDF pair.

Symmetrix Manager also automates the use of SRDF and TimeFinder® to provide business continuity and disaster recovery.

- ◆ SRDF creates and maintains a mirror image of one or more logical volumes on a remote Symmetrix array. Before you can use SRDF, the local and remote Symmetrix arrays must each be set up with at least two Remote Link Directors (RLDs) through which the two arrays are linked. The Symmetrix array being mirrored is designated as the source (R1); the Symmetrix array maintaining the remote mirror is designated as the target (R2). Data is transferred across the SRDF link from the source to the target array.
- ◆ TimeFinder manages the relationship between a standard storage device (STD) and business continuance volumes (BCVs) within the local Symmetrix system. These mirrored volumes contain a copy of the data while the original device is online for regular I/O operation. After the mirror image is established, you can split it from the standard device, manipulate the data (back it up or perform applications testing), and later reestablish the mirror image with the standard device.
- ◆ The TimeFinder clone feature allows you to make copies of data simultaneously on multiple target devices from a single source device. The data is available to a target's host once the session is

activated. You can copy data from a single source device to as many as sixteen target devices. A source device can be either a Symmetrix standard device or a TimeFinder BCV device. A target device can also be either an STD or BCV device designated to be a clone.

- ◆ EMC Snap[™] allows virtual copying operations that can save space and create instant, point-in-time copies of logical volumes. Snapping to a virtual device (VDEV) creates the appearance of copying volumes by simply copying the original data from changed tracks and the pointers to that data.
- ◆ QoS for TimeFinder/SRDF allows you more flexibility in managing the performance of Symmetrix arrays. By controlling the pace of BCV or SRDF copy operations on selected devices, you can increase the performance of selected BCV or SRDF devices within those groups, or increase the performance of primary devices relative to BCV and SRDF devices.

Symmetrix Manager Quick Summary	
Source	Available with the ControlCenter base product—enabled with a license key.
Required Licenses	Symmetrix Manager functions are enabled by entering the Symmetrix Manager license key provided in your ControlCenter package. Refer to <i>Step 37: License the Desired Applications</i> on page 171 for details.
Allows these open systems agents to be deployed: ◆ Storage Agent for Symmetrix	Enables these features and applications: ◆ SRDF ◆ TimeFinder ◆ TimeFinder clone ◆ EMC Snap ◆ QoS for TimeFinder/SRDF ◆ Visual Storage: EMC Symmetrix ◆ Symmetrix Manager

8.4 Plan for StorageScope

StorageScope provides a variety of Storage Resource Management reports to help customers assess their current storage environment and determine future storage requirements.

- ◆ *Service Consumers* reports assist in managing storage as a service by facilitating chargeback, capacity planning, and application availability activities.

- ◆ *Infrastructure* reports provide historical data about the configuration, capacity, and capacity utilization of the multi-vendor physical storage assets in the customer enterprise.

Users can create custom report layouts and export reports into CSV or XML format. Integration with third-party applications (for example, billing or customer care) is enabled through standard SQL views in the ControlCenter Repository and direct access to StorageScope XML files.

StorageScope Quick Summary	
Source	ControlCenter installation CDs (or a shared folder—refer to <i>Step 27: Set Up Shared Folder Installation (Recommended)</i> on page 120 for details).
Required Licenses	StorageScope functions are enabled by entering the StorageScope license key provided in your ControlCenter package. The license allows you to deploy the agents and enable the functions listed below. Refer to <i>Step 37: License the Desired Applications</i> on page 171 for details on entering license keys.
Provides deployment, discovery, & monitoring for: ◆ Fibre Channel Connectivity Agent ◆ Storage Agents for HDS, CLARiiON, Symmetrix ◆ Symmetrix SDM Agent Provides deployment and full functionality for: ◆ Backup Agents for EDM, Legato NetWorker[™], TSM, and VERITAS NetBackup ◆ Database Agent for Oracle ◆ Host Agent for Novell ◆ Storage Agents for HP StorageWorks (excluding LUN masking) and ESS Provides full functionality for: ◆ Host Agents for AIX, HP-UX, Linux, Solaris, and Windows	Enables these features and applications: ◆ StorageScope reporting ◆ StorageScope API (see description below) ◆ Free Space View (refer to <i>Step 11: Plan for Console Views</i> on page 46) ◆ Real-time explore of hosts with Host Agents ◆ Autofixes ◆ Visual Storage

StorageScope API

The StorageScope API, which is enabled with a StorageScope license, provides access to the following:

- ◆ StorageScope-generated XML files that contain structured historical snapshots of the data in the ControlCenter Repository.
- ◆ StorageScope-defined database views of current data by means of SQL queries into the ControlCenter Repository.

Using StorageScope API, your installation could create its own applications, such as reporting tools, that use the StorageScope interface. Install StorageScope API only if you plan to create

applications that offer functionality beyond that of StorageScope. Install StorageScope API only on the Repository host.

Important: StorageScope API is useful only to advanced users who want to create reporting functionality in addition to that offered by StorageScope. Most users should not install StorageScope API.

StorageScope API Quick Summary	
Source	ControlCenter installation CDs.
Required Licenses	Depends on the desired reports. Refer to <i>EMC StorageScope Reference Guide</i> for details.

8.5 Plan for Symmetrix Optimizer

Optimizer helps increase the performance of Symmetrix arrays by:

- ◆ Spreading I/O activity evenly across the physical disks. When a particular drive is in high demand, there are excessive seek operations on that drive. These operations slow down read and write activity. By balancing highly active logical devices and lower-activity logical devices across drives, seek activity is balanced, and contention among drives is reduced. Throughput within the overall Symmetrix system is improved, and users experience optimal response times.
- ◆ Monitoring physical drives that operate at different speeds, as well as location of the data on the physical media, which influences the I/O rate. This information is used when determining which logical devices to move.

Symmetrix Optimizer Quick Summary	
Source	Available with the ControlCenter base product—enabled with a license key.
Required Licenses	Symmetrix Optimizer functions are enabled by entering the Symmetrix Optimizer license key provided in your ControlCenter package. This license allows you to install the agents described below, which collect data used by Symmetrix Optimizer. Refer to <i>Step 37: License the Desired Applications</i> on page 171 for details.
Allows these open systems agents to be deployed: Storage Agent for Symmetrix	Enables these features and applications: Symmetrix Optimizer

8.6 Plan for Performance Manager

EMC ControlCenter Performance Manager allows you to monitor and analyze components in your ControlCenter environment.

Performance Manager collectively refers to the following components.

- ◆ The Performance Manager interface (formerly Workload Analyzer Performance View) is a Windows-based component used for viewing the historical, performance statistics processed by the Workload Analyzer Archiver and configuration data collected by other ControlCenter agents. When a Performance Manager license key is entered, *Performance Manager* is available from the ControlCenter Console (File, then Launch) and the Windows Programs menu (EMC, then EMC ControlCenter).
- ◆ *Performance Manager Automated Reports* (formerly Workload Analyzer Reports) presents historical performance data in reports that can be accessed through your Web browser. The data shown in the reports is defined through the Automated Reports Job Scheduler, which is accessed from Performance Manager.
- ◆ *Workload Analyzer Archiver* collects historical performance statistics collected by ControlCenter agents for storage systems, hosts, connectivity devices, and databases. Performance Manager generates views of the data collected by this agent.
- ◆ *WLA data collection policies* manage how and when the historical, statistical performance data is collected by the ControlCenter agents. Performance statistics data collection policies manage how and when the real-time, statistical performance data is collected by the Storage Agent for Symmetrix and Connectivity agent. The Historical Data DCP manages how the last 24-hours worth of data is collected for the Performance view.

Performance Manager Quick Summary	
Source	Installed from the ControlCenter installation CDs (or a shared folder—refer to <i>Step 27: Set Up Shared Folder Installation (Recommended)</i> on page 120).
Required Licenses	Performance Manager is available for installation with Open Integration Components (the ControlCenter base package). Full functionality is available with the Performance Manager license key provided in your ControlCenter package (refer to <i>Step 37: License the Desired Applications</i> on page 171 for details).
Allows these open systems agents to be deployed: - Discovery and monitoring only: Fibre Channel Connectivity Agent, Storage Agent for CLARiiON, Storage Agent for Symmetrix - Full functionality: Workload Analyzer Archiver	Enables these features and applications: - Performance Manager - Performance View

8.7 Plan for Celerra, Centera, and CLARiiON Agents

These licenses are required to install the following agents:

- ◆ Storage Agent for NAS (Celerra Agent), which monitors and manages Celerra Network Server, which works with EMC Symmetrix and CLARiiON storage arrays, and Network Appliance Filer from Network Appliance, Inc. For details refer to *Plan for Storage Agent for NAS* on page 86.
- ◆ Storage Agent for Centera™, which communicates with the EMC Centera systems in your environment and allows you to view detailed information about each of the systems, such as system components, file systems, and volumes. For details refer to *Plan for Storage Agent for Centera* on page 81.
- ◆ Storage Agent for CLARiiON, which allows you to explore and monitor EMC CLARiiON subsystems and their components, such as storage processors, devices, and the registered hosts that are connected to them. For details refer to *Plan for Storage Agent for CLARiiON* on page 82.

Step 9 Plan for Console Interfaces

This section describes the following interfaces, through which users can monitor and manage the ControlCenter environment:

- ◆ The *ControlCenter Console*, a Java application through which you can view and manage your ControlCenter environment, and perform a basic set of common functions, like discovery, monitoring, management, and ControlCenter administration (for authorized users only).

Remote users can alternatively use the *Web Console* (described next) or they can use VNC, Terminal Services, or Citrix to access the ControlCenter Console.

- ◆ The *Web Console*, a Web-based interface through which you can perform a limited number of ControlCenter functions, like monitoring, reporting, and alert management. Unlike the Console, no installation of the Web Console is necessary—users can access it through a Web browser. The Web Console is best suited to users who are to monitor ControlCenter remotely, or local users that do not require full Console capabilities.

Follow these steps when planning to install and run ControlCenter interfaces:

- ◆ 9.1 *Know when to install the ControlCenter Console.*
- ◆ 9.2 *Determine if you need remote access to the ControlCenter Console on page 41.*
- ◆ 9.3 *Determine ControlCenter Console hosts and verify their setup on page 41.*
- ◆ 9.4 *Know when to use the Web Console on page 44.*

9.1 Know when to install the ControlCenter Console

The *ControlCenter Console* is the user interface through which you can view and manage your storage environment and perform administrative functions, like agent deployment. It is a stand-alone, Java-based application that is installed on Windows or Solaris hosts using Microsoft Internet Explorer or Netscape Communicator, and launched from a desktop icon or from the command line. Multiple ControlCenter Consoles can exist within a single ControlCenter configuration.

Most ControlCenter applications are implemented as plug-ins to the ControlCenter Console. For an object to be displayed in the

ControlCenter Console, it must first be discovered by an agent. Once discovered, the object appears in the ControlCenter Console, grouped into its appropriate folder, such as Storage Systems, Hosts, or Connectivity. Information about the object can be retrieved by the ControlCenter Console from the Repository or in real-time directly from the agent. Any ControlCenter Console command that is issued for an object is passed from the ControlCenter Console to the ECC Server, and then forwarded to the appropriate agent to act on.

Install the *ControlCenter Console* when the intended user needs to perform most or all functions related to:

- ◆ Storage allocation
- ◆ Monitoring
- ◆ Performance management
- ◆ Administration maintenance
- ◆ Data protection
- ◆ Reporting (through StorageScope, which can be accessed directly from the ControlCenter Console)

Before installing the ControlCenter Console, consider the following:

- ◆ Do not install the Console software more than once on a host. To access more than one ECC Server from the same host, you can run separate instances of the same installed Console software.
- ◆ Do not install a Console that is intended for access over a VPN. The Console does not support VPN access. Alternatively, you can access Consoles *across* a VPN using Terminal Services, Citrix, or VNC (all are described in the next step, 9.2).

9.2 Determine if you need remote access to the ControlCenter Console

Citrix, Terminal Services, and VNC can help remote users access the ControlCenter Console, which is installed on a host where a server component is running, while the display is transmitted over the network to client hosts. Refer to *Step 23: Consider Services for Remote Access* on page 105 for details about using Citrix, Terminal Services, and VNC.

9.3 Determine ControlCenter Console hosts and verify their setup

Install the ControlCenter Console on hosts that meet the minimum requirements. The specifications are for hosts that do not contain any ControlCenter infrastructure components (ECC Server, Repository,

and Store) and ControlCenter Consoles that run with logging turned on.

For information about minimum requirements, refer to *EMC ControlCenter Planning and Scalability Guidelines* at Powerlink.

The following are additional requirements for Console hosts.

- ❑ Set virtual memory to at least 1 GB. (Virtual memory is managed most by the operating system, and is typically twice the amount of physical memory.)

For information about physical memory size requirements, refer to *EMC ControlCenter Planning and Scalability Guidelines* at Powerlink.

- Windows — To check the current virtual memory setting, from the Windows Start menu, select **Settings, Control Panel, System**. Then click **Advanced**. Then do one of the following, depending on the operating system.
 - Windows 2000: Click the **Performance Options** button. If necessary, change the virtual memory setting by clicking the **Change** button in the *Performance Options* dialog box.
 - Windows 2003: Click **Settings** in the **Performance** section and then click **Advanced**. If necessary, change the virtual memory setting by clicking **Change** in the *Virtual Memory* section.
 - XP: To check the current virtual memory setting, click **Control Panel**, and then click **System Info, Performance, Virtual Memory**.
- Solaris — To check the current virtual memory, type **vmstat 1 1** (every 1 second, 1 sample). The total available virtual memory is displayed in the swap column with the value in kilobytes. Type **man vmstat** to read more about virtual memory. The following example displays virtual memory in a **bold font**:

```
# vmstat 1 1
```

```

kthr      memory          page        disk          faults        cpu
r  b  w   swap  free  re  mf  pi  po  fr  de  sr  s6  s4  s3  s3    in   sy   cs  us  sy  id
0  0  0   5247512 3555336 1   9   0   0   0   0   0   0   0   0   0   944   86  126   0   0 100

```

- ❑ All previous ControlCenter Console instances must be uninstalled (refer to *Uninstall ControlCenter* on page 271).

- ❑ On Windows, the %TEMP% system variable must be configured and pointing to a valid directory. If %TEMP% is not set properly, the Console download stops at: Initializing Wizard.
- ❑ Internet Explorer or Netscape (see *EMC ControlCenter Support Matrix* on Powerlink for version information) must be installed to use the Web interface for ControlCenter Console installation.
- ❑ The browser used to install the Console must have a Java Virtual Machine (JVM) that can run the installation download program. If your browser does not have a suitable JVM, the Console installation program will tell you to download and install a valid JVM from the Sun Microsystems website before beginning the installation, and provide a hyperlink to the download area on the Sun Microsystems website.
- ❑ If using Internet Explorer, under **Tools, Internet Options, Advanced**, ensure that under Java (Sun), **Use Java %version% for <applet> (requires restart)** is selected, where %version% is the version of the JVM installed on the system.

9.4 Know when to use the Web Console

The *Web Console* is a Web interface to ControlCenter that allows you to remotely monitor and report on your storage-attached network. The Web Console provides a more portable solution than the ControlCenter Console because you can simply access it through a Web browser. However, the Web Console does not offer all the functionality of the ControlCenter Console. Use the *Web Console* in the following cases:

- ◆ You need to perform ControlCenter monitoring through a Web browser.
- ◆ You have Web access to ControlCenter and do not have ControlCenter Console installed.
- ◆ There are bandwidth limitations on the network that prevent you from using the ControlCenter Console.
- ◆ To monitor ControlCenter remotely (perhaps through a firewall).

You can perform the following ControlCenter functions remotely using the Web Console:

- ◆ View the properties and relationships of a managed object
- ◆ Monitor active alerts for managed objects
- ◆ View the history of issued commands
- ◆ Build a dynamic topology map of a SAN
- ◆ Monitor the I/O paths in a SAN
- ◆ Monitor the performance of Symmetrix storage array Fibre Channel connectivity device ports
- ◆ Alert Management
- ◆ Assign alerts
- ◆ Acknowledge alerts
- ◆ Clear alerts
- ◆ View, add, or edit alert notes
- ◆ Review alert history
- ◆ Generate reports (access StorageScope to perform reporting tasks)

Step 10 Plan for PowerPath Volume Manager

ControlCenter allows you to take advantage of the advanced volume management features of PowerPath Volume Manager (PPVM) if you have it installed on a UNIX host. Using ControlCenter, you can explore, configure, and manage your logical volumes and their component elements to better utilize your storage resources.

None of the operations require a license key (all are available as part of the ControlCenter OIC).

The following PPVM operations are available through ControlCenter:

- ◆ *Volumes*: Explore and view the properties of volumes defined on a host. Create, remove, or extend logical volumes. Explore the physical extents of a volume. Explore the logical extents of a volume.
- ◆ *Images*: Explore the images of a volume. Add, remove, disable, and set preferred status for volume images.
- ◆ *Volume Groups*: Create or remove volume groups, explore the storage elements assigned to volume groups, add and remove storage elements to and from volume groups.

To learn more about using PPVM in ControlCenter, refer to *ControlCenter Console Online Help*.

Step 11 Plan for Console Views

This section explains how to plan for views that are accessed through the ControlCenter Console and Web Console.

- ◆ 11.1 *Plan for Topology View.*
- ◆ 11.2 *Plan for Relationship View* on page 47.
- ◆ 11.3 *Plan for Free Space View* on page 47.

11.1 Plan for Topology View

The *topology view* represents the physical configuration of the network. It displays the connectivity topology from the host, through the connectivity devices, to the underlying storage arrays.

The topology can be viewed at the host, switch, and array level, or expanded to show the actual physical port-level connectivity (HBA, switch port, array port). ControlCenter host, connectivity, and storage agents collect all the information required to generate the topology map, as shown in Table 6. The connectivity agents collect most of the information required to develop the topology. If no host or storage agents are present, the HBA-to-host or FA port-to-array mapping information can be manually entered.

Table 6 Required Agents for Topology View Functions

Operation	Required Agents
◆ Discover hosts and configuration properties	Host agent for the target platform
◆ Discover switch, fabric, and configuration properties ◆ Discover switch neighbors (HBA and FA ports)	Fibre Channel Connectivity Agent
◆ Discover storage array and configuration properties	Storage agent for the particular array
◆ Map hosts to HBAs	◆ Host agent for the target platform ◆ Fibre Channel Connectivity Agent
◆ Map FA ports to storage arrays	◆ Storage agent for the particular array ◆ Fibre Channel Connectivity Agent

11.2 Plan for Relationship View

Multiple agents are required for a full visual display of the relationship between host structures (databases, file systems, volume groups) and their logical and physical locations in storage arrays as shown in Table 7:

- ◆ Host agents discover and collect data on the file system, volume manager, and host volumes for that host, as well as the storage array logical devices within the array where these host structures reside.
- ◆ Database Agent (Oracle) or Common Mapping Agent (Informix, Sybase, SQL Server, DB2) collects database internal relationships (instances, tablespaces, databases, data files) and their relationship to the file systems or raw devices where they reside.
- ◆ Storage agents discover and collect data on logical device mapping. Storage Agent for Symmetrix and SYMAPI Server additionally collect LUN-to-physical drive mapping information.

Table 7 Required Agents for Relationship View Functions

Operation	Required Agents
◆ Discover database and configuration ◆ Map database to file system	◆ Database Agent for Oracle ◆ Common Mapping Agent
◆ Discover hosts and host data structures ◆ Discover storage arrays and logical devices and map their relationships	◆ Host agent for the target platform ◆ Fibre Channel Connectivity Agent
◆ Map logical devices to physical disks	◆ Storage Agent for Symmetrix ◆ SYMAPI Server (part of EMC Solutions Enabler)

11.3 Plan for Free Space View

Free Space View shows free space and allocated space for storage arrays related to a selected host or host cluster with options to get detailed information for HBAs, ports, devices, and pools. The following storage arrays are supported: EMC CLARiiON, EMC Symmetrix, Hitachi Data Systems, HP StorageWorks HSG80 (EMA), HP StorageWorks XP, and IBM ESS.

You can use Free Space View to address the following questions:

- ◆ How much storage has been allocated to the host, where is it, and how much storage has not yet been used by the host?
- ◆ How much storage has been mapped to a host-accessible port, but has not been allocated?
- ◆ How much storage is available to the host from a specific storage array?
- ◆ How much storage has been allocated, and used, by databases, tablespaces, file systems, and other logical objects?

Note: Free Space view cannot display information about Symmetrix arrays that have been discovered through Storage Agent for SMI. To view a Symmetrix array in Free Space View, use Storage Agent for Symmetrix to manage the array.

Table 8 Required Agents and Licenses for Free Space View

Operation	Required Agents	Required Licenses
Displaying Free Space View	Storage Agent for Symmetrix, CLARiiON, IBM ESS, HDS, or HP StorageWorks	Automated Resource Manager (ARM) or StorageScope

ControlCenter uses *agents* to collect data about physical and logical resources in your environment. Agents can also monitor the health of those resources and run user commands for configuring disk groups, volumes, and file systems.

There are different agents for each type of resource. You can deploy more than one agent on a host. The resource(s) to be monitored must reside on the local host or another resource in your environment that is accessible to that host. A *Master Agent* controls all the agents on each host.

Planning to deploy agents involves determining which agents are required and where they are to be deployed, using the steps in this section.

◆ Step 12: Perform General Agent Planning	50
◆ Step 13: Plan for Master Agents.....	54
◆ Step 14: Plan for Common Agents.....	57
◆ Step 15: Plan for Backup Agents.....	61
◆ Step 16: Plan for Common Mapping Agent.....	67
◆ Step 17: Plan for Connectivity Agents	70
◆ Step 18: Plan for Database Agent for Oracle	74
◆ Step 19: Plan for Host Agents.....	76
◆ Step 20: Plan for Storage Agents.....	80
◆ Step 21: Plan for EMC Solutions Enabler.....	97

Step 12 Perform General Agent Planning

ControlCenter *application agents* (in other words, all agents except the Master Agent) are programs that run on hosts to control, collect data from, and monitor the health of resources. You must determine which application agents to install and the hosts where those agents are to reside.

The main factors in determining which agents to install are your ControlCenter applications which require agents to collect their source data. *Plan to install only the agents that are needed to provide data required by your ControlCenter environment.*

This chapter explains how to plan for agent installation, using the following steps:

- ◆ 12.1 *Know the agents, managed objects, and groups.*
- ◆ 12.2 *Understand basic agent requirements on page 52.*

12.1 Know the agents, managed objects, and groups

Table lists all the application agents and the managed objects that they control, along with references to sections of this book that describe each agent in detail. Use the table to determine the agents required by your installation. Then use the referenced detailed steps in this book to plan for installation of those agents.

Table 9 Summary of Agents and Associated Managed Objects

Agent	Install to Discover	Reference to Details
<i>Backup Agent for EDM</i>	EMC Data Manager servers	<i>Plan for Backup Agent for EDM on page 61</i>
<i>Backup Agent for Legato NetWorker</i>	Legato NetWorker servers	<i>Plan for Backup Agent for Legato NetWorker on page 63</i>
<i>Backup Agent for Tivoli Storage Manager (TSM)</i>	Tivoli Storage Manager servers	<i>Plan for Backup Agent for TSM on page 64</i>
<i>Backup Agent for VERITAS NetBackup</i>	VERITAS NetBackup servers	<i>Plan for Backup Agent for VERITAS NetBackup on page 65</i>
<i>Common Mapping Agent</i>	Windows, Linux, and UNIX hosts, Informix, Sybase, SQL Server, DB2/ UDB databases (monitoring only)	<i>Plan for Common Mapping Agent on page 67</i>

Table 9 Summary of Agents and Associated Managed Objects (continued)

Agent	Install to Discover	Reference to Details
<i>Database Agent for Oracle</i>	Oracle databases (on the agent host or remote hosts)	<i>Plan for Database Agent for Oracle on page 74</i>
<i>Fibre Channel Connectivity Agent</i>	Fibre Channel storage area networks (SANs)	<i>Plan for Fibre Channel Connectivity (FCC) Agent on page 70</i>
<i>Integration Gateway</i>	N/A—Allows management applications to communicate with ControlCenter	<i>Plan for the Integration Gateway on page 57</i>
<i>Host Agents for AIX, HP-UX, Linux, Solaris</i>	Hosts running AIX, HP-UX, Linux, and Solaris operating systems	<i>Plan for AIX, HP-UX, Linux, and Solaris Host Agents on page 76</i>
<i>Host Agent for Novell</i>	Novell Netware servers	<i>Plan for Host Agent for Novell on page 77</i>
<i>Host Agent for Windows</i>	Hosts running the Windows operating system	<i>Plan for Host Agent for Windows on page 78</i>
<i>Storage Agent for Centera</i>	EMC Centera storage arrays	<i>Plan for Storage Agent for Centera on page 81</i>
<i>Storage Agent for CLARiiON</i>	EMC CLARiiON subsystems and components	<i>Plan for Storage Agent for CLARiiON on page 82</i>
<i>Storage Agent for ESS</i>	IBM Enterprise Storage System (ESS) disk arrays	<i>Plan for Storage Agent for ESS on page 81</i>
<i>Storage Agent for HDS</i>	Hitachi Lightning, Hitachi Thunder, Hewlett-Packard XP series, or Sun StoreEdge 99x0 subsystems	<i>Plan for Storage Agent for HDS on page 83</i>
<i>Storage Agent for HP StorageWorks</i>	HP StorageWorks HSG80 (EMA) arrays	<i>Plan for Storage Agent for HP StorageWorks on page 85</i>
<i>Storage Agent for Invista</i>	EMC Invista TM	<i>Plan for Storage Agent for Invista on page 93</i>
<i>Storage Agent for NAS</i>	Celerra Network Server and Network Appliance Filer	<i>Plan for Storage Agent for NAS on page 86</i>
<i>Storage Agent for SMI</i>	SMI-enabled arrays not discovered by other agents	<i>Plan for Storage Agent for SMI on page 91</i>
<i>Storage Agent for Symmetrix</i>	EMC Symmetrix systems	<i>Plan for Storage Agent for Symmetrix on page 92</i>
<i>Workload Analyzer Archiver</i>	N/A—Processes and stores performance data from all agents	<i>Plan for Workload Analyzer Archiver on page 58</i>

Example Data Center

To help with agent planning, our example data center creates a spreadsheet containing a list of hosts. They will use the Table 10 to help distribute agent processing across available hosts.

Table 10 Agent Planning Data Center Example

Host Name	IP Address	Host OS	Master Agent	Storage Agents	Connectivity Agents	Host Agents	Mapping Agent	Oracle Agent	Common Agents	Backup Agents	Solutions Enabler
cawti	168.159.90.60	Windows									
l82ar12	172.23.172.123	Windows									
l82ar15	172.23.172.154	Linux									
pshcd1	10.15.64.23	Solaris									

12.2 Understand basic agent requirements

The following are basic requirements for all ControlCenter application agents:

- ◆ Each host where ControlCenter agents reside also requires a *Master Agent*, which requires proper privileges. Refer to *Log on with the proper privileges* on page 192.
- ◆ The C shell (csh) must reside on all agent hosts that run UNIX.
- ◆ Agents can reside:
 - On the same host as the objects to be managed.
 - On a host that is accessible to the agent host, storage array, etc. containing the objects to be managed.
- ◆ For information about disk space requirements for agents, refer to *EMC ControlCenter Support Matrix* on Powerlink.
- ◆ You can deploy multiple agents on a single host. In some cases, you might have to make configuration changes so agents running on the same host can communicate effectively. For example, if Storage Agent for NAS and Fibre Channel Connectivity Agent are

installed on the same host, configure one of those agents to use a port other than 162 to listen for SNMP traps. Refer to *Plan for Fibre Channel Connectivity (FCC) Agent* on page 70 or *Plan for Storage Agent for NAS* on page 86 for details.

- ◆ The impact of an agent on host resources depends on its type, polling frequency, and the number of agents installed. Agents that collect information more frequently have a greater impact on CPU utilization and memory usage.
- ◆ With the exception of Database Agent for Oracle running on AIX, which is supported only for 32-bit architecture hosts, ControlCenter agents can run on hosts with 32-bit or 64-bit architectures. Refer to *EMC ControlCenter Support Matrix* on Powerlink for supported versions.

There is no significant performance advantage to running an agent on a 64-bit architecture host versus running on a 32-bit architecture host.

- ◆ To reduce the amount of memory used by a ControlCenter agent (except for Storage Agent for Symmetrix) running on an HP-UX host, set the following environment variable from the command line:

```
export _M_ARENA_OPTS=1:2
```

Performance and Scalability Guidelines: Gatekeepers

Follow these minimum gatekeeper recommendations.

For each Symmetrix array connected to a host:

- ◆ Two gatekeepers are required when the Storage Agent for Symmetrix is installed on the host, and two (total of four) additional gatekeepers are required when you use Symmetrix Configure commands to manage the Symmetrix system. Each Symmetrix system needs only two Symmetrix agents. The agents need to be installed on separate hosts. This is to provide for failover when the primary agent goes down for maintenance (or failure).
- ◆ Common Mapping Agent and host agents do not require a gatekeeper.

Note: SYMCLI scripts should not use gatekeepers assigned to ControlCenter; they should have their own.

Step 13 Plan for Master Agents

You must deploy the Master Agent on each host to be monitored by ControlCenter agents.

Plan for Master Agent deployment as follows:

- ◆ 13.1 *Understand the Master Agent deployment methods* below.
- ◆ 13.2 *Ensure the target host meets hardware and software requirements* on page 55.
- ◆ 13.3 *Enter information about Master Agent installation* on page 55.

13.1 Understand the Master Agent deployment methods

Depending on the target host operating system and the current state of Repository connectivity, use one of the following methods to deploy the Master Agent on each host where ControlCenter agents are to be installed:

- ◆ Local deployment on Windows using the ControlCenter installation wizard (refer to *Deploy the Master Agent on Windows (GUI)* on page 193).

EMC recommends using this method for Master Agent deployment when a target Windows host can communicate with the Repository host. Unlike the command-line methods listed next, when connected to the Repository, the Windows GUI can access data from previous installations and automatically utilize data that applies to the current installation. This can reduce the total number of questions asked during Master Agent deployment and help ensure accuracy of the installation data (because already verified data is reused, there is no need to re-enter it manually).
- ◆ Local deployment on Windows using the command line (refer to *Deploy the Master Agent on Windows (Command Line)* on page 195).

Use this method when a target Windows host does not have a graphics card that can support 256 color displays, or if you do not want to install the ControlCenter Install Tools on the target host.
- ◆ Local deployment on AIX, HP-UX, Linux, or Solaris with scripts, using the procedure in *Deploy the Master Agent on UNIX (Command Line)* on page 196.

Always use this method when deploying the Master Agent on UNIX hosts.

13.2 Ensure the target host meets hardware and software requirements

Ensure that the target hosts meet the hardware and software requirements shown in *EMC ControlCenter Support Matrix* on Powerlink.

Important: Before deploying the Master Agent on Linux, ensure that the C++ libraries on the target host are at a supported level (6.2-2 or below, for example `libstdc++-libc6.2-2.so`). If the libraries are above that level, ensure that the correct compatibility standard C++ runtime libraries are installed (check <http://www.rpmfind.net> for the `compat-libstdc++` package that is required for your Linux system).

13.3 Enter information about Master Agent installation

Enter information required for Master Agent deployment, using the field descriptions in Table 11 as a guide.

Table 11 Master Agent Installation Notes

Required Field	Description
<i>Enter Master Agent port number</i>	The Master Agent listening port number. <i>Default: 5798</i>
The installation program does not display the following fields if the target host is running Windows and can connect with the Repository.	
<i>Enter ECC Server component name</i>	Hostname (recommended) or IP address of the host on which the ECC Server resides. This value must exactly match the value of <code>ECCSERVER_NAME</code> in the following file on the ECC Server host: <code><Install_Root>/installIGS520.answers</code> where, <code><Install_Root></code> is the ECC infrastructure install directory. For example, the correct value in the following entry is <code>svrmyHost: ECCSERVER_NAME=svrmyHost</code> <i>Default: None.</i>

Table 11 Master Agent Installation Notes (continued)

Required Field	Description
<i>Enter ECC Server port number</i>	Listening port number for the ECC Server host. <i>Default: 5799</i>
The following field appears only when the ECC Server host is multihomed.	
<i>ECC Server network name for Master Agent communications</i>	Network interface at the ECC Server host that will receive Master Agent communications. If the target host is running Windows and can connect with the Repository, this field displays a drop-down list of available NICs. This value must exactly match the value of <code>ECCSERVER_NAME</code>, minus the <code>svr</code> prefix, in the following file on the ECC Server host: <code><Install_Root>/installIGS520.answers</code> where, <code><Install_Root></code> is the ECC infrastructure install directory. For example, the correct value in the following entry is <code>myHost</code>: <code>ECCSERVER_NAME=svrmyHost</code> <i>Default: None</i>

Example Data Center

In the host spreadsheet, the example data center enters X's in the Master Agent column for the four hosts where they plan to deploy other agents (which require the Master Agent for communication).

Table 12 Master Agent Data Center Example

Host Name	IP Address	Host OS	Master Agent	Storage Agents	Connectivity Agents	Host Agents	Mapping Agent	Oracle Agent	Common Agents	Backup Agents	Solutions Enabler
cawti	555.159.90.60	Windows	X								
l82ar12	555.23.172.123	Windows	X								
l82ar15	555.23.172.154	Linux	X								
pshcd1	55.15.64.23	Solaris	X								

Step 14 Plan for Common Agents

Deploy one or more of the ControlCenter *common agents* to allow other agents or operations, supported by that common agent, to function in the ControlCenter environment, using the following steps:

- ◆ 14.1 *Plan for the Integration Gateway* below.
- ◆ 14.2 *Plan for Workload Analyzer Archiver* on page 58.

14.1 Plan for the Integration Gateway

The Integration Gateway connects the ECC Server (refer to *Step 3: Know the ControlCenter Architecture* on page 8 for details) to management framework applications, enabling those applications to display ControlCenter information. The information is transmitted using SNMP. Two or more Integration Gateway instances can point to the same management framework application.

Table 13 Integration Gateway Quick Summary

Parameter	Description
License Keys	None are required. This agent is available with Open Integration Components (the ControlCenter base package).
Location	A Windows or Solaris host that is one of the following: The host where the ECC Server resides, the host running the management framework application, or any host that is accessible to the ControlCenter infrastructure components.
Number to Deploy	Only one agent is required for your entire ControlCenter configuration. You can deploy two or more agents for redundancy, but you would receive duplicate traps from each gateway. For certain network configurations, you can deploy one gateway on a private network to send traps to a different framework.
Prerequisites	Ensure that the target host is running Windows or Solaris. Refer to <i>EMC ControlCenter Support Matrix</i> on Powerlink for supported versions.

When deploying the Integration Gateway, plan to provide input for the following field, which will be requested by the agent administration wizard.

Table 14 Integration Gateway Deployment Field

Required Field	Description
<i>IP address of the Enterprise Management Framework</i>	The IP address of the host on which the Enterprise Management Framework is installed. <i>Default: None</i>

14.2 Plan for Workload Analyzer Archiver

Workload Analyzer Archiver processes and stores data collected by ControlCenter agents. Performance Manager (refer to *Step 40: Install Performance Manager (Optional)* on page 177) can generate views of that data, which describe system performance and configuration.

Table 15 Workload Analyzer Archiver Quick Summary

Parameter	Description
Managed Objects	All managed objects for which Archiver data is to be collected, based on Workload Analyzer Archiver data collection policies (refer to <i>EMC ControlCenter 5.2 Administration/User Guide</i> for details about data collection policies).
License Keys	This agent is available with a Performance Manager license key. Refer to <i>Step 37: License the Desired Applications</i> on page 171 for details on entering license keys.
Location	You can deploy this agent on the host where the ECC Server resides, or any host that is accessible to the ControlCenter infrastructure components. In a distributed configuration, you can deploy this agent on a host where a Store resides. When you deploy this agent on a host where ControlCenter infrastructure components reside, keep in mind that the performance and scalability of the host, and the number of ControlCenter objects that can be effectively managed, is likely to be reduced.
Number to Deploy	Only one agent is required for full functionality. Consider adding more agents for performance and scalability (refer to <i>EMC ControlCenter 5.2 Performance and Scalability Guidelines</i> on Powerlink for details). When multiple agents are installed, ControlCenter assigns an archiver to each top-level managed object (for example, storage array, connectivity device, host, etc.) based on estimated processing and space considerations. With the assistance of EMC CS Technical Support Group, you can change the allocation of managed object data to specific Archivers. Contact CS Technical Support Group using a Service Alert for details.
Prerequisites	Ensure that the target host is running the Windows operating system. Refer to <i>EMC ControlCenter Support Matrix</i> on Powerlink for supported versions.

When installing the agent, plan to provide the following information.

Table 16 Workload Analyzer Archiver Deployment Field

Required Field	Description
<i>Archive path</i>	Directory on the target host where the Workload Analyzer Archiver archives will reside. Ensure that enough disk space is available to support a growing archive. If you specify the same directory for <i>Report path</i> (described below), the Archiver writes the archives to an archive subdirectory under the directory specified in this field. EMC recommends that you do not specify the ENW520 directory where the Archiver source files reside. <i>Default:</i> None. <i>Example:</i> C:\ecc\WLAArchives
<i>Report path</i>	Directory on the target host where the Workload Analyzer Archiver reports will reside. If you specify the same directory for <i>Archive path</i> (described above), the Archiver writes the reports to an reports subdirectory under the directory specified in this field. EMC recommends that you do not specify the ENW520 directory where the Archiver source files reside. <i>Default:</i> None. <i>Example:</i> C:\ecc\WLAArchives
<i>Time (in minutes) to wait after midnight before closing daily files</i>	Files containing Workload Analyzer Archiver data automatically close at the end of each day. If Workload Analyzer Archiver stops sending data, this setting ensures that files are closed at the specified time after midnight in the collecting agent's time zone. <i>Default:</i> 90 minutes
<i>Time (in minutes) to wait before closing revolving files</i>	Amount of time <i>after</i> the last receipt of revolving collection data at which the files for collecting that data are closed, if the Archiver agent stops sending data for any reason. <i>Default:</i> 30 minutes
<i>Time (in minutes) to wait before closing analyst files</i>	Amount of time <i>after</i> the time designated to close analyst data collection files (defined in the WLA Analyst data collection policy—refer to <i>EMC ControlCenter 5.2 Administration/User Guide</i> for more information) at which the files for collecting that data are closed, if Workload Analyzer Archiver stops sending data for any reason. <i>Default:</i> 60 minutes
<i>IP Address</i>	IP address of the host system where Workload Analyzer Archiver is to reside. <i>Required only for a multihomed host.</i>
<i>Port</i>	Port number to provide Workload Analyzer Archiver access through a firewall. <i>Required only for firewall access.</i>

Performance and Scalability Guidelines:
Workload Analyzer Archiver

Limit the number of managed objects per Workload Analyzer Archiver.

When the number of managed objects exceeds the managed object counts listed in Table 17, consider adding one or more WLA Archiver Agents to sustain optimum performance. For example, one WLA Archiver can process up to a total count of 330 managed objects, before a second WLA Archiver needs to be added. These statistics are

based on an agent host with two CPUs (700 MHz to 1.0 GHz) and 1 GB of memory.

Table 17 **Managed Objects per WLA Archiver**

Managed Object Type (Medium-Sized Objects)	Managed Object Count
Storage arrays	50
Hosts	200
Databases	50
Switches	30

Step 15 Plan for Backup Agents

Backup agents monitor and manage the ControlCenter environment for backup systems.

This section contains the following steps.

- ◆ 15.1 *Plan for Backup Agent for EDM* below.
- ◆ 15.2 *Plan for Backup Agent for Legato NetWorker* on page 63.
- ◆ 15.3 *Plan for Backup Agent for TSM* on page 64.
- ◆ 15.4 *Plan for Backup Agent for VERITAS NetBackup* on page 65.

Example Data Center

The data center plans to monitor a VERITAS NetBackup Server through ControlCenter. The data center plans to deploy Backup Agent for VERITAS NetBackup on host `pshcd1` (which can communicate with the VERITAS NetBackup Server).

Table 18 BackupAgent Data Center Example

Host Name	IP Address	Host OS	Master Agent	Storage Agents	Connectivity Agents	Host Agents	Common Map Agent	Oracle Agent	Common Agents	Backup Agents	Solutions Enabler
cawti	555.159.90.60	Windows	X								
l82ar12	172.23.172.123	Windows	X								
l82ar15	172.23.172.154	Linux	X								
pshcd1	10.15.64.23	Solaris	X							V*	

* Indicates Backup Agent for VERITAS NetBackup.

15.1 Plan for Backup Agent for EDM

The Backup Agent for EDM enables you to monitor your EMC Data Manager (EDM) operations within ControlCenter and to explore the storage resources used by your EDM environment within StorageScope. The agent pro-actively monitors your EDM server, looking for backup performance and job failure issues that you define as significant and displaying alerts in the ControlCenter Console. Within StorageScope, the agent provides EDM server, client, data set,

schedule, and job details, including a report that provides detailed information about exceptions.

Table 19 Backup Agent for EDM Quick Summary

Parameter	Description
Monitored Objects	EMC EDM servers (only through StorageScope reports—discovery and monitoring through Console interfaces are not currently available).
License Keys	This agent is available with a StorageScope or ARM license key. Refer to <i>Step 37: License the Desired Applications</i> on page 171 for details on entering license keys.
Location	The Solaris host that is provided with your EDM hardware package.
Number to Install	One for each EMC Data Manager server.
Prerequisites	Ensure the following are true (refer to <i>EMC ControlCenter Support Matrix</i> on Powerlink for supported versions): • The target host is running the level of Solaris supported by EDM. • The target host has EMC Data Manager (EDM) is installed, configured, and running on the target host. Logging Prerequisites - The ControlCenter Backup Agent for EMC EDM does not rely on the population of any logs. Therefore it is not a consideration here as the agent utilizes the data from the EDM data stores. The agent issues CLI commands against the Backup server directly to collect job data. The agent does however use data from the <code>recoveries.log</code> file to fill in progress information and failure/success status for restore jobs. If that file doesn't exist, there will be no progress information for restore jobs, and all restore jobs will have a status of 'uncertain.'

When installing Backup Agent for EDM, plan to provide the following information.

Table 20 Backup Agent for EDM Deployment Field

Required Installation Field	Description
<i>Installation path for EDM</i>	The full installation path for EDM.

15.2 Plan for Backup Agent for Legato NetWorker

Backup Agent for Legato NetWorker® allows you to monitor your NetWorker operations and their associated storage resources using the ControlCenter Console. Install this agent only if you have Legato NetWorker servers in place at your installation.

Table 21 Backup Agent for Legato NetWorker Quick Summary

Parameter	Description
Managed Objects	Legato NetWorker servers.
License Keys	This agent is available with a StorageScope or ARM license key. Refer to <i>Step 37: License the Desired Applications</i> on page 171 for details on entering license keys.
Location	The Legato NetWorker Server host.
Number to Deploy	One agent for your Legato NetWorker installation
Prerequisites	Ensure that Legato NetWorker Server 6.0 or higher is installed on the host, and that the host is running the AIX, HP-UX, Solaris, or Windows operating system (refer to <i>EMC ControlCenter Support Matrix</i> on Powerlink for supported operating system versions). Logging Prerequisites - The ControlCenter Backup Agent for Legato NetWorker uses the NetWorker Messages file for all information pertaining to backup jobs. As a result, this agent requires that logging is active on the NetWorker server and the message file is written to in its default location on the Backup Server.

When installing Backup Agent for Legato NetWorker, plan to provide the following information.

Table 22 Backup Agent for Legato NetWorker Deployment Field

Required Field	Description
<i>Backup Agent for Legato NetWorker installation path</i>	The full installation path for Legato NetWorker. <i>Windows default:</i> C:\Program Files\nsr <i>UNIX default:</i> /usr/nsr

15.3 Plan for Backup Agent for TSM

This agent monitors TSM backup systems, looking for defined events, such as failed backups and increasing space utilization. TSM is a storage management system that manages business information in an enterprise-wide SAN and traditional network environment.

In previous releases of ControlCenter, this agent supported active commands for volumes, storage pools, nodes, databases, and client options. In ControlCenter 5.2, active commands are no longer supported for this agent.

Table 23 Backup Agent for TSM Quick Summary

Parameter	Description
Managed Objects	Tivoli Storage Manager (TSM) servers.
License Keys	This agent is available with an ARM or StorageScope license key. Refer to <i>Step 37: License the Desired Applications</i> on page 171 for details on entering license keys.
Location	A host that can access the Tivoli Storage Manager server(s).
Number to Deploy	One agent for your Tivoli Storage Manager installation.
Prerequisites	Ensure that TSM and the TSM administrative client are installed on the target host (refer to <i>EMC ControlCenter Support Matrix</i> on Powerlink for version information). Ensure that all TSM servers have the same version level and all TSM server names are unique. Logging Prerequisites - The ControlCenter Backup Agent for IBM TSM uses the Backup Server's activity log file for all information pertaining to backup and restore jobs. As a result, this agent requires that logging is active on the Backup Server and the activity file is written to its default location. For TSM data collections to be successful, ensure all events are enabled for the activity log. To check this, type: q enabled actlog, and make sure the return is: All server events are ENABLED for the ACTLOG receiver. Additionally, use the query eventrules command to make sure that activity log receiver entries are not turned off for any Nodes. Refer to the TSM administration reference manual for details.
Additional Configuration	If you are running multiple TSM servers on a host, the servers that you did not specify in the ControlCenter deployment (where you can only specify one TSM server) can be added to ControlCenter management as follows. 1. In the ControlCenter Console tree panel, expand Hosts. 2. Right-click the desired host. Select Tivoli Storage Manager Agent, Setup, Add TSM Server. 3. In the Dynamic Server Definition dialog box, configure the TSM server you want ControlCenter to manage.

When deploying Backup Agent for Tivoli Storage Manager, the agent install wizard prompts for the values shown below.

Table 24 Backup Agent for TSM Deployment Field

Required Field	Description
<i>Tivoli Storage Manager administrator ID</i>	TSM user ID used by this agent to access TSM. EMC recommends using a default ID, created on the TSM server prior to starting the agent, with operator-level authority. When a higher authority level is required, users are prompted for a TSM login. <i>Default: admin</i>
<i>Tivoli Storage Manager administrator password</i>	Password associated with TSM administrator ID. <i>Default: password</i>
<i>TSM Server name in the TSM database</i>	TSM server name, as defined in the TSM database. Access the Tivoli Server Administration page in the TSM Web interface. At the top of the page, you see the server's name after the words "Connected to." <i>Default: ServerName</i>
<i>Tivoli Storage Manager server port (Windows only)</i>	Port that is used by the TSM server, listed as TCPPort in the <code>dsmsrvr.opt</code> file. <i>Default: 1500</i>
<i>TSM Service name in the Client Option File (dsm.sys) (AIX, HP-UX, or Solaris only)</i>	TSM server as defined in the client system option file (<code>dsm.sys</code>) that is used by the TSM Administration Client (<code>dsmaadm</code>). <i>Default: ServerName</i>

15.4 Plan for Backup Agent for VERITAS NetBackup

This agent allows you to monitor NetBackup operations and their storage resources. It provides shortcuts for most system management tasks and pro-actively monitors your NetBackup servers, looking for backup performance and job failure issues, and alerting you with detailed information so you can take corrective action. The platform-specific agents can help you manage servers and clients, backup jobs and processes, storage and media, and policies.

Table 25 Backup Agent for VERITAS NetBackup Quick Summary

Parameter	Description
Managed Objects	VERITAS NetBackup servers.
License Keys	This agent is available with an Automated Resource Manager (ARM) or StorageScope license key. Refer to <i>Step 37: License the Desired Applications</i> on page 171 for details.
Location	A host that can access the VERITAS NetBackup server(s).

Table 25 Backup Agent for VERITAS NetBackup Quick Summary (continued)

Parameter	Description
Number to Deploy	One instance for each VERITAS NetBackup server.
Prerequisites	Ensure that the target host has VERITAS NetBackup Server Version 3.4 or 4.5 (with NetBackup CLI) installed and configured, and that the host is running the AIX, HP-UX, Solaris, or Windows operating system (refer to <i>EMC ControlCenter Support Matrix</i> on Powerlink for supported versions). Logging Prerequisites - The ControlCenter Backup Agent for VERITAS NetBackup does not rely on the population of any logs. Therefore it is not a consideration here. The agent issues CLI commands against the Backup Server directly to collect job data.

When installing Backup Agent for VERITAS NetBackup, the agent install wizard prompts for the following values.

Table 26 Backup Agent for VERITAS NetBackup Deployment Field

Required Field	Description
<i>Backup Agent for VERITAS NetBackup installation path</i>	The installation path for Backup Agent for VERITAS NetBackup. <i>Windows default:</i> C:\Program Files\VERITAS\NetBackup <i>UNIX default:</i> /usr/openv/netbackup

Step 16 Plan for Common Mapping Agent

Common Mapping Agent allows you to discover and monitor (but not manage) databases and host configuration information locally on a single host or on remote hosts (via proxy). When operating on one host, CMA can look for databases and file systems on remote hosts, so only one CMA is required in place of individual agents for the desired databases and host systems (which can improve host performance and reduce overhead). Data collected by this agent is used in the Topology, Properties, and Relationship views (refer to *EMC ControlCenter 5.2 Administration/User Guide* for details) in the ControlCenter Console or Web Console.

The following features, which are available with host agents, are not supported with Common Mapping Agent.

- ◆ Issuing active commands
- ◆ Performing real-time explore
- ◆ Sending alerts
- ◆ Displaying host devices properties: Free size, tracks per cylinder, and sectors per track
- ◆ Displaying the following for VERITAS Volume Manager: VM disk count, maximum free space, utility state, VM Disks, and details about VERITAS sub-disks, plexes, etc.
- ◆ Displaying the following for HP-UX: Allocation state for logical volumes
- ◆ Windows: IDE Drive size
- ◆ Windows: In the ControlCenter Console Resource View, the parent and child relationship for PowerPath cannot be displayed
- ◆ Informix databases: The agent does not collect information about temporary tablespace data files (the Console displays the temporary tablespace names, but no data files)

Table 27 Common Mapping Agent Quick Summary

Parameter	Description
Managed Objects	◆ Windows, Solaris, Tru64, AIX, Linux, HP-UX, and Fujitsu-Siemens BS2000 hosts ◆ SQL7/SQL2000 databases on Windows hosts ◆ Sybase and Informix (32-bit) databases on AIX, HP-UX, and Solaris hosts ◆ DB2 databases on AIX hosts
License Keys	None required. This agent is available with Open Integration Components (the base package).

Table 27 Common Mapping Agent Quick Summary (continued)

Parameter	Description
Location	A Windows or Solaris host. The agent can detect and monitor databases on HP-UX and AIX hosts via proxy. The agent can detect and monitor file systems on AIX, HP-UX, Linux, and Tru64 hosts via proxy, and report information about logical volumes, storage devices, partitions, and volume groups. The agent can report information about logical volumes, storage devices, partitions, and volume groups for BS2000 hosts (but not file system information).
Number to Deploy	The minimum number needed to monitor the desired hosts and databases. If agent CPU utilization exceeds recommended levels on the agent host, consider adjusting the manner and frequency of data collection, or deploying more agents (refer to <i>Performance and Scalability Guidelines: Common Mapping Agent</i> on page 69 for details).
Prerequisites	Do the following before you deploy Common Mapping Agent (CMA). Refer to <i>EMC ControlCenter Support Matrix</i> on Powerlink for supported software versions. ◆ Deploy EMC Solutions Enabler 6.0.x on the target host (refer to <i>Plan for EMC Solutions Enabler</i> on page 97). When you deploy Solutions Enabler through ControlCenter, all required components are installed by default, and SYMAPI Server (which must be running for the agent to function properly) is started. If you deploy Solutions Enabler using a different method (necessary in a proxy setup when the Master Agent is <i>not</i> deployed on the target host), ensure SYMAPI Server is started. If Common Mapping Agent is to act as a proxy for remote hosts, Solutions Enabler is required on both the local and remote host(s). ◆ To monitor MS SQL, Sybase, Informix, or DB2 database instances, ensure the databases are running on the agent host (if CMA is installed locally) or on the proxy host (if CMA is acting as a proxy for one or more remote hosts). ◆ When CMA monitors two or more SQL Server instances on the same host, specify unique database username/password combinations for each instance. Otherwise, the agent uses default database instance information for all SQL Server instances. ◆ When discovering a Sybase database, this agent will not start on a UNIX host unless you add the Sybase executable file to the PATH and the location of the Sybase libraries to LD_LIBRARY_PATH, using the following procedure: 1. While logged on to the agent host as <code>root</code>, permanently set the following environment variables: <pre>export SYBASE=(SYBASE_HOME); PATH=\$PATH:\$SYBASE/ASE-12_5(or your ase directory)/bin; export SYBASE_OCS=OCS-12_5; export LD_LIBRARY_PATH=\$LD_LIBRARY_PATH:\$SYBASE/OCS-12_5 (or your OCS directory)/lib; export DSQUERY=SYBASE_INSTANCE_NAME</pre> 2. Stop this agent, the Master Agent, and SYMAPI Server. Then restart those components. 3. Using the ControlCenter Console, rediscover the Sybase database(s).

Table 27 Common Mapping Agent Quick Summary (continued)

Parameter	Description
Configuration	If you deployed Common Mapping Agent to run in proxy mode, to view the properties of a database or file system, apply a data collection policy to the database or host discovered via proxy. Ensure that the SYMAPI Server component of Solutions Enabler is running on any host where Common Mapping Agent is to collect information. Databases must be running and online to be detected. To discover SQL databases, SQL Server must be configured to use SQL Server and Windows authentication. SQL user authentication must be set to Windows Authentication. For all databases, the user ID supplied for discovery must have access to any database instance that you want to discover. A hostname collected via proxy by the Common Mapping Agent may not match the hostname collected by a host agent running locally on the same host due to a missing domain name. This issue can be resolved by the following: On a Windows host: Select My Computer, Properties, Network Identification, Properties, More and ensure that the field Primary DNS suffix of this computer shows the name of the domain in which that the host resides. On an UNIX host: Ensure that <code>/etc/resolv.conf</code> contains the fully-qualified hostname. In addition, ensure that the Common Mapping Agent's assisted discovery takes place after the host agents complete their automatic discovery so that the menu in the Assisted Discovery dialog box already includes all of the names of the discovered hosts.

Performance and Scalability Guidelines: Common Mapping Agent

Limit the number of managed objects per Common Mapping Agent

When the number of managed objects exceeds the managed object counts listed in Table 28 following, consider adding one or more Common Mapping Agents to sustain optimum performance. For example, one Common Mapping agent can manage up to a total count (100) before adding a second Common Mapping Agent. Discovery polling will be done in five off-peak hours. The Common Mapping Agent may coexist with other agents or Infrastructure components. The limitation is based on an agent host with two CPUs (700 MHz to 1.0 GHz) and 1 GB of memory.

Table 28 Managed Objects per Common Mapping Agent

Managed Object Type (Medium-Sized Objects)	Managed Object Count
Hosts: (Windows, Solaris, HP-UX, and AIX)	60
Databases (Sybase, Informix, and SQL Server)	40

Step 17 Plan for Connectivity Agents

These agents manage connectivity devices and fabrics in Storage Area Networks (SANs) and the VCM database on Symmetrix arrays.

- ◆ 17.1 *Plan for Fibre Channel Connectivity (FCC) Agent* below.
- ◆ 17.2 *Plan for Symmetrix SDM Agent* on page 73.

17.1 Plan for Fibre Channel Connectivity (FCC) Agent

This agent is required if you use a Fibre Channel SAN to connect hosts to storage arrays. This agent allows you to monitor the SAN, discover topology and fabric information for Fibre Channel switches, and manage information gathered by SNMP agents running on connectivity devices in the storage network.

Table 29 Fibre Channel Connectivity Agent Quick Summary

Parameter	Description
MOs	Connectivity devices and fabrics in fibre channel storage area networks
License Keys	This agent is available with a SAN Manager (full functionality), StorageScope (discovery and monitoring only), or Performance Manager (discovery and monitoring only) license.
Location	Deploy at least one FCC Agent on each subnet. You can deploy FCC Agent on the ECC Server host. When multiple subnets are managed by a single ECC Server but do not communicate, to manage connectivity devices in both subnets, run FCC Agent on at least one host in each subnet. When multiple FCC Agents run in the same subnet, if load balancing is disabled (see <i>Step 33: Configure Agent Load Balancing (Optional)</i> on page 154), the first agent to respond to discovery for a connectivity device becomes the primary agent and controller for that device. If the primary agent fails, failover to any available secondary FCC Agent occurs. Although different switches in the same fabric may be controlled by different FCC Agents, fabric zoning is managed through a single switch, and the primary FCC Agent for that switch thus becomes the primary FCC Agent for the fabric.
Number to Deploy	One agent, or more for redundancy or load balancing. You can deploy: • Multiple instances of FCC Agent managed by one ECC Server, but not more than 3 per subnet, and not more than one FCC agent per host (only one can be active at a time). • Up to four instances of FCC Agent per ECC Server (because one FCC Agent is required for each subnet, you can manage up to four subnets with one ECC Server).

Table 29 Fibre Channel Connectivity Agent Quick Summary (continued)

Parameter	Description
Number to Deploy	When multiple FCC agents are deployed, agent processing depends on how load balancing is configured (refer to <i>Step 33: Configure Agent Load Balancing (Optional)</i> on page 154). When load balancing is <i>disabled</i>, one agent acts as <i>primary</i> (runs data collection policies and user tasks) while the others wait to take over processing if the primary agent fails. When load balancing is <i>enabled</i>, up to two FCC agents can participate in load balancing when a configuration contains McDATA devices. If more than two FCC agents are deployed, the others wait to take over processing in failover situations. Consider the risk associated with switch contention by the two agents involved in load balancing. If no McDATA devices exist, all deployed FCC agents can participate in load balancing.
Prerequisites	Before deploying Fibre Channel Connectivity Agent: ◆ Enable SNMP v1 on all switches. ◆ By default, ControlCenter uses the default SNMP community string <code>public</code>. To enable connectivity device discovery for switches and service processors: - If necessary, change the ControlCenter community string to match the string for Brocade and McDATA switches and service processors. For Brocade switches, enter the command <code>snmpmibcapset</code>, and ensure that the FA Management Information Base (MIB) and the SW MIB are enabled. Refer to <i>EMC ControlCenter Support Matrix</i> on Powerlink for MIB and firmware versions required to support the first stage of connectivity device discovery. - Use the Cisco Command Line Interface to update all Cisco switches to specify the same community string (for example, one with write privileges, such as <code>private</code>). ◆ Ensure that FCC Agent has exclusive access to port 162 (the default), where it listens for SNMP traps from the devices it manages. If other processes (such as Storage Agent for NAS or Microsoft SNMP Trap Service) use port 162, they can prevent FCC agent from receiving traps and subsequently sending ControlCenter alerts. If necessary, you can change the Fibre Channel Connectivity Agent listening port—refer to <i>Controlling Port 162 Usage for SNMP</i> on page 310 for details. ◆ Refer to switch vendor documentation for details on configuring switch controller software for SNMP. For example, refer to <i>Connectrix Enterprise Storage Network System Planning Guide</i> (P/N 069001082) for information about configuring Connectrix agents and <i>Installing FibreZoneBridge and FibreZone CLI</i> on page 287 in this book for FibreZone information. Note: McDATA switches must support EMC FibreZoneBridge requirements. ◆ Enable the CNT Enterprise Manager API license key (required to perform a full discovery for CNT Enterprise Manager Version 3.2.1 and higher), which is provided without charge for using the CNT feature number 10-241 (any systems shipped from the factory include this model number). Systems shipping from the factory with version 4.1.2 and higher will always have the API enabled, and do not require feature code 10-241. You can enable the EM API License key by contacting McData support.

Table 29 Fibre Channel Connectivity Agent Quick Summary (continued)

Parameter	Description
Prerequisites	◆ Ensure that Fibre Channel connections to switches use the Source ID (SID) lockdown feature in SAN Manager to fix ports to specific World Wide Names (WWNs). This feature creates an association among the SID of a switch port, the host bus adapter (HBA) attached to the port, and the WWN of the HBA. This association is remembered, and attempts to <i>spoof</i> a WWN can be foiled. Spoofing a WWN occurs when an intruder is able to substitute an intruding host with the same WWN as a legitimate host. When spoofing occurs, the WWN changes the port it is on. SID lockdown prevents a WWN from changing ports, thus foiling most attempts to spoof. For more information on how to use the SID lockdown feature through ControlCenter, refer to the <i>EMC ControlCenter Console Online Help</i>. ◆ For a switch to be discovered and managed by Fibre Channel Connectivity agent, SNMP v1 must be enabled on the switch. ◆ To optionally enable collection of HDS statistics for Performance Manager, turn FCC Agent data collection policies “on” after deploying and starting FCC Agent.

Performance and Scalability Guidelines:
FCC Agent

Do not install more than four primary Fibre Channel Connectivity (FCC) Agents.

When multiple subnets are managed by ControlCenter but cannot communicate with each other, install at least one FCC Agent for each subnet. If subnets can communicate with each other, only one primary FCC Agent is required.

When multiple FCC Agents are deployed to manage one or more subnets, only one will act as primary (executing data collection policies and user tasks) and others will be candidates for failover.

ControlCenter can manage up to four stand-alone subnets and can support up to 4096 *total ports* (across all managed subnets). Any one subnet can contain up to 4096 ports and be managed by one primary and up to two failover agents.

If you need to manage more than 4096 ports across multiple subnets, contact Customer Support for assistance.

Enable FCC Agent WLA data collection policies (DCPs).

If you enable any FCC Agent WLA DCP, you will also get real-time statistics collection. For example, if any WLA DCP is enabled, then it is as if a Performance DCP is also running.

17.2 Plan for Symmetrix SDM Agent

Symmetrix SDM Agent monitors the VCM database for each Symmetrix array in your storage network, looking for configuration changes to volume access control.

Table 30 Symmetrix SDM Agent Quick Summary

Parameter	Description
Managed Objects	EMC Symmetrix systems.
License Keys	This agent is available with a SAN Manager, or StorageScope license key. Refer to <i>Step 37: License the Desired Applications</i> on page 171 for details.
Location	A host that is directly connected to a Symmetrix array. Can be installed on hosts with Fibre Channel connections to Symmetrix arrays. Usually installed on the same host as Storage Agent for Symmetrix. You can deploy this agent on the ECC Server host.
Number to Deploy	Typically depends on the number of Storage Agents for Symmetrix (refer to "Location" above for details).
Prerequisites	Before you deploy Symmetrix SDM Agent: ◆ A Fibre Channel connection must exist on the target host. ◆ Deploy EMC Solutions Enabler 6.0.x on each host through which a Symmetrix VCM database is to be monitored (usually, the host running the Symmetrix SDM Agent). Refer to <i>Plan for EMC Solutions Enabler</i> on page 97. ◆ Configure a connection to a VCM-enabled Symmetrix system on the target host. ◆ A Fibre Channel HBA must exist on the target host. EMC strongly recommends an HBA with the appropriate driver/firmware to support the Storage Networking Industry Association (SNIA) API (the agent will still communicate and offer SDM capabilities without an SNIA-qualified HBA). Refer to <i>EMC ControlCenter Support Matrix</i> on Powerlink for the specific drivers.
Configuration	After deploying Symmetrix SDM Agent, change the default discovery policy to run once daily.

For performance and scalability guidelines relating to Symmetrix SDM Agent, refer to *EMC ControlCenter 5.2 Performance and Scalability Guidelines* on Powerlink.

Step 18 Plan for Database Agent for Oracle

Database Agent for Oracle allows you to discover, monitor, and view configuration and allocation information for Oracle databases. You can also view real-time information about Oracle errors, initialization parameters, and user connection sessions. A single agent supports all the databases instances installed on the agent host (subject to scalability limitations) or any machines that can communicate with the agent host.

Table 31 Database Agent for Oracle Quick Summary

Parameter	Description
Managed Objects	Oracle databases that reside on the agent host or on remote hosts that can communicate with the agent host. Those databases can reside on <i>raw devices</i> (unformatted disks or disk partitions that applications can use to bypass the normal operating system procedures for writing and reading data to and from a disk).
License Keys	This agent is available with Open Integration Components, the ControlCenter base package (discovery and alerts only). Optionally enter a StorageScope or ARM license key to enable full functionality.
Location	Hosts that can access the Oracle databases to be monitored and managed. Do not install Database Agent for Oracle on the same host as the ControlCenter Repository. Do not deploy Database Agent for Oracle on hosts running 64-bit versions of AIX—the agent is supported only for 32-bit architecture hosts). Refer to E-Lab™ Navigator on Powerlink for supported versions.
Number to Deploy	You can deploy only one agent for all Oracle databases to be monitored and managed (if the agent host can communicate with all hosts where Oracle databases reside). The number of tablespaces Database Agent for Oracle can manage is partly influenced by whether Workload Analyzer is deployed and how frequently data collection policies run.
Prerequisites	If you plan to monitor Oracle databases on remote hosts: ◆ Deploy the Solutions Enabler client libraries, and ensure that Oracle or the Oracle Client is installed, on the host where Database Agent for Oracle is to reside (refer to <i>Step 21: Plan for EMC Solutions Enabler</i> on page 97 for details). ◆ Deploy Solutions Enabler on the remote hosts (refer to <i>Step 21: Plan for EMC Solutions Enabler</i> on page 97 for details) and ensure that the SYMAPI Server component of Solutions Enabler is running on those remote hosts. If you plan to monitor Oracle databases on local hosts: ◆ Deploy the Solutions Enabler client libraries, and ensure that Oracle or the Oracle Client is installed, on the local host where Database Agent for Oracle is to reside. ◆ Ensure that the SYMAPI Server component of Solutions Enabler is running on the local host. Database Agent for Oracle grants only select privileges on some SYS views and tables to Oracle Agent User. Review the access privileges in the <code>sys8.sql</code> file and object creation in the <code><ECC_HOME>/exec/EGO520/oraagent8.sql</code> script.

Table 31 Database Agent for Oracle Quick Summary (continued)

Parameter	Description
Configuration	Define and enable Database Agent for Oracle DCPs Data collection policies enable the Database Agent for Oracle to retrieve information about discovered Oracle database instances in specified intervals. You must define and enable the data collection policies yourself to begin collecting data with the agent. Collected data appears under the Database Instances folder in the tree panel of the main Console window. Refer to the “Database Agent for Oracle data collection policies” topic in the ControlCenter Console Online Help for details. Change the tablespace for Database Agent for Oracle (optional) By default, Database Agent for Oracle control data is stored in the USERS tablespace of each database that it monitors. Do the following to specify a different tablespace for that data: 1. Stop Database Agent for Oracle, using the ControlCenter Console. 2. Open the following file with a text editor: <code><Install_Root>\exec\EGO.ini</code>, where <code><Install_Root></code> is the ECC infrastructure install directory. 3. Update the following field to specify the new tablespace: Tablespace to store ECC Management info = MY_TSPACE 4. If the specified tablespace does not exist, the agent uses the SYSTEM tablespace. 5. Save and exit EGO.ini. 6. Restart Database Agent for Oracle. Manually run Database Agent for Oracle (optional) To manually run Database Agent for Oracle without providing sys password: 1. Locate ManualSetup.sql in <code><ECC_HOME>\exec\EGO520</code>. Replace all occurrences of OUSER with the username Database Agent for Oracle is to use for database connections. 2. If you would like ManualSetup.sql to create the user account, uncomment the appropriate lines beginning with CREATE USER and set the password and DEFAULT TABLESPACE for the user in ManualSetup.sql. Alternatively, you could logon to the oracle instance and manually create the user with another tool and leave the CREATE USER lines in ManualSetup.sql commented out. 3. Using SQLPLUS, connect as user sys and run ManualSetup.sql. Ignore the error while executing the drop table ecc_fet. At this point there should be a number of views created in the schema of the new user you created. 4. Start Database Agent for Oracle, using the Agent Administration Wizard in the ControlCenter Console. 5. Select Discover, Other, Database, Oracle Agent and provide the database connection information for Database Agent for Oracle. Provide a dummy SYS password (required). For Oracle Agent User Name, provide the database username and password you created in the first step of this procedure.

Step 19 Plan for Host Agents

These agents monitor and manage the host environment. They gather information about configuration, status, and performance data from the hosts on which they run, and might support control actions. You must deploy host agents to fully populate StorageScope reports and generate reliable data in those reports. If no host agents are deployed, some columns in StorageScope reports will be empty. If host agents run on some hosts but not others, some numbers in the reports will appear as the following string of question marks: ????

- ◆ 19.1 *Plan for AIX, HP-UX, Linux, and Solaris Host Agents* below.
- ◆ 19.2 *Plan for Host Agent for Novell* on page 77.
- ◆ 19.3 *Plan for Host Agent for Windows* on page 78.

19.1 Plan for AIX, HP-UX, Linux, and Solaris Host Agents

These agents allow you to monitor and manage hosts running the corresponding operating systems. They provide shortcuts for many system management tasks, and pro-actively monitor your systems, looking for storage issues that you define as significant, and alerting you with detailed information so you can take corrective action.

Table 32 Host Agents for AIX, HP-UX, Linux, and Solaris Quick Summary

Parameter	Description
Managed Objects	AIX, HP-UX, Linux, and Solaris hosts
License Keys	These agents are available with Open Integration Components, the ControlCenter base package (discovery and monitoring only). Optionally, enter a StorageScope or Automated Resource Manager (ARM) license key for full functionality.
Location	All UNIX hosts to be monitored through ControlCenter (for example, install Host Agent for Linux on every Linux host to be monitored through ControlCenter).
Number to Deploy	One agent on each UNIX host to be monitored and managed through ControlCenter.
Prerequisites	Optionally install the base VERITAS Volume Manager for all VERITAS functionality, and update the PATH environment variable for the agent superuser account to point to the VERITAS-installed commands. Each host must be running a supported version of the appropriate operating system (refer to <i>EMC ControlCenter Support Matrix</i> on Powerlink for version information). Before deploying Host Agent for Linux, ensure that the target host has SNIA libraries installed—this enables the agent to discover HBAs from all supported vendors.

19.2 Plan for Host Agent for Novell

This agent allows you to manage Novell NetWare 5.x and 6.x servers. In addition to providing shortcuts for many system management tasks, the agent pro-actively monitors your NetWare servers, looking for storage issues that you define as significant, and alerting you with detailed information so you can take corrective action. The agent can help you manage the following aspects of your Novell storage systems: NetWare 5.x and 6.x servers, volumes, directories, files, NetWare load modules (NLM), users, and user space restrictions.

Table 33 Host Agent for Novell Quick Summary

Parameter	Description
Managed Objects	Novell NetWare 5.x and 6.x servers.
License Keys	This agent is available with a StorageScope or Automated Resource Manager (ARM) license key. Refer to <i>Step 37: License the Desired Applications</i> on page 171 for details.
Location	A Windows host that can communicate with the Novell NetWare 5.x and 6.x servers to be monitored and managed.
Number to Deploy	One agent for each Novell NetWare 5.x and 6.x server to be managed.
Prerequisites	Before deploying this agent, ensure that the target host is running Windows (refer to <i>EMC ControlCenter Support Matrix</i> on Powerlink for supported versions) and the NetWare client, which has a dedicated login for this agent. In Novell, only one active, licensed login can be maintained per NDS tree for a given machine. Secondary user logins on the workstation will interfere with the agent operation.

When deploying Host Agent for Novell, you will be required to enter the following information.

Table 34 Host Agent for Novell Deployment Requirement

Novell Agent Install Field	Description
<i>NDS tree into which the agent will log</i>	NDS tree to which the NetWare servers to be monitored belong. The agent will log in to this NDS tree. <i>Default: acme_corp</i>
<i>NDS login context</i>	Context to use to log in to the NDS tree. <i>Default: roger . acme</i>
<i>Name or IP address of preferred NetWare server used during login</i>	Name or IP address of the NetWare server to log in to. <i>Default: None</i>
<i>NetWare user name</i>	NetWare username that the agent will use to log on. <i>Default: admin</i>
<i>Password</i>	NetWare password that the agent will use to log on. <i>Default: password</i>

19.3 Plan for Host Agent for Windows

This agent allows you to monitor and manage hosts running the Windows operating system. In addition to providing shortcuts for many system management tasks, this agent pro-actively monitors your systems, looking for storage issues that you define as significant, and alerting you with detailed information so you can take corrective action.

Table 35 Host Agent for Windows Quick Summary

Parameter	Description
Managed Objects	Hosts running the Windows operating system.
License Keys	This agent is available with Open Integration Components, the ControlCenter base package (discovery and monitoring only). Optionally enter a StorageScope or Automated Resource Manager (ARM) license key for full functionality.
Location	One instance on each Windows host to be managed. You can deploy Host Agent for Windows on a host where the ECC Server or one or more Stores are also installed.
Number to Deploy	Deploy one instance of this agent on each Windows host to be monitored and managed through ControlCenter.

Table 35 Host Agent for Windows Quick Summary (continued)

Parameter	Description
Prerequisites	Before installing Host Agent for Windows, ensure that the target host is running a supported version of Windows (refer to <i>EMC ControlCenter Support Matrix</i> on Powerlink for details). Also do the following: • Ensure that the target host has the Microsoft Windows Management Instrumentation (WMI) interface installed. The WMI core components (including <code>MOFComp.exe</code>) are a standard part of the Microsoft Windows 2000 and Windows Server 2003 operating systems. • To ensure that Host Agent for Windows can discover SNIA-qualified HBAs, ensure that the appropriate vendor-provided SNIA libraries are installed on the target host (the libraries might be installed with HBA device drivers or installed separately from those drivers). Verify that the mappings used by the SNIA common library find and load the vendor-specific libraries are in the <code>hkey_local_machine\software\snia\hba</code> key in the Windows Registry. • Optionally, has logical and physical disk counters enabled for performance monitoring functionality. While logged on as a member of the Administrators group, do the following: 1. Enter the <code>diskperf</code> command to see if the Logical and Physical Disk Performance counters are set to start when the system boots. 2. If the counters are not set to start, do one of the following: – If the system's physical drives are <i>nonstriped</i>, enter the command: <code>diskperf -y</code> – If the physical drives are <i>striped</i>, enter the command: <code>diskperf -ye</code> 3. Reboot the system to enable the counters.
Configuration	Configure log monitoring for Host Agent for Windows (optional) To configure Event Log Monitoring, which allows Host Agent for Windows to monitor the event log on the agent host: 1. In the tree panel, expand Hosts. 2. Right-click the host, and select Agents, Host Agent for Windows, Setup, Event Log Monitoring. 3. In the Event Log Monitoring dialog box, select or clear the checkboxes to enable or disable monitoring for the various event logs. 4. In the Retention Time dialog boxes, type for each event type how many hours worth of messages the agent should monitor.

Step 20 Plan for Storage Agents

This group of ControlCenter agents monitors and manages storage arrays. The agents can run on hosts that are connected to the storage arrays, or in the case of a proxy configuration, connected to other agents that have access to those arrays. The agents gather configuration, status, and performance data and might support control actions. Typically, storage agents run on hosts that are connected through SCSI or through a SAN to storage arrays. Follow these steps to plan for storage agents:

- ◆ 20.1 *Plan for Storage Agent for Centera* on page 81.
- ◆ 20.2 *Plan for Storage Agent for ESS* on page 81.
- ◆ 20.3 *Plan for Storage Agent for CLARiiON* on page 82.
- ◆ 20.4 *Plan for Storage Agent for HDS* on page 83.
- ◆ 20.5 *Plan for Storage Agent for HP StorageWorks* on page 85.
- ◆ 20.6 *Plan for Storage Agent for NAS* on page 86.
- ◆ 20.7 *Plan for Storage Agent for SMI* on page 91.
- ◆ 20.8 *Plan for Storage Agent for Symmetrix* on page 92.
- ◆ 20.9 *Plan for Storage Agent for Invista* on page 93
- ◆ 20.10 *Consider Using Proxy Agents* on page 95.

Our sample data center plans to deploy Storage Agent for CLARiiON on host `cawti` to monitor a CLARiiON FC4700, and Storage Agent for Symmetrix on host `l82ar12` to monitor a Symmetrix DMX 800.

Table 36 Storage Agent Data Center Example

Host Name	IP Address	Host OS	Master Agent	Storage Agents	Connectivity Agents	Host Agents	Mapping Agent	Oracle Agent	Common Agents	Backup Agents	Solutions Enabler
cawti	168.159.90.60	Windows	M	C ^a							
l82ar12	172.23.172.123	Windows	M	S ^b							
l82ar15	172.23.172.154	Linux	M								
pshcd1	10.15.64.23	Solaris	M							V ^c	

a. Indicates Storage Agent for CLARiiON.

b. Indicates Storage Agent for Symmetrix.

c. Indicates Backup Agent for VERITAS NetBackup.

20.1 Plan for Storage Agent for Centera

This agent communicates with EMC Centera arrays and allows you to view detailed information about each of the systems, such as system components, file systems, and volumes.

Table 37 Storage Agent for Centera Quick Summary

Parameter	Description
Managed Objects	EMC Centera storage arrays.
License Keys	This agent is available with a Centera license key. Refer to <i>Step 37: License the Desired Applications</i> on page 171 for details on entering license keys.
Location	A Windows host that can access the EMC Centera storage arrays to be monitored.
Number to Deploy	Deploy one agent to manage all your Centera arrays. If the agent generates high CPU utilization on the agent host, consider adding more agents for load balancing.
Prerequisites	Do the following before deploying this agent: • Ensure that the target host is running Windows (refer to <i>EMC ControlCenter Support Matrix</i> on Powerlink for supported versions). • Optional: For Centera Versions 2.2 and higher, to run Centera Viewer from the ControlCenter Console, install EMC Centera Viewer on hosts that are to run the Console (refer to <i>Step 35: Install the ControlCenter Console</i> on page 164 for details). To use Centera Viewer to monitor ControlCenter managed objects, set up a Centera Viewer profile with monitoring capabilities (if Storage Agent for Centera is using a profile—otherwise, ensure that anonymous has monitoring enabled). Refer to the Centera product documentation for details on Centera Viewer.

20.2 Plan for Storage Agent for ESS

This agent allows you to monitor IBM ESS (Shark) disk arrays, including disks, volumes, and cache activity. The agent monitors backup performance and job failure issues that you define as significant, and alerts you with detailed information so you can take corrective action. If a system error occurs, Storage Agent for ESS uses alerts to notify you of the problem, while the IBM ESS disk array places an automatic service call to IBM Technical Support (if you enable the *automatic call for service* feature—refer to your IBM ESS documentation for details).

Table 38 Storage Agent for ESS Quick Summary

Parameter	Description
Managed Objects	IBM ESS (Shark) disk arrays.

Table 38 Storage Agent for ESS Quick Summary (continued)

Parameter	Description
License Keys	This agent is available with a StorageScope license key. Refer to <i>Step 37: License the Desired Applications</i> on page 171 for details on entering license keys.
Location	A Windows host that can access IBM ESS (Shark) arrays over the network.
Number to Deploy	Deploy one agent to manage your IBM ESS (Shark) arrays. If the agent generates high CPU utilization on the agent host, consider adding more agents for load balancing—refer to <i>Step 33: Configure Agent Load Balancing (Optional)</i> on page 154 for details.
Prerequisites	Before installing this agent, ensure that the ESS CLI is installed on the target host. Before you can perform assisted discovery of IBM ESS arrays, you must set up user account access to the ESS Storage Specialist server.

20.3 Plan for Storage Agent for CLARiiON

This agent allows you to explore and monitor EMC CLARiiON subsystems and their components, such as storage processors, devices, and the registered hosts that are connected to those resources. Using the ControlCenter Console, you can manage CLARiiON storage groups and use SnapView™ on the FC4700 and CX series arrays to add, view, and manage snapshots.

Table 39 Storage Agent for CLARiiON Quick Summary

Parameter	Description
Managed Objects	EMC CLARiiON storage arrays.
License Keys	This agent is available with the following license keys: • Performance Manager or StorageScope (discovery and monitoring only) • SAN Manager (discovery, monitoring, and LUN masking) • CLARiiON (full functionality, except LUN masking) Refer to <i>Step 37: License the Desired Applications</i> on page 171 for details on entering license keys.
Location	For CLARiiON models FC4700 and higher (including the CX series), deploy this agent on any Windows, AIX, HP-UX, or Solaris host that can communicate with the CLARiiON array over the network (the FC4700 and higher models can be managed directly over IP through their storage processors). The target host must have Navisphere CLI installed. For models FC4500/5300, install this agent on any host that can communicate with a second network attached host that is directly connected to the array (the FC4500/5300 models cannot be managed directly over IP through their storage processors—they must be managed through another host that is directly connected to the array). Both the agent host and the second network-attached host must have Navisphere CLI installed. The second network-attached host must also have Navisphere host agent installed and running.

Table 39 Storage Agent for CLARiiON Quick Summary (continued)

Parameter	Description
Number to Deploy	The number of CLARiiON arrays that can be managed partly depends on if Workload Analyzer Archiver is running and the frequency of its data collection (as defined in Storage Agent for CLARiiON data collection policies). Begin by installing one agent to manage all your CLARiiON arrays. If the agent generates high CPU utilization on the agent host, consider adding more agents for load balancing—refer to <i>Step 33: Configure Agent Load Balancing (Optional)</i> on page 154 for details.
Prerequisites	Before deploying this agent: - To enable metaLUN support, ensure that Java Runtime Environment (JRE) 1.4.2_01 (required by NaviCLI) is installed on the target host. If the target host is running UNIX, ensure that the JRE location is in the PATH. Check the operating system vendor's website to ensure all patches that support JRE 1.4.2_01 are applied. MetaLUNs are not supported when the agent is deployed on the ControlCenter Repository host. - Ensure that the target host has Navisphere CLI is installed and enabled, and that CLARiiON unit serial numbers are set to Array in Navisphere. On UNIX hosts, you must manually add the Navisphere CLI installation directory to the PATH. - Ensure that the storage processor host has Navisphere SP Agent and Access Logix™ software installed and running. - If you use Navisphere for security, add SYSTEM@hostname (where <i>hostname</i> is the network name of the target host) to the list of privileged users. To access the privileged user list in Navisphere, right-click the storage processor icon and select Properties; then click the Agent tab. If you do not add SYSTEM@hostname to this list, ControlCenter commands that operate on the array will fail. - Enable statistics collection to allow viewing of performance data for CLARiiON arrays. In Navisphere, right-click CLARiiON Storage, then click General, then select the checkbox under Configuration to enable statistics collection. If you do not manually turn statistics collection ON, performance data will not be collected, and the following message will appear in the agent log: Statistics logging is not enabled on SPA on the array <array_id>.

20.4 Plan for Storage Agent for HDS

This agent allows you to monitor and explore supported Hitachi Lightning, Hewlett-Packard XP series, or Sun StoreEdge subsystems. You can also perform business continuance functionality on the subsystems. You can create, split, suspend, and resume BCVs for an HDS subsystem through the ControlCenter Console.

Table 40 Storage Agent for HDS Quick Summary

Parameter	Description
Managed Objects	Hitachi Lightning, Hewlett-Packard XP series, or Sun StoreEdge subsystems.

Table 40 Storage Agent for HDS Quick Summary

Parameter	Description
License Keys	This agent is available with a SAN Manager (full functionality) or StorageScope (discovery and monitoring only) license key. Refer to <i>Step 37: License the Desired Applications</i> on page 171 for details.
Location	A host that can communicate with the Hitachi Lightning, Hewlett-Packard XP series, or Sun StoreEdge subsystems. You can deploy this agent on the ECC Server host.
Number to Deploy	Deploy as many agents as needed to monitor the desired subsystems (for example, if one host can reach all subsystems, you could deploy one agent on that host).
Prerequisites	• If monitoring HP-XP subsystems, CommandView CLI must be installed on the target host and be able to communicate with the CommandView Server. Required HP-XP licenses must be entered on the CommandView Server. EMC highly recommends that you <i>do not</i> deploy the agent on the CommandView Server. • If monitoring Hitachi arrays, ensure that the target host can communicate with the HiCommand Device Manager Server. EMC highly recommends that you <i>do not</i> deploy the agent on the HiCommand Device Manager Server. • Optimally, you should deploy Storage Agent for HDS and HiCommand Tuning Manager (HTM) on the same host, which has a TCP/IP connection to the Hitachi Raid Agent host, which has an inband connection to Hitachi arrays. • If you intend to perform configuration changes using active commands on an XP512, ensure that LUN Security Manager XP and LUN Configuration Manager XP Licenses are installed. You must use assisted discovery with this agent (refer to <i>Step 50: Perform Assisted Discovery</i> on page 228 for details). To optionally enable collection of HDS statistics for Performance Manager: • Ensure that the target host can reach the HiCommand Tuning Manager (HTM) server and that HTM and its agents are installed and running on that server. • After deploying the agent, change the collection interval for the HTM RAID Agent from every <i>hour</i> (default) to every <i>minute</i> (using the HTM GUI). Ensure that the HDS Agent collection interval for revolving data is 5 minutes or greater. • After deploying Storage Agent for HDS, during assisted discovery of HDS arrays (refer to <i>Step 50: Perform Assisted Discovery</i> on page 228 for details), ensure that you enter the HTM server address and port correctly in the assisted discovery dialog boxes. • Install JDK/JRE V1.4.2 or higher and make it the default JRE for the host (refer to http://java.sun.com for details).

20.5 Plan for Storage Agent for HP StorageWorks

This agent monitors StorageWorks arrays and logs general information about StorageWorks subsystems and units. You can display information that this agent collects about subsystems, controllers, storagesets, remote copy sets, connections, units, and configured hosts. You can also disable or enable host access to a unit or set the offset for a connection.

Table 41 Storage Agent for HP StorageWorks Quick Summary

Parameter	Description
Managed Objects	HP StorageWorks arrays.
License Keys	This agent is available with the following license keys: ◆ StorageScope (full functionality, except LUN Masking). ◆ SAN Manager (discovery, monitoring, and LUN masking).
Location	The following configurations may be used: A host that is either physically connected to StorageWorks arrays and running the requisite API. A standalone host running the requisite API that is connected to HP StorageWorks arrays. You can install this agent on the ECC Server host. If you are using the StorageWorks Command Console Agent, you can connect over the network through that agent. If you have a SANworks Management Appliance or OpenView Management Appliance in your environment, you can connect to the HSG Element Manager Agent that is running on either of these appliances. When you connect to one of these products, you establish connections to all the StorageWorks subsystems to which these products are connected.
Number to Deploy	In general, deploy one agent to manage your StorageWorks arrays. If the agent generates high CPU utilization on the agent host, consider adding more agents.

Table 41 Storage Agent for HP StorageWorks Quick Summary (continued)

Parameter	Description
Prerequisites	Ensure that the agent host is running Windows (refer to the <i>EMC ControlCenter Support Matrix</i> on Powerlink for supported versions). Do the following to ensure that the host can access the StorageWorks Command Console Agent: 1. Run the Agent Configuration Utility (provided by HP) on the host running the StorageWorks Command Console Agent. 2. In the utility, add the name of the target agent host to the list of hosts allowed to access the StorageWorks Command Console Agent over the network. Specify <i>Configuration</i> as the Access Privilege for the newly added host. Configure the SANworks Management Appliance so Storage Agent for HP StorageWorks can access the HSG Element Manager Agent: 1. Start HSG Element Manager. 2. Select Options, Agent Options. The HSG Element Manager Agent Options panel appears. 3. In the Add Client row, for <i>Host Name</i>, enter the name of the host where Storage Agent for HP StorageWorks is to be installed. Select the Agent Config access level. Then click Submit. For Tru64 support, ensure that the array has HP Array Control software installed.

20.6 Plan for Storage Agent for NAS

This agent monitors and manages Celerra Network Server, which works with EMC Symmetrix and CLARiiON storage arrays, and Network Appliance Filer—both provide fast, scalable, high-capacity network storage. The agent collects Celerra and Network Appliance Filer device information as required by the NAS object model, and monitors those devices for alertable conditions.

Table 42 Storage Agent for NAS Quick Summary

Parameter	Description
Managed Objects	Celerra Network Servers and Network Appliance Filer servers.
License Keys	This agent is available with a Celerra Agent or StorageScope license key. Refer to <i>Step 37: License the Desired Applications</i> on page 171 for details on entering license keys.
Location	A host that can access NAS servers. You can deploy this agent on the ECC Server host.
Number to Deploy	One agent is typically sufficient for an entire ControlCenter configuration. Deploy more agents for scalability or failover.

Table 42 Storage Agent for NAS Quick Summary (continued)

Parameter	Description
Prerequisites	You must use assisted discovery with this agent (refer to <i>Step 50: Perform Assisted Discovery</i> on page 228 for details). Before deploying this agent: ◆ To discover Network Appliance systems, you must enable <code>rsh</code> on those systems, and ensure that the username/password specified in the Discovery Settings dialog box is a valid administrative user on those systems (to allow access through <code>rsh</code>). ◆ Ensure that this agent has exclusive access to port 162 (the default) where it listens for SNMP traps from the devices it manages. If other processes (such as Fibre Channel Connectivity Agent or Microsoft SNMP Trap Service) use port 162, they can prevent this agent from receiving traps and subsequently sending ControlCenter alerts. If necessary, you can change the Storage Agent for NAS listening port—refer to <i>Controlling Port 162 Usage for SNMP</i> on page 310 for details. Do the following when using this agent in a proxy setup: ◆ Ensure that Symmetrix serial numbers do not exceed nine digits. If a Celerra Network Server is attached to a Symmetrix array with a serial number that has more than nine digits, Symmetrix Fibre Channel information returned by the Celerra might be incorrect or not displayed. ◆ Ensure that, when Symmetrix or CLARiiON arrays are attached to a Celerra Network Server, disks are mapped from the storage array to the Celerra system and that disks are mapped to Symmetrix Fibre Channel ports and CLARiiON front-end ports. Otherwise ControlCenter will not display information for those ports (even if a physical connection exists between the array and the Celerra). ◆ Beware that when CLARiiON front-end port are discovered via proxy by this agent, information about those ports will not contain the WWN attribute.

Table 42 Storage Agent for NAS Quick Summary (continued)

Parameter	Description
Configuration	The <code>emcplink</code> utility allows you to specify security policies for secure shell (<code>ssh</code>) client authentication (required for Storage Agent for NAS to discover Celerra). The highest <code>ssh</code> security level (<i>full security</i>) requires that users manually run <code>emcplink</code> to provide a username/password for <code>ssh</code> authentication and manually accept an <code>ssh</code> key returned from <code>emcplink</code> to discover the Celerra. When accepted, the key is stored on the NAS Agent host for subsequent discoveries. If the key changes, to discover the Celerra again, the user must manually run <code>emcplink</code> again and accept the changed key. If your environment does not require full <code>ssh</code> security, you can use <code>emcplink</code> to set lower security levels that automatically accept new/changed keys without requiring manual entering of <code>ssh</code> usernames, passwords, and keys. To run <code>emcplink</code>, change to the <code><install_root>/exec/CNN520</code> directory on the host where Storage Agent for NAS resides, where <code><install_root></code> is the ECC infrastructure install directory. Then do one of the following: ◆ If your installation uses <code>ssh</code> version 2, update your agent configuration so <code>emcplink</code> uses <code>ssh</code> version 2 when handling <code>ssh</code> keys (the default is version 1). 1. Stop Storage Agent for NAS, using the ControlCenter Console. 2. Edit the following file: <code><install_root>/exec/CNN520/cnn.ini</code> 3. In <code>cnn.ini</code>, under <code>[ssh]</code> change <code>version = 1</code> to: <code>version = 2</code> 4. Save and exit <code>cnn.ini</code>. Restart Storage Agent for NAS. ◆ Enter the following command to add or remove an <code>ssh</code> security policy: <pre>emcplink -setpolicy [+ -]policy_name</pre> <i>Example:</i> <code>emcplink -setpolicy +EMC_SSH_KEY_SECURITY_FULL</code> In the command, specify <code>+</code> (add a policy) <i>or</i> <code>-</code> (remove a policy) immediately before <code>policy_name</code>, which is one of the following: • <code>EMC_SSH_KEY_SECURITY_FULL</code> (default)—Do not automatically accept any new or changed Celerra keys—they must be accepted manually, using <code>emcplink</code> (refer to <code>emcplink -interactive</code>). Provides the same functionality that <code>plink</code> (no longer valid) provided in previous ControlCenter versions, when manual username/password/key entry was required. • <code>EMC_SSH_KEY_SECURITY_ALLOW_NEW</code>—Accept new keys, but not changed keys. <code>ssh</code> authentication occurs automatically for initial discovery, and also for subsequent discoveries as long as the Celerra key does not change. If a key is changed, discovery is attempted via <code>telnet</code>. • <code>EMC_SSH_KEY_SECURITY_ALLOW_CHANGE</code>—Accept changed keys, but not new keys. When a Celerra is initially discovered, <code>ssh</code> authentication occurs manually. If the key is changed for subsequent discoveries of that Celerra, <code>ssh</code> authentication occurs automatically. • <code>EMC_SSH_KEY_SECURITY_NONE</code>—Accept both new and changed keys. <code>ssh</code> authentication occurs automatically at initial discovery and all subsequent discoveries, regardless of whether Celerra keys are changed.

Table 42 Storage Agent for NAS Quick Summary (continued)

Parameter	Description
Configuration (continued from previous page)	You can add more than one policy. EMC_SSH_KEY_SECURITY_ALLOW_CHANGE and EMC_SSH_KEY_SECURITY_ALLOW_NEW, for example, produce the same effect as EMC_SSH_KEY_SECURITY_NONE. If added policies contradict one another, the most recently added policy takes effect. If <code>ssh</code> is not enabled, Storage Agent for NAS uses non-secure access. - Manually enter <code>ssh</code> security information and accept/reject Celerra keys, if the current security policy is EMC_SSH_KEY_SECURITY_FULL (the default): <code>emcplink -ssh -interactive [-2] -pw <i>password</i> <i>username</i>@<i>ip_address</i></code> <i>Example:</i> <code>emcplink -ssh -interactive -2 -pw akz sshuser@127.127.127.127</code> where <i>password</i> and <i>username</i> are the login name/password for the user requiring <code>ssh</code> access and <i>ip_address</i> is the IP address of the NAS appliance, and <code>-2</code> optionally tells <code>emcplink</code> to use <code>ssh</code> version 2 (version 1 is the default). Note that <code>ssh</code> version 2 is not backward compatible with version 1 (<code>plink</code>, used in previous ControlCenter versions, used <code>ssh</code> version 1). If you switch to <code>ssh</code> version 2, you must run <code>emcplink</code> to discover again all Celerras previously discovered with <code>ssh</code> version 1. - If upgrading from a previous version of ControlCenter, upgrade existing <code>ssh</code> keys from the user account (used with the old <code>plink</code> program, which required the Master Agent to run as a system service) to the system account for use with <code>emcplink</code>: <code>emcplink -upgrade</code> Notes: If the <code>ssh</code> user has backup and restore privileges, Storage Agent for NAS performs <code>emcplink -upgrade</code> automatically. If <code>emcplink</code> displays the error message <i>Failed</i> when upgrading <code>ssh</code> keys from a current user account to a local machine account, the reason is one of the following: 1) The <code>ssh</code> directory is already created on the local machine account, or 2) The current user does not have backup and restore privileges for the upgrade to occur. Configure NetApp Filers to send traps to ControlCenter To send traps to the host that is running Storage Agent for NAS, enter: <code>snmp traphost add <IP_address></code> <i>Example:</i> <code>snmp traphost add 127.127.127.127</code> where <i>IP_address</i> is the IP address of the host running Storage Agent for NAS. To enter a user-defined trap, refer to the man pages for SNMP.

Table 42 Storage Agent for NAS Quick Summary (continued)

Parameter	Description
Configuration (continued)	Configure Celerra to send SNMP traps to ControlCenter Do the following to configure Celerra to send SNMP traps to ControlCenter: - If you <i>did not</i> configure Storage Agent for NAS to listen for SNMP traps on a port other than 162 (refer to <i>Changing the Storage Agent for NAS Listening Port</i> on page 311 for more information), add the following line to <code>/nas/site/trap.cfg</code> on the Celerra Network Server, where <i>ip_address</i> is the IP address of the host running Storage Agent for NAS: <pre>snmpmanager <ip_address>; communityname public</pre> <i>Example:</i> <code>snmpmanager 127.127.127.127; communityname public</code> - Enter the following command to check the events that are bound to sending traps from the Celerra: <pre>/nas/bin/nas_event -list -a trap</pre> - If an event is not in the list, edit <code>/nas/sys/nas_eventlog.cfg</code> to add an event, adding a line under the correct facility policy as follows, where <i>ID1</i> and <i>ID2</i> are event ID values: <pre>disposition range=<ID1>-<ID2>, trap "/nas/site/trap.cfg 2"</pre> - Load the changes to the <code>nas_eventlog.cfg</code> file: <pre>/nas/bin/nas_event -Load /nas/sys/nas_eventlog.cfg</pre> - Verify that the configuration file is loaded: <pre>/nas/bin/nas_event -Load -info</pre> - Verify the events are bound to traps: <pre>/nas/bin/nas_event -list -a trap</pre> - Run the following command to generate the trap: <pre>/nas/sbin/postevent -f 131 -s 1 -i 8 "fan 1 has failed"</pre> The command contains values from <code>/nas/sys/nas_eventlog.cfg</code>, where <code>-f</code> indicates the facility identifier (in this case, 131 identifies BoxMonitor), <code>-s</code> is the trap severity, <code>-i</code> is the event identifier (obtained from the <code>nas_event -1 -a trap</code>), and the phrase within quotes is a comment. All hosts configured in <code>/nas/site/trap.cfg</code> should receive the trap. - List all Celerra facilities that generate events: <pre>/nas/bin/nas_event -list -f -info</pre> - List all the events for a Celerra facility: <pre>nas_event -list -f <facility></pre> where <i>facility</i> is one of the facilities indicated using the <code>-list -f -info</code> command shown above, for example BoxMonitor. Refer to <i>Celerra File Server Reference Manual</i> for details on <code>nas_event</code>.

20.7 Plan for Storage Agent for SMI

This agent discovers and monitors SMI-enabled storage arrays that are not previously discovered by other ControlCenter agents. The agent gathers identifying properties and real-time data that applies to those storage arrays, and tracks configuration data for the arrays and their components.

Table 43 Storage Agent for SMI Quick Summary

Parameter	Description
Managed Objects	The following SMI-enabled storage arrays (if not previously discovered by other agents) and their listed components: ◆ Unknown arrays: Front-end adapters, front-end ports, and storage devices (logical devices) ◆ Symmetrix arrays: Fibre Channel directors, front-end ports, and logical devices ◆ HDS/Sun arrays: Fibre Channel ports, LDEVs, and controllers ◆ HP XP-series arrays: Front-end ports, LDEVs, and controllers ◆ CLARiiON arrays: Storage processors, front-end ports, and LUNs ◆ IBM ESS arrays: SCSI and ESCON ports, Fibre Channel and FICON ports, logical volumes (devices) ◆ Tape libraries
License Keys	This agent is available with Open Integration Components (OIC), the ControlCenter base package.
Location	A host that can access SMI-enabled arrays. You can deploy this agent on the ECC Server host.
Number to Deploy	In general, install one agent for all the subsystems to be managed. If CPU utilization on the agent host becomes high, consider installing additional agents.
Prerequisites	Ensure that the target host is running Windows (refer to <i>EMC ControlCenter Support Matrix</i> on Powerlink for supported versions) and has network connectivity to the SMI provider(s). When monitoring Symmetrix and CLARiiON arrays with Storage Agent for SMI, you must deploy EMC Solutions Enabler using the Solutions Enabler CDs (components of Solutions Enabler required for Storage Agent for SMI are not included when deploying Solutions Enabler through the ControlCenter Console). Refer to <i>Deploying Solutions Enabler</i> on page 213 for details.

20.8 Plan for Storage Agent for Symmetrix

This agent populates the Symmetrix data for ControlCenter. It gathers real-time data that applies to the Symmetrix array as a single unit, as well as to each component within the Symmetrix array. The agent tracks configuration and performance data for devices, ports, directors, physical drives, and Symmetrix arrays. The agent generates alerts relating to Symmetrix performance (based on threshold settings), overall system and individual component status, and error messages and alarms.

Table 44 Storage Agent for Symmetrix Quick Summary

Parameter	Description
Managed Objects	EMC Symmetrix arrays
License Keys	This agent is available with the following license keys: ◆ Discovery, monitoring only: Performance Manager, StorageScope, SAN Manager. ◆ Full functionality: Symmetrix Manager or Symmetrix Optimizer. Refer to <i>Step 37: License the Desired Applications</i> on page 171 for details.
Location	A host that can access Symmetrix arrays (either directly or through a Fibre Channel network). The agent can monitor all arrays to which the host is connected and can be used in proxy configurations. You can deploy this agent on the ECC Server host.
Number to Deploy	The number of Symmetrix arrays that this agent can manage mainly depends on whether Workload Analyzer Archiver is running and the frequency of data collection defined in Storage Agent for Symmetrix data collection policies.
Prerequisites	Before deploying Storage Agent for Symmetrix (refer to <i>EMC ControlCenter Support Matrix</i> on Powerlink for supported hardware and software versions): ◆ Ensure that the target host is running one of the following operating systems: Windows, Sun Solaris, HP-UX, or IBM AIX. ◆ Deploy EMC Solutions Enabler 6.0.x on each host through which a Symmetrix storage array is managed (usually, the host running the Storage Agent for Symmetrix). You can install Solutions Enabler 6.0.x locally (using the Solutions Enabler CDs) or through the ControlCenter Console. Before deploying Solutions Enabler 6.0.x, refer to <i>Plan for EMC Solutions Enabler</i> on page 97.

Table 44 Storage Agent for Symmetrix Quick Summary (continued)

Parameter	Description
Configuration	Configure the Proxy Discovery data collection policy so Storage Agent for Symmetrix can communicate in proxy mode: 1. In the ControlCenter Console tree panel, expand Administration, Data Collection Policies, Policy Templates, Storage Agent for Symmetrix. 2. Right-click Proxy Discovery. Select New. 3. In the Source tab, enter the Hostname, IP address, and port for the host with connections to Symmetrix arrays. 4. In the Apply To tab, select the host that is running Storage Agent for Symmetrix (which will act as proxy). Then click OK. 5. Other agents that can run in proxy mode do not require additional steps.

20.9 Plan for Storage Agent for Invista

The EMC Invista Agent runs on a server connected to an EMC Invista. The agent collects detailed information about the Invista which you can view through ControlCenter Properties views. It does not have any capabilities for configuring or managing an Invista instance. For those functions, use the Invista's native management software, which can be launched from within ControlCenter by right-clicking an Invista instance and selecting **Management Tools**.

For more information about EMC Invista configuration and management or other Invista Agents, refer to the *EMC Invista Administration Guide* (EMC P/N 300-001-907).

Table 45 Storage Agent for Invista Quick Summary

Parameter	Description
Managed Objects	EMC Invista
Prerequisites	Before deploying Storage Agent for Invista: ◆ The Master Agent has been installed on the host. ◆ Ensure that the target host is running a supported Windows operating system (refer to <i>EMC ControlCenter Support Matrix</i> on Powerlink for supported versions). ◆ The host is running the Invista CLI. ◆ The host is running a supported version of the Java JRE or SDK (with the path to the Java executable in the PATH environment variable). For information about operating systems that support the Invista Agent and required versions of the Java JRE, refer to the <i>EMC ControlCenter Support Matrix</i>.

Table 45 Storage Agent for Invista Quick Summary (continued)

Parameter	Description
License Keys	This agent is available with the following license keys: ◆ StorageScope ◆ SAN Manager Refer to <i>Step 37: License the Desired Applications</i> on page 171 for details.
Location	The agent uses the Invista CLI to communicate with the Invista. If the EMC Invista Agent has been installed on a host that does not have the Invista CLI installed in the default directory, you must edit the agent's initialization (INI) file to include the correct path to the Invista CLI installation directory. Alternatively, you can modify the location of the Invista CLI at the time of installation using the Agent Installation Wizard. If the Invista CLI has been installed in the default directory, there is no need to modify the Invista Agent INI file. To modify the EMC Invista Agent's initialization file: 1. Navigate to the directory where the EMC Invista Agent is installed. 2. Open the file <code>FGX.ini</code> in a text editor. 3. Under <code>[[Global Section]]</code>, locate the following line: <code>Invista CLI Location = PATH_TO_INVISTA_CLI</code> 4. Replace the text after the <code>=</code> with the path to the EMC Invista CLI installation directory. The default installation path is <code>C:\Program Files\EMC\INVCLI</code> 5. Save the <code>FGX.ini</code> file.
Configuration	Once it has been installed, there is no further need to configure the EMC Invista Agent.

20.10 Consider Using Proxy Agents

Proxy agents can communicate with other hosts that have connectivity to resources to be monitored by agent hosts. Table 46 lists required software for enabling proxy agents.

Table 46 Interface Software for Proxy Agents

Agent	Required Interface Software
<i>Common Mapping Agent</i>	EMC Solutions Enabler is required on the agent and remote hosts (refer to <i>Step 16: Plan for Common Mapping Agent</i> on page 67 for details).
<i>Database Agent for Oracle</i>	EMC Solutions Enabler client libraries are required on the agent host. EMC Solutions Enabler is required on remote hosts (refer to <i>Step 18: Plan for Database Agent for Oracle</i> on page 74 for details).
<i>Storage Agent for CLARiiON</i>	Navisphere Agent on storage processor (for CLARiiON models FC4500/5300 only, which must be managed through a second host that is connected to the array—Navisphere Agent is required on the second host). Refer to <i>Plan for Storage Agent for CLARiiON</i> on page 82 for details.
<i>Storage Agent for HP StorageWorks</i>	Command Console Agent for StorageWorks Command Console, installed on a host that is connected to one or more HP StorageWorks arrays (refer to <i>Plan for Storage Agent for HP StorageWorks</i> on page 85 for details).
<i>Storage Agent for Symmetrix</i>	SYMAPI Server component of EMC Solutions Enabler (refer to <i>Step 21: Plan for EMC Solutions Enabler</i> on page 97 for details).

Figure 11 shows Storage Agent for Symmetrix on a host that is connected to a proxy host running OS/390 and Solutions Enabler, which is in turn connected to a Symmetrix array.

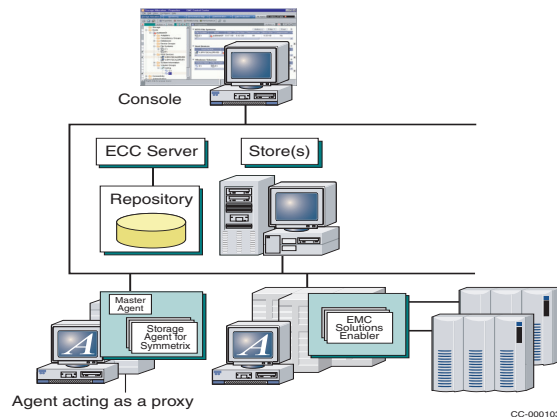


Figure 11 Storage Agent for Symmetrix in a Proxy Configuration

Performance and Scalability Guidelines: Symmetrix Proxy

Know the scalability limit for Symmetrix proxy.

Manage no more than 12 medium-size Symmetrix arrays (refer to Table u on page 5 for managed object sizes) with default polling policies except for WLA Revolving. A single Symmetrix agent can proxy up to four Solution Enabler instances on different hosts each managing up to three medium Symmetrix systems. The recommended dedicated hardware configuration is two 1 GHz processors with 1.5 GB of RAM.

Table 47 lists the recommended WLA Revolving policy schedules for Storage Agent for Symmetrix in proxy mode.

Table 47 Suggested WLA Revolving Policy for Proxy Symmetrix Agent

Number of Devices	Polling Interval
1-4000	2 Minutes (default)
4001-8000	5 Minutes
8001-16000	10 Minutes
16001- 24000	15 Minutes

Step 21 Plan for EMC Solutions Enabler

EMC Solutions Enabler is required software for the following ControlCenter agents:

- ◆ Common Mapping Agent
- ◆ Database Agent for Oracle (if you want to discover and manage databases on remote hosts)
- ◆ Storage Agent for Symmetrix
- ◆ Storage Agent for SMI (if you are using the agent to discover Symmetrix or CLARiiON arrays)
- ◆ Symmetrix SDM Agent

Plan to use one of the following methods to deploy Solutions Enabler on hosts where the listed agents are to be installed (and the required conditions exist for installing the software):

- ◆ **ControlCenter Console deployment (Recommended):** Make Solutions Enabler remotely available on the ECC Server host, using the procedure in *Make Solutions Enabler available for remote deployment* on page 138. Then deploy Solutions Enabler using the ControlCenter Console Agent Administration Wizard (refer to *Using the Agent Administration Wizard* on page 210 for details). The Agent Administration Wizard tells you when Solutions Enabler is required on target hosts.

Upgrade note: If you are upgrading agents, you *must* make EMC Solutions Enabler available for installation on the ECC Server host (when running of the ECC Server upgrade program or anytime thereafter, by launching the Start ECC Install desktop icon on the ECC Server host). The Console administration wizard automatically includes Solutions Enabler when upgrading hosts with agents that require it. Refer to *EMC ControlCenter 5.2 Upgrade Guide* for details.

- ◆ **Local deployment using CDs (or a shared folder):** Deploy Solutions Enabler locally on each host that requires it, using the Solutions Enabler CDs. You can also copy the contents of the CDs to a shared folder, as described in *Step 27: Set Up Shared Folder Installation (Recommended)* on page 120, which simplifies the deployment process (you will not need to use the Solutions Enabler CDs at each required host). This procedure is required when deploying Storage Agent for SMI. Refer to *Deploying Solutions Enabler* on page 213 for details.

Plan for Security and Remote Access

In this section, you will consider available options for user authentication, and optionally plan to implement ControlCenter access through a firewall.

Important: Follow these steps before continuing to other sections of this book. Careful planning of the infrastructure can greatly simplify ControlCenter installation and ensure that the ControlCenter configuration is optimized for your installation.

- ◆ Step 22: Plan for User Authentication..... 100
- ◆ Step 23: Consider Services for Remote Access..... 105

Step 22 Plan for User Authentication

You must implement user security for ControlCenter using only *one* of the following two methods:

- ◆ *Windows Authentication*
- ◆ *Lightweight Directory Access Protocol (LDAP)*

This step includes information needed to plan for user authentication using one of the above methods.

Important: You must choose *either* LDAP *or* Windows security for ControlCenter (you cannot mix the two types of security). User authentication through *Windows Active Directory* is supported only with Windows authentication (not with LDAP).

Windows Authentication

ControlCenter users must first exist (or be created through Windows Administrative Tools) on the ECC Server host before they can be added to ControlCenter.

Initially, a single user account, `eccadmin`, must be created on the ECC Server host to access the ControlCenter Console. This user will have complete access rights to all ControlCenter objects including ControlCenter administrative rights, which allow the user to add new ControlCenter users and to set the permissions that govern a user's access rights within ControlCenter.

Your ControlCenter administrator can set up ControlCenter user access rights after ControlCenter is fully installed. Only one user account (`eccadmin`) must exist for installation—refer to *Step 25: Create the eccadmin Account* on page 114 for more information.

Refer to the *Managing ControlCenter Users* chapter in *EMC ControlCenter 5.2 Administration/User Guide* for details on creating Windows users on the ECC Server host and adding users to ControlCenter.

Lightweight Directory Access Protocol (LDAP)

LDAP is a protocol that provides access to directories and may be used to authenticate users through usernames and passwords. LDAP directories provide a hierarchical organization of entities that represent functions, groups, and users in an organization. A *distinguished name* (DN) identifies a user entry in the directory

hierarchy. A user can access a specific function if the user's distinguished name has the appropriate permissions.

ControlCenter administrators must work with LDAP server administrators to configure LDAP for ControlCenter user authentication. LDAP requires a secure network connection, using SSL or TLS protocols, because passwords are sent across the network.

22.1 Set up LDAP to work with ControlCenter

- a. Ensure that your LDAP server has a signed digital certificate that can identify the LDAP server to the ECC Server.
- b. To configure an LDAP connection over SSL or TLS, copy the LDAP server's digital certificate to a local working subdirectory that the ControlCenter LDAP configuration utility can access (for example, C:/TEMP). Each certificate must be in a file that is accessible to the ControlCenter LDAP configuration utility—the filenames will be used as input to the ECC Server installation (refer to *Step 30.4: Install the ECC Server* on page 135 for details).
- c. To configure backup LDAP servers that use separate self-signed LDAP server certificates, copy those certificates to the local working directory, following the instructions in the previous step.
- d. Ask the LDAP administrator for a *bind DN* for ControlCenter.

The ControlCenter DN must be allowed to search for a username attribute (UID).

A distinguished name (also known as a *bind DN*) uniquely identifies ControlCenter to the LDAP server. The bind DN is used in access control lists (ACLs), which control access to data within a specific directory. The ControlCenter DN must be allowed to search for a username attribute (UID).

To ensure that a bind DN is set up for ControlCenter, ask the LDAP administrator to create a new bind DN for ControlCenter or reassign an existing entry. For example:

```
cn=ControlCenter,ou=Applications,dc=emc,dc=com
```

Figure 12 on page 102 shows an example of part of an LDAP directory that contains subtrees for user data (OU=Users) and application data (OU=Applications).

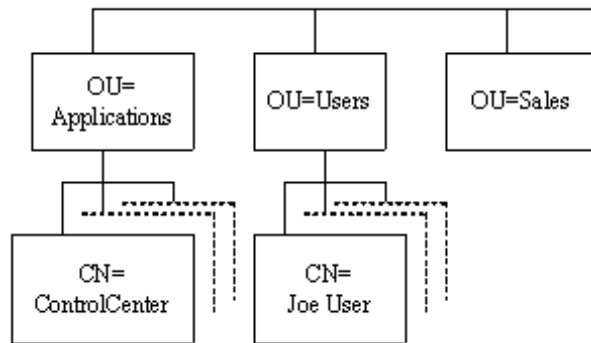


Figure 12 Example Cross-Section of an LDAP Directory

- Give ControlCenter access to the *username* and *user full name* attributes in the directory entry for the bind DN.
 - Provide the password for the bind DN, which will be obfuscated before it is stored on the ECC Server.
 - Provide the LDAP primary and backup server URLs (*ldaps://hostname:port*). The default port for LDAP over SSL is 636.
 - Provide the *search base DN* (the distinguished name where the username search will begin). For example, if all ControlCenter user entries fall under *ou=Users,dc=EMC,dc=COM*, the search DN should be *ou=Users,dc=EMC,dc=COM*.
 - The *username attribute* (the name of the directory attribute that specifies the ControlCenter user's logon ID, or *username*). Typically the attribute name is *UID*.
 - The *full name attribute*, which is typically specified by "cn" (commonName) or "freeFormName". Some directories only respond to the abbreviated attribute name.
- e. Be aware that if your LDAP implementation is *not* case-sensitive (case ignore string, or CIS), ControlCenter users must still provide user IDs and passwords that are case-sensitive (they are required by the ControlCenter interface).
- f. Ask the LDAP administrator to add user `eccadmin` to LDAP.

The `eccadmin` user has administrative access to ControlCenter and is required to log on to ControlCenter for the first time to add users and create and edit user groups and authorization rules.

- g. Plan to enter the information for LDAP installation listed in Table 48. You will need the recorded values when you install the ECC Server using the installation wizard (refer to *Step 30.4: Install the ECC Server* on page 135 for details).

Table 48 LDAP Installation Notes

Field	Description
<i>LDAP Directory URL</i>	The LDAP directory URL, written as: <code>ldaps://hostname:port</code> The host entry must match the host entry in the LDAP Server's certificate Common Name field and be a valid hostname, usually the fully qualified hostname. The default port for LDAP over SSL is 636; but your site may have assigned a different port.
<i>Bind Name</i>	The distinguished name (DN) of the entry in the Directory Information Tree (DIT) that identifies an application. This DN is used in ACLs, which control access to data within the directory. The DN entry must be granted access to the username and user full name attributes within the directory entries. ControlCenter must bind to the LDAP server as this application. For example: <code>cn=ControlCenter,ou=Applications,dc=emc,dc=com</code> Your LDAP administrator may need to create a separate entry for ControlCenter or assign an existing entry for ControlCenter to use.
<i>Bind Password</i>	You will need to know the BIND credentials (password) for the BIND DN. This is required to bind to the directory. ControlCenter supports simple username (bind DN) and password authentication. The password for the LDAP bind will be obfuscated before being stored on the ControlCenter server. You may want to commit this to memory.
<i>Start for User Search</i>	The search base is the distinguished name of the point in the directory hierarchy from which the search for a username should start. This is wholly dependent upon the design of the directory. For example: directory, all user entries come under <code>ou=Users,dc=EMC,dc=COM</code> . The search DN would be <code>ou=Users,dc=EMC,dc=COM</code> . If user entries were distributed throughout the directory by organizational unit (ou), then the search start DN would be <code>dc=EMC,dc=com</code> .
<i>Attribute Name for User's Logon Id</i>	The username attribute is the name of the directory attribute whose value is the ControlCenter user's logon ID, commonly called a username. Typically, the attribute name is "UID". ControlCenter will search the directory for an instance of this attribute whose value is the username specified by a ControlCenter user at logon time.
<i>Enter Password for LDAP User</i>	The password assigned to the LDAP <code>eccadmin</code> account.
<i>Attribute Name for User's Full Name</i>	User directory entries usually carry the full name of the user in addition to their username. The attribute used to hold this information is typically <code>cn</code> (commonName) or "freeFormName." Some directories only respond to the abbreviated attribute name. If you have entered "commonName" and get nothing returned, try <code>cn</code> .

Table 48 LDAP Installation Notes (continued)

Field	Description
<i>LDAP Backup Directories</i>	ControlCenter may be configured to use one or more backup copies as a fallback if the primary directory is unavailable. Backup directories must have the same hierarchy and data as the primary directory. This is the LDAP directory that owns the directory data and through which all updates to the directory must pass before being replicated to backup directories. The directory configured to ControlCenter as its primary LDAP directory may well be a backup copy of the primary LDAP directory. If there is more than one backup directory, the directories will be searched in the order that they are specified to ControlCenter. Each backup directory must be configured as a URL, and once again, the hostname must match the Common Name field of the LDAP Server's certificate.
<i>Location of the Certificate File(s)</i>	If your LDAP server certificates are signed by a third party or in-house Certificate Authority, then you will need to obtain a copy of that CA certificate. If the LDAP server has its own self-signed certificate, you will need a copy of the primary LDAP server's certificate as well as one for each of your backup LDAP servers. Certificates must be in one or more files available to the ControlCenter LDAP Configuration utility.

22.2 Configure ACLs for ControlCenter access

Ensure that the LDAP administrator provides read access for the ControlCenter DN to the UID (or equivalent) and Common Name (or equivalent) attributes in ACLs that manage access to LDAP entries.

22.3 Enable or disable user authentication through LDAP

To enable or disable ControlCenter user authentication with LDAP:

- a. Stop the ECC Server and all Stores.
- b. On the ECC Server host, find the line that begins with [Authentication] in the following file (<install_root> is the root ControlCenter install directory and <hostname_or_IP> is the ECC Server host IP address or hostname).


```
<install_root>\ecc_inf\data\<hostname_or_IP>\data\ecc_server.ini
```
- c. Update the line below [Authentication] as follows.
 - To disable LDAP authentication:
Authentication type = standard
 - To enable LDAP authentication:
Authentication type = LDAP
- d. Save ecc_server.ini and exit the file. Restart the ECC Server and Stores.

Step 23 Consider Services for Remote Access

If your storage networks are segmented with firewalls, or if high latency exists between ControlCenter components and products, you can provide access to ControlCenter interfaces through one or more of the following (described in this section):

- ◆ *Terminal Services* below.
- ◆ *Citrix Server* on page 106.
- ◆ *VNC (Virtual Network Computing)* on page 107.
- ◆ *Port Configuration* on page 107.

If users are to access the ControlCenter Console or Performance Manager through network resources that perform network address translation (NAT) such as firewalls or routers, the ControlCenter configuration requires Terminal Services (Console only), Citrix, or VNC.

Terminal Services

When the ControlCenter Console is installed on a server that is running Terminal Services, the Console application is transmitted over the network and displayed on a Terminal Services client host.

When running Terminal Services on a host where ControlCenter infrastructure components (ECC Server, Repository, and Store) reside, bear the following in mind:

- ◆ You cannot install or upgrade ControlCenter nor deploy ControlCenter hotfixes from a Terminal Services session.
- ◆ You cannot use Terminal Services to access the ControlCenter Console on infrastructure hosts (because the Console sessions might impact the performance of infrastructure components).
- ◆ Run the Console at least once on the Terminal Services server before running it remotely through Terminal Services (required to populate directories that are required for the Console to run).

Important: Be aware that some issues have been reported with installing or upgrading the ControlCenter Repository on Windows hosts that are configured with Terminal Services. EMC suggests that you disable Terminal Services (which requires a reboot) before installing or upgrading the Repository on hosts where Terminal Services is configured. You can restart Terminal Services after the install or upgrade is complete.

Depending on the operating system, refer to one of the following websites for information about installing Terminal Services:

<http://www.microsoft.com/windowsserver2003/technologies/terminalservices/default.msp>

<http://www.microsoft.com/windows2000/technologies/terminal/default.asp>

Important: Read *Preparing Citrix and Terminal Services Hosts for Console Access* on page 107 before accessing the Console through Terminal Services.

Citrix Server

Citrix Server is Windows server software that manages applications from a central location and allows users to access those applications from any approved location. Citrix Server allows you to access the ControlCenter Console and Performance Manager across firewalls that perform Network Address Translation (NAT) as well as those that don't perform that translation.

When the ControlCenter Console or Performance Manager are installed on a Citrix Server host, those applications can be transmitted over the network and displayed on a Citrix client host—users can then access those applications to perform runtime operations. For Performance Manager to run under Citrix, the Citrix MetaFrame server must have Citrix MetaFrame Service Pack 2 or later (available from <http://www.citrix.com>) installed.

Performance Manager and the ControlCenter Console must be running on a Citrix Server that is within the perimeter of the firewall. Users must access the ControlCenter Console from a host that resides outside the firewall.

Do the following to enable ControlCenter Console access through a Citrix Server:

1. Plan and deploy Citrix Server. Refer to the following website:

<http://www.citrix.com/site/PS/products/documents.asp?familyID=19&productID=186&featureID=DOC>

2. Install a Console on a host where the Citrix server resides. Refer to *Step 35: Install the ControlCenter Console* on page 164 for details.
3. Run the Console at least once on the Citrix server before running it remotely through Citrix (this is required to populate directories that are required for the Console to run).

Important: The only ControlCenter components that can be installed on the Citrix Server are the ControlCenter Console and Performance Manager. Be sure to read *Preparing Citrix and Terminal Services Hosts for Console Access* on page 107, before accessing the ControlCenter Console or Performance Manager through Citrix.

VNC (Virtual Network Computing)

VNC allows you to view and interact with one computer (the server) using a program (the viewer) on another computer anywhere on the Internet. You can perform ControlCenter installation, upgrade, and monitoring/management activities through VNC. You can download VNC from the RealVNC website (<http://www.realvnc.com>).

Port Configuration

The ECC Server requires certain ports to be accessible to the ControlCenter Console for communication through a firewall. For information about configuring openings in ControlCenter listening ports so ControlCenter communications can cross firewall boundaries, refer to *Port Usage and Firewall Configuration* on page 297..

Preparing Citrix and Terminal Services Hosts for Console Access

The default mode for running Terminal Services and Citrix is *execute*—for ControlCenter Console installation, the mode must be *install*. Do the following to change the mode to *install* before installing the ControlCenter Console on a host where Terminal Services or Citrix is configured.

1. Log on to the host as a member of the Administrators group.
2. In a command window, enter the following.
`change user /install`
3. Install the ControlCenter Console as described in *Step 35: Install the ControlCenter Console* on page 164.
4. After the Console install is complete, enter the following in a command window.
`change user /execute`
5. Enter the following command at any time to verify the current mode setting.
`change user /query`

**Performance and
Scalability Guidelines:
Terminal Emulation**

Use Citrix, Terminal Services, or VNC when latency between the Console and the Infrastructure exceeds 8 ms.

When latency between the ControlCenter Console and infrastructure components exceeds **8 ms**, consider using Citrix, Terminal Services, or VNC to access the Console.

Prepare to Install ControlCenter

This section describes how to install ControlCenter infrastructure components.

- ◆ Step 24: Prepare the Network and Hosts..... 110
- ◆ Step 25: Create the eccadmin Account..... 114
- ◆ Step 26: Install the Installation Tools on the Target Host 116
- ◆ Step 27: Set Up Shared Folder Installation (Recommended)..... 120

Step 24 Prepare the Network and Hosts

Prepare your local network for ControlCenter installation as follows:

- ◆ 24.1 *Ensure that DNS is set up correctly on this page.*
- ◆ 24.2 *Recommended: Specify hostnames instead of IP addresses on page 110.*
- ◆ 24.3 *Check network connectivity on this page.*
- ◆ 24.5 *Understand what network functions are not supported on page 112.*
- ◆ 24.6 *Prepare hosts for ControlCenter installation on page 112.*
- ◆ 24.7 *Ensure proper security for the Repository on page 113.*

24.1 Ensure that DNS is set up correctly

Verify that both forward and reverse DNS lookup is properly configured and active. If necessary, consult your network administrator or the DNS documentation.

24.2 Recommended: Specify hostnames instead of IP addresses

EMC strongly recommends specifying host network names instead of IP addresses during ControlCenter installation. By using this approach, when IP addresses change, you will not have to change the configuration of the ControlCenter infrastructure or agents.

24.3 Check network connectivity

Ensure that the ControlCenter infrastructure hosts have active connections to all network resources that ControlCenter is to monitor. Use the `ping` command to check connectivity between the infrastructure hosts and network resources.

For example, ensure that network adapters and switch ports have matching duplex levels and transfer speed settings. An example of a problem situation is, if network adapters on ControlCenter infrastructure hosts are set to *auto configure*, and switch ports are configured as *force 100*, communication might not be able to occur between the ControlCenter infrastructure and agent hosts that are connected via those switch ports.

24.4 Check network latency

Do the following to maintain network performance and minimize network latency.

- ◆ Plan to install ControlCenter infrastructure components on hosts within the same physical network switch.
- ◆ Ensure that latency between the infrastructure, agents, and Console interfaces conforms to the levels described in *EMC ControlCenter 5.2 Performance and Scalability Guidelines* on Powerlink. Use the `ping` command to check latency between hosts where ControlCenter components and products reside.
- ◆ If latency between ControlCenter components and products exceeds recommended levels, or users need to access ControlCenter through a firewall, consider using Terminal Services, Citrix, or VNC (refer to *Step 23: Consider Services for Remote Access* on page 105 for details).

Performance and Scalability Guidelines Networking

Minimize the effect of network latency on ControlCenter.

As network latency increases, so does execution time. In situations where latency is high, some ControlCenter operations may time out, especially for real-time actions. Do the following to reduce the effect of latency on a ControlCenter configuration:

- ◆ Ensure that latency between infrastructure components (ECC Server, Store, and Repository) is less than 8 ms (milliseconds). Try to keep infrastructure components on the same LAN segment.
- ◆ Ensure that latency between ControlCenter agents and infrastructure components does not exceed 200 ms. The minimum bandwidth is 386 Kb/s with 50 percent to 60 percent utilization.

Because data traffic between agents and the infrastructure is far less than between infrastructure components or between the Console and the infrastructure, agents can tolerate a higher latency.

- ◆ Ensure that latency between the Console and the infrastructure never exceeds 15 ms. Optimally, latency should be at 8 ms or less.
- ◆ If network latency exceeds 8 ms, use Citrix MetaFrame XP for Windows or Microsoft Terminal Services for the Console. The Console should not be accessed through Citrix or Terminal Services running on an infrastructure host. Using Citrix MetaFrame XP provides the following advantages.

- You can access the Console over a high-latency, low-bandwidth network.
- You can run the Console through a Network Address Translation (NAT) firewall; for example, on a virtual private network (VPN) over cable/DSL. Note that this only applies when the Console is accessed through Citrix MetaFrame XP.
- You are provided with an additional layer of security.

24.5 Understand what network functions are not supported

In general, VPN access is not supported for ControlCenter components. For example, you cannot install the ControlCenter Console on a remote host and then use it to communicate with ControlCenter infrastructure components across a VPN. However, you *can* access Consoles across a VPN using Terminal Services or Citrix (refer to *Step 23: Consider Services for Remote Access* on page 105 for details).

24.6 Prepare hosts for ControlCenter installation

Do the following to prepare hosts for ControlCenter installation.

- ◆ Ensure the following for hosts where infrastructure components (ECC Server, Repository, and Store) are to reside:
 - ❑ The *fully-qualified domain names* (FQDNs) and hostnames do not contain underscores.
 - ❑ The hosts do not have network interface cards (NICs) that are configured for DHCP.
 - ❑ No applications are currently running (to ensure that the ControlCenter installation wizard has adequate available memory to perform installation tasks).
- ◆ Ensure the following for the host where the ControlCenter Repository is to reside:
 - ❑ All Oracle software is removed.
Refer to <http://www.oracle.com> for details about removing Oracle products.
 - ❑ Terminal Services is not running (refer to *Terminal Services* on page 105 for details).
 - ❑ Disable antivirus software.

- ☐ Stop Distributed Transaction Coordinator service.
- ◆ Ensure the following for hosts where ControlCenter agents are to reside:
 - ☐ The hosts are able to connect to the ECC Server host during agent installation.
 - ☐ The hosts do not have NICs that are configured for DHCP.
- ◆ Ensure the following for *all* hosts where ControlCenter components and products are to reside:
 - ☐ All 3D screen savers are disabled.
 - ☐ You can log on to the host(s) as a member of the local Administrators group.

24.7 Ensure proper security for the Repository

The ControlCenter Repository is an Oracle database that is maintained by the Windows user group ORA_DBA. The database can be managed only by ControlCenter and authorized administrators, whose Repository actions should be restricted to:

- ◆ Moving Repository backup files to tape libraries (or other backup media at the installation).
- ◆ Adjusting schedules for performing Repository backups automatically.
- ◆ Running scripts to obtain the status of the Repository.

Oracle usernames are populated automatically in the Repository and cannot be changed. Do not delete or change the ORA_DBA user group. Do not attempt to update the content or structure of the Repository outside the scope of ControlCenter—doing so could impact ControlCenter operations and cause data to be lost.

For more information, refer to the *Oracle Installation Guide* (go to <http://www.oracle.com>, then follow the **database** link under Products, and click **documentation**).

Step 25 Create the eccadmin Account

To install and start the ECC Server, the `eccadmin` account must exist on the host where the ECC Server is to run, or as an LDAP user (refer to *Step 22: Plan for User Authentication* on page 100 for more information about LDAP). Follow the steps in this section to set up the `eccadmin` account using LDAP or Windows authentication.

Important: To install any ControlCenter components on a host, you must be logged in as a user that is part of the local Administrators group. If the `eccadmin` account does not exist on the ECC Server host, the installation wizard displays a dialog box that says the account must be created. Exit the installation wizard, create the account, then double click the **Start ECC Install** desktop icon to re-launch the installation wizard.

Using LDAP

If you are using LDAP for user authentication, ask the LDAP administrator to assign ControlCenter administrator access to the `eccadmin` account in the LDAP directory:

```
CN=ECC Administrator
UID=eccadmin
Password=a_really_secure_password
SN=NoneKnown
```

The `eccadmin` account must exist in LDAP prior to installing ControlCenter (refer to *Step 22: Plan for User Authentication* on page 100 for more information about LDAP).

Be aware that if your LDAP implementation is *not* case sensitive (case ignore string, or CIS), ControlCenter users must still provide userids and passwords that are case sensitive (they are required by the ControlCenter interface).

Using Windows

If you are using Windows for user authentication, create a user ID called `eccadmin`, using the following procedure:

1. Log in as a user that is part of the local Administrators group.
2. From the **Start** menu, select **Settings, Control Panel**.
3. From the Control Panel, open **Administrative Tools**, and then open **Computer Management**. The Computer Management dialog box appears.
4. From the tree, under **System Tools**, select **Local Users and Groups**.
5. Under **Local Users and Groups**, select **Users**.
6. From the **Action** menu, select **New User**. The New User dialog box appears.
7. In the **New User** dialog box, enter the following information:

User name: `eccadmin`

Full Name: `<Administrator name>`

Description: `<Administrator description>`

Password: `<password>`

Confirm Password: `<re-enter password>`



CAUTION

EMC strongly encourages the use of strong, unguessable passwords. Because `eccadmin` is authorized to perform many sensitive tasks, access to the `eccadmin` account, in the wrong hands, could damage your systems.

8. Clear the **User Must Change Password at Next Logon** checkbox.

EMC recommends that you select **Password Never Expires** for the `eccadmin` account. If you do not select this option and the password expires, the user will not be able to log in and will see the following error message:

User `<username>` authentication failed, your password has expired.

9. Click **Create** and then click **Close**.
10. Click **OK** to exit any open dialog boxes.

Step 26 Install the Installation Tools on the Target Host

The ControlCenter installation tools run on the target host to install ControlCenter components. Do the following to install the tools.

- ◆ 26.1 *Log on as a member of the Administrators group* on this page.
- ◆ 26.2 *Verify the Windows setup* on this page.
- ◆ 26.3 *Install the installation tools* on page 117.

Distributed infrastructure

Ensure that you install the installation tools (begin with ControlCenter installation CD #1, unless installing from a shared folder) on all hosts where ControlCenter components are to reside.

26.1 Log on as a member of the Administrators group

Ensure that you are logged on to the host with an account that is a member of the local Administrators group.

26.2 Verify the Windows setup

Do the following using Windows Services:

- ◆ Turn off antivirus software (if you do not do this, the installation might take much longer to complete).
- ◆ Stop the Distributed Transaction Coordinator Service.
From the Windows Start menu, select **Settings, Control Panel, Administrative Tools, Services**, and then right-click **Distributed Transaction Coordinator Service** and select **Stop**.
- ◆ If the target host is also where you intend to install the ControlCenter Repository, ensure that Terminal Services is not running on the host.

You can restart antivirus software, the Distributed Transaction Coordinator Service, and Terminal Services after ControlCenter infrastructure installation is complete.

26.3 Install the installation tools

- a. Insert ControlCenter installation CD #1 in the CD-ROM drive on the target host.

If autorun is enabled, the installation wizard relauches automatically.

- b. If autorun is not enabled, launch:

```
<cd_drive>:\ecc.exe
```

The installation wizard displays the following options:

- **Ensuring Installation Success Tutorial**—View a quick tutorial about planning and installing ControlCenter. Reviews the concepts described in this book.
 - **Begin Installing**—Proceed with install.
 - **Support Information**—View latest EMC contact information.
 - **Exit**—Discontinue the installation.
- c. Recommended: Click **Quick Start Tutorial** or **Support Information** to view helpful planning, installation, and support information.
 - d. Click **Begin Installing**.

The installation wizard displays the copyright and terms of use notices.

- e. Click **Accept** to continue.

The installation wizard displays a dialog box asking you to ensure that any antivirus software running on the target host is disabled before continuing.

Important: Some antivirus programs might be monitored by Services and therefore restart automatically after being stopped initially. Refer to your antivirus software documentation to determine if additional Services need to be stopped.

- If antivirus programs are running, stop the programs, and then click **OK**.
- Otherwise, click **OK** to indicate that no antivirus programs are running.

The installation wizard displays a message indicating the program is loading. When loading is complete, the installation wizard displays a screen requesting the installation directory.

Important: The next step requests the root installation directory for installation tools. In addition to the tools, the installation wizard will also install all other ControlCenter components selected for installation (if there is enough disk space) in the specified directory.

Ensure that the specified drive has adequate disk space to accommodate the ControlCenter components to be installed, and also account for future growth of components such as the Repository (which stores data about all ControlCenter managed objects). The recommended disk space is typically 36 GB.

- f. Select the installation directory where you want to install the installation tools. The default values are described in Table 49.

Table 49 Tools Installation Notes

Field	Description
<i>Choose installation directory</i>	The directory where the installation tools are installed. You must specify both the target drive and a directory name (for example, X:\ECC). Any ControlCenter component selected for installation will also be installed in this directory. <i>Default:</i> C:\ECC Restrictions: ◆ Do not include spaces in the directory path (for example, the following directory path is <i>not</i> valid: C:\Program Files\ecc). ◆ Do not specify universal naming convention (UNC) paths (for example, the following directory path is <i>not</i> valid: \\hostX\ECC).

- g. Click **Next**.

If you do not have enough disk space to install *all* available ControlCenter components on the target host, the installation wizard displays a dialog box indicating that not enough space is available and the amount of available disk space. Do one of the following:

- Click **Back** to select another drive location
- Click **Continue** to proceed while knowing there is not enough space on the designated drive for all available components.

When the *component progress bar* (the one on top—the one on the bottom shows the progress of individual files) reaches 100 percent, the installation tools installed successfully. The installation wizard launches from the specified host directory.

The installation of ControlCenter tools is now complete. The installation wizard prompts for a Repository installation method.

Do one of the following:

- ◆ If you plan to install ControlCenter from a shared folder, exit the installation, and continue with *Step 27: Set Up Shared Folder Installation (Recommended)* on page 120.
- ◆ If you plan to install ControlCenter from the ControlCenter installation CDs, continue with *Step 29: Be Sure You are Ready to Install ControlCenter* on page 130.



Helpful Hints: Using the Installation Wizard

In the install wizard, you can use the following buttons, located at the bottom of most wizard screens, to assist with installation.

- ◆ **Next**—Proceed to the next page.
- ◆ **Back**—Access the previous page.
- ◆ **Exit**—Exit the installation wizard.
- ◆ **Help**—Display a help panel.
- ◆ **Troubleshooting**—Access troubleshooting help, which lists potential problem situations and suggestions for resolution.
- ◆ **Installed Components**—Display a list of ControlCenter components and products that you have successfully installed.

Step 27 Set Up Shared Folder Installation (Recommended)

This section describes how to copy the contents of the ControlCenter installation CDs to a shared folder so you can install ControlCenter on remote clients without having to transfer the ControlCenter installation CDs to different machines.

This procedure is especially useful when installing Master Agents on multiple hosts. You can also use it when installing any of the ControlCenter infrastructure components (ECC Server, Repository, and Store) and optional components and products that are normally installed from the ControlCenter installation CDs (StorageScope, Performance Manager, WebConsole Server, and Master Agent) on multiple hosts.

Distributed infrastructure

Ensure that you install the installation tools (begin with ControlCenter installation CD #1, unless installing from a shared folder) on all hosts where ControlCenter components are to reside.

Copy the Installation CDs to a Shared Folder

From any host with network connectivity and access to the shared drive, create the folder to share, and then copy the ControlCenter installation CDs to that folder using the provided CD copy utility, using the procedure in this section.

Important: The copying of ControlCenter installation CDs to a shared folder is supported only on hosts that are running supported versions of the Windows operating system.

1. Create a folder that will contain the contents of all ControlCenter installation CDs (for example, you could name it `ECC_VirtualCD`). The drive on which you create the folder should have at least 2.4 GB free (not including Solutions Enabler, which you can optionally copy to the same folder).
2. Share the folder you created in the previous step.
3. Ensure that you install the installation tools to the target hosts (refer to *Step 26: Install the Installation Tools on the Target Host* on page 116 for details).

If ControlCenter components were previously installed on the target host (for example, the ECC Server host), it is not necessary to install the installation tools to that host (because they were previously installed, either manually or automatically, to handle the previous installations).

4. From the folder where the ControlCenter tools reside (if you can't remember the folder name and location, refer to Table 49 on page 118), expand the `tools` folder, then the `utils` folder.
5. Double-click the icon labeled **`copy_cds_to_disk.bat`**.

The copy utility prompts for the drive letter where the ControlCenter installation CDs will reside for this copy operation. If ControlCenter installation CD #1 is not in the CD-ROM drive, a CDCopy Utility screen appears. If autorun is enabled, the ControlCenter Main Menu GUI appears. Click EXIT to close it.

6. Enter the drive letter (for example, E:) where the ControlCenter CDs will reside for the copy operation. Then press ENTER.

The copy utility prompts for path to the shared folder to which the contents of the ControlCenter installation CDs will be copied.

7. Enter the full absolute path to the destination shared folder created at the beginning of this procedure. Then press ENTER.

After each ControlCenter installation CD is 100 percent copied, the program prompts you to insert the next CD.

Important: If you plan to install EMC Solutions Enabler using a shared folder (refer to *Make Solutions Enabler available for remote deployment* on page 138 for information about when Solutions Enabler is required), you must manually copy the source files from the Solutions Enabler CD (included in your ControlCenter package) to the shared folder. (`copy_cds_to_disk.bat` does not copy the Solutions Enabler source files to a shared location). Ensure that you have at least 520 MB free disk space to copy the Solutions Enabler source files.

Insert the Solutions Enabler CD in the CD-ROM drive. Then use Windows Explorer to copy all the files from the root directory on the CD (include all files in all subdirectories) to the shared folder. You can use the same shared folder that you used for the ControlCenter installation CDs (for example, ECC_VirtualCD). When the copy is complete, you are ready to make Solutions Enabler available through ControlCenter from the shared folder (refer to *Make Solutions Enabler available for remote deployment* on page 138 for details).

8. After all CDs have been copied, do one of the following to specify if the host should be configured to point to the shared folder for future ControlCenter installations:
 - Enter **y** for yes, and then press **ENTER**, to point the installation program to the shared location (instead of the installation CDs), for any products that you'd like to install in the future from this host. Refer to *Changing the Media Source for ControlCenter Installation* on page 123 for information about how to change the ControlCenter installation source location.
 - Enter **n** for no, and then press **ENTER**, to specify that future invocations of the installation program will look for required installation files on the disk inserted in the CD-ROM drive.

You are now ready to install ControlCenter from a shared location. Go on to the next section, *Install ControlCenter from a Shared Folder*.

Install ControlCenter from a Shared Folder

After you have copied the ControlCenter installation CDs to a shared folder, you can install ControlCenter from that shared folder, using the following procedure.

- a. Map the `ECC_VirtualCD` shared folder (created in *Copy the Installation CDs to a Shared Folder* on page 120) that is to contain the EMC ControlCenter installation CDs to a network drive on the target host.

Distributed infrastructure

If you are installing ControlCenter components and products on multiple machines, ensure that the `ECC_VirtualCD` shared folder is mapped to a network drive on all those hosts.

When you map the network drive, you must map down to the top level of the virtual CD. Do not map to a higher level, and then navigate down to the CD folder. You must map all the way down to the CDs. For example:

Correct: `\\<host>\<drive>\ECC_virtualCD`

Incorrect: `\\<host>\<drive>`

- b. Verify that the installation location for ControlCenter is set to the new shared folder (created in *Copy the Installation CDs to a Shared Folder* on page 120):

- If ControlCenter *was* previously installed on the target host using the ControlCenter installation CDs, the installation wizard is set to use the CD-ROM drive as the installation source location for installation. Perform the steps in the next section, *Changing the Media Source for ControlCenter Installation*, to change the installation source location to the shared folder.
 - If ControlCenter *was not* previously installed on the target host using the ControlCenter installation CDs, no action is necessary.
- c. Display the contents of the top-level directory of the network drive you mapped in step a in this procedure.
 - d. Run `ECC.exe` (in Windows explorer, double-click the icon, or in a command window, enter the filename and press ENTER).
 - e. Click **Install EMC ControlCenter** and **Accept** to agree to the licensing terms.
 - f. Install ControlCenter components or products (refer to *Install and Start the Infrastructure* on page 129 for specific instructions).

Changing the Media Source for ControlCenter Installation

When installing ControlCenter, the target host records the drive letter where the installation source media resided (for example, the CD-ROM drive letter). When you install additional ControlCenter components or products on that same host, the installation program uses that previously recorded drive letter as the installation source. Follow the procedure in this section to tell the installation program to use a different drive letter (other than the one remembered from a previous installation) as the installation source.

Important: Keep in mind that if you change the source for ControlCenter installation, if you want to use the installation CDs again later, you must change the installation source back to the CD-ROM drive letter.

- a. From the root ControlCenter installation directory, expand the `tools` folder, and then the `utils` folder.
- b. Double-click the icon for the following file:

`configure_install_source.bat`

The program displays a command window with a message indicating the current drive for reading ControlCenter install media and a prompt to change the installation source.

- c. Answer **Y** to change the installation source. When prompted, enter the letter of the network drive that you mapped in *Install ControlCenter from a Shared Folder* on page 122 and press ENTER.

The program changes the source to the newly specified location. You are now ready to install ControlCenter components and products from the new location.

To change the source drive back to the CD-ROM drive, repeat this procedure, entering the CD-ROM drive letter as the new source.

Step 28 Create Native Installable Images for UNIX Master and Host Agents

Users can now create native installable images for all UNIX host agents (AIX, HP-UX, LINUX, Solaris). Previously, users could create native installable images for the Master Agent on supported UNIX platforms.

To create installable images for UNIX host agents (AIX, HP-UX, LINUX, and Solaris) as well as the Master Agent on a UNIX host, follow these steps.

1. On the target host, ensure that the only ControlCenter agent installed is the Master Agent. No ControlCenter application agents should be installed yet. If necessary, uninstall any application agents on the target machine before proceeding with creating the native installable image.
2. Using the ControlCenter Console, push *only the host agent* (AIX, HP-UX, LINUX, or Solaris) to the target host.
3. Log on to the target host, and change directory to the *<Master agent install directory>/exec/M*R520* directory.
4. Run the following script:

package_agents.sh

Example: `./package_agents.sh`

5. Specify the output directory for the created packages. Then press Enter.
The program creates the installable image file, where *<host_os_identifier>* is a unique identifier for the operating system installed on the target host: `magent-5.2.00-1<host_os_identifier>`
6. Deploy other agents to the target host as necessary.

If you receive the following message while running `package_agents.sh`, other agents (in addition to the host and Master Agent) could still reside on the host and possibly cause errors in creating the images:

Warning: Only ControlCenter Master and Host Agents should be installed to `/usr/ecc/exec`. Other Agents have been detected on this system.

The images are now available for use with your local scripts or commands for pushing the host agents to the desired hosts.

The native installable images can be uninstalled with the same package manager that is used to install them.

Deploying Host Agent for Windows and/or Windows Master Agent from the Command Line

You can now use a Windows executable to deploy the Host Agent for Windows and/or the Windows Master Agent from the command line.

1. To deploy Host Agent for Windows or the Windows Master Agent (or both) on a host:
2. Change to the following directory on the ECC Server host:
`<inst_root>\media_rep\remoteinstall\WinNativeInstall`
Example:
`cd C:\ecc\media_rep\remoteinstall\WinNativeInstall`
3. Copy **setup.exe** from the directory accessed in the previous step to a location on the host where the agents are to reside.
4. Change to the directory where you copied **setup.exe** and run it as follows:

```
setup.exe /s /v"/qn INSTALLDIR=<ecc_install_root>
SERVERHOSTNAME_ORIP=<eccserver_hostname_or_ip_addr>
[SERVERHOSTNAME_NAME=<ecc_server_hostname>]
[SERVER_PORT=<port_#>]
[MAPORT=<port_#>]
/Liwrmo!veacup+ <log_output_file>
[INSTALLHOSTAGENT=false]
Example (creates only the Windows Master Agent image):
```

```
setup.exe /s /v"/qn INSTALLDIR=C:\ecc
SERVERHOSTNAME_ORIP=ecchost INSTALLHOSTAGENT=false
/Liwrmo!veacup+ C:\temp\CmdLine.log"
```

In the command syntax:

- **INSTALLDIR** is the root directory where the agents are to be installed.
- **SERVERHOSTNAME_ORIP** is the ECC Server hostname or IP address. If you specify the IP address, you must also specify the hostname on the **SERVERHOSTNAME_NAME** parameter.

- `SERVERHOSTNAME_NAME` is the ECC Server hostname or IP address. This parameter is required only if you provided an IP address on the `SERVERHOSTNAME_ORIP` parameter. Do not specify this parameter if you specified a hostname on the `SERVERHOSTNAME_ORIP` parameter.
- `SERVER_PORT` is the ECC Server listening port number. This parameter is optional—if not specified, the default value (5799) is used.
- `MAPORT` is the Master Agent listening port number. This parameter is optional—if not specified, the default value (5798) is used.
- `[/Liwrmo!veacup+]` indicates that `setup.exe` is to create a log file (`<log_output_file>`) that describes its progress.
- `<log_output_file>` is the location of the log file for `setup.exe`. The directory must exist in the file system before you enter the command. Messages that would normally appear in dialog boxes during interactive installation will be prefixed with the following string:
`ECC_LOG_MESSAGE`
For example:
`C:\ecc\ecc_testing.log`
- `INSTALLHOSTAGENT` indicates that only the Windows Master Agent image is to be created (not the host agent image). This parameter is optional—if not specified, the default value (true) is used.

If `setup.exe` completes successfully, the log output file specified in the command contains a message indicating completion. If the command contains syntax errors, `setup.exe` will attempt to invoke its GUI version to request additional command input.

Install and Start the Infrastructure

The ControlCenter *infrastructure* consists of an ECC Server, a Repository, and one or more Stores. The infrastructure is the common foundation that drives ControlCenter.

This section describes how to install and start the infrastructure.

Important: Before installing the infrastructure, ensure that you read *Plan the Infrastructure* on page 7.

- ◆ Step 29: Be Sure You are Ready to Install ControlCenter 130
- ◆ Step 30: Install the Infrastructure 131
- ◆ Step 31: Install the WebConsole Server (Optional) 145
- ◆ Step 32: Configure SSL for Web Applications (Optional) 147
- ◆ Step 33: Configure Agent Load Balancing (Optional) 154
- ◆ Step 34: Start Infrastructure Components 160

Step 29 Be Sure You are Ready to Install ControlCenter

Important: If you do not meet all the prerequisites described in this step, you might experience installation errors or poor system performance during ControlCenter installation.

As a last minute check, ensure that:

- ☐ You log in to the host as one of the following:

- A user who is a member of the local administrator group, or
- A domain account with local administrator group privileges.

Important: If the target host is a member of an NT domain, you must log in as the local user using "Administrator" as the username (or other supported language equivalent).

- ☐ If you plan to install the ECC Server, the `eccadmin` account is created as described in *Step 25: Create the eccadmin Account* on page 114.
- ☐ Terminal Services is disabled on the host where you intend to install the ControlCenter Repository (refer to *Step 23: Consider Services for Remote Access* on page 105 for details).
- ☐ The MS Distributed Transaction Coordinator Service is stopped on the target host(s) (refer to *Step 23: Consider Services for Remote Access* on page 105 for details).
- ☐ **Antivirus software is not running on the target host(s).**

Important: Some antivirus programs might be monitored by Services and therefore restart automatically after being stopped initially. Refer to your antivirus software documentation to determine if additional Services need to be stopped.

- ☐ The Windows Services window is not open.
- ☐ You have met and verified all prerequisites for agents that you intend to deploy, as described in *Plan for Agents* on page 49.
- ☐ You have the Solutions Enabler CD-ROM available (refer to *Step 21: Plan for EMC Solutions Enabler* on page 97 for details).

Step 30 Install the Infrastructure

Use the installation wizard to install the ControlCenter infrastructure, as follows:

- ◆ 30.1 *Log on as a member of the Administrators group* on this page.
- ◆ 30.2 *Understand the functions of buttons in the installation wizard* on page 132.
- ◆ 30.3 *Install the Repository* on page 132.
- ◆ 30.4 *Install the ECC Server* on page 135.
- ◆ 30.5 *Make Solutions Enabler available for remote deployment* on page 138.
- ◆ 30.6 *Install one or more Stores* on page 140.
- ◆ 30.7 *Install other components and products on the infrastructure host* on page 143.
- ◆ 30.8 *Finish the infrastructure installation* on page 144.

Important: EMC strongly recommends that you do not install any third-party software applications on the infrastructure host where the ControlCenter Repository resides.

30.1 Log on as a member of the Administrators group

Log in to the host as one of the following:

- ◆ A user who is a member of the local administrator group, or
- ◆ A domain account with local administrator group privileges.

Important: If the target host is a member of an NT domain, you must log in as the local user using "Administrator" as the username (or other supported language equivalent).

30.2 Understand the functions of buttons in the installation wizard

Be aware that the installation wizard panels display the following buttons during the installation.

Click	To
Next	Proceed to the next page.
Back	Access the previous page.
Exit	Exit the installation wizard.
Help	Display a help panel.
Installed Components	Display a list of currently installed ControlCenter components and products.
Troubleshooting	Display help if you encounter any problems during installation.

30.3 Install the Repository

Each ControlCenter configuration contains exactly one Repository. It is always the first ControlCenter infrastructure component to be installed.

The order of installing products, regardless of host distribution, is controlled by the installation wizard through the installation tables in the Repository. For example, you cannot install the ECC Server without first successfully installing and starting the Repository. The installation tables also allow components to share system information.

The installation wizard displays the following options:

- ◆ Install ECCRepository
- ◆ Specify existing ECCRepository

Before you begin: Ensure that all previously existing Oracle products are removed from the host (the Repository is based on an Oracle database—Oracle installs with the product, but the installation is not visible to the user). If an Oracle product exists on the host, see the procedures for removing the product at <http://www.oracle.com>.

Important: Be aware that some issues have been reported with installing or upgrading the ControlCenter Repository on Windows 2000 or Windows

Server 2003 hosts that are configured with Terminal Services. EMC suggests that you disable Terminal Services (an action that requires a reboot) before installing or upgrading the Repository. You can restart Terminal Services after the install or upgrade is complete. For details, see *Terminal Services* on page 105.

- a. Select **Install ECCRepository** (it should already be selected by default). Then click **Next**.

The installation wizard displays the Repository Data Entry screen.

- b. Enter information about the Repository installation in the Repository Data Entry screen, using Table 50 as a guide:

Table 50 Repository Installation Notes

Required Field	Description
<i>Enable ECC Repository Access via a Firewall</i>	Fixes the Repository port number at 1521, disallowing later dynamic port assignment by the network and allowing the Repository to be configured for access through a firewall. <i>Required for firewall access.</i>
<i>Choose Your Database Backup Directory</i>	The directory that holds Repository hot backup and export files. The drive where the directory resides must have free space that is equal to or greater than the amount of space currently used by the Repository, and reside on a drive other than the drive on which the Repository currently resides. Back up this directory daily to external media such as tape. These files are overwritten every day with the automated scheduled jobs that run, by default, from 2:00 a.m. to 6:00 a.m. (for hot backup) and 10:00 p.m. to 11 p.m. (for export). Run the backup commands manually when needed. <i>For multihoming only:</i> It is recommended but not necessary that the directory reside on a shared disk. <i>Default:</i> None
The following fields appear only when the target host is multihomed.	
<i>Select Primary Network Name for ECC Repository</i>	The default channel at the Repository host for communication to all other hosts. You cannot select the primary network name as the alternative network name for use by the ControlCenter Repository.
<i>Select Alternative Network Names for Repository Communication</i>	The alternate network names at the Repository host for communication to all other hosts.

- c. Click **Next**.

The installation wizard prompts for ControlCenter installation CD #2 (unless you are installing from a shared folder).

- d. Insert ControlCenter installation CD #2 and click **OK**.

The installation wizard begins installing the Repository. The installation wizard shows two progress bars. The top bar shows the progress of the entire component installation. The bottom bar shows the progress of individual file installation for subcomponents.

You may notice delays at certain progress bar percentages while the Repository is installing. Please wait for the installation to complete.

When installation completes, a message appears asking if you want to install more components.

Distributed infrastructure

If the Repository is the only ControlCenter component to be installed on the target host, click **No** to exit the installation. You can restart the installation program later if you decide to install other components or products on the Repository host.

- e. Click **Yes** to continue the installation.

The installation program displays the Available Components list. The Repository appears in a table of installed components immediately below the Available Components list.

Important: The displayed Available Components list includes StorageScope API, which is useful only to advanced users. Most users should skip installing StorageScope API. Refer to *Step 42: Install StorageScope API (Optional)* on page 185 for details.

- f. Proceed to the next section to install the ECC Server.

30.4 Install the ECC Server

Each ControlCenter implementation contains exactly one ECC Server component. The ECC Server contains a main program and a *Media Repository* component, which configures the WebApplications Server, WebConsole Server, API Server, and the SupportTools (ELU), and has installation media for ControlCenter agents, the ControlCenter Console, and the Integration Packages application.

Distributed infrastructure

Do the following to install the ECC Server in a distributed infrastructure (on a host other than the Repository host).

- a. Ensure that the ControlCenter Installation Tools are installed on the target host (refer to *Step 26: Install the Installation Tools on the Target Host* on page 116 for details).
 - a. Double-click the **Start ECC Install** desktop icon to start the installation wizard.
 - b. Select **Specify existing ECCRepository**. Enter the Repository hostname and port number.
 - c. Click **Next** to complete the installation.
 - d. Continue with *Step 30.5: Make Solutions Enabler available for remote deployment* on page 138.
- a. Select **ECCServer** from the Available Components list and click **Add** to add the ECC Server to the Selected Components list.
 - b. Click **Next** to begin installation of the Media Repository component.

The installation wizard prompts for CD #3 (unless you are installing from a shared folder).
 - c. Insert ControlCenter installation CD #3 in the CD-ROM drive. Then click **OK**.



CAUTION

Important: At this point, the installation wizard might display a dialog indicating that a reboot is necessary at the earliest possible point after completing the installation. Remember to reboot the target host after all desired components are installed on the host.

The installation wizard installs the ECC Server component's Media Repository. Then it prompts for ControlCenter installation CD #4 (unless you are installing from a shared folder) to install the SupportTools component of the ECC Server.

- d. Insert ControlCenter installation CD #4 in the CD-ROM drive. Then click **OK**.

The installation wizard installs the SupportTools component of the ECC Server (also known as the *Log Utility*) and prompts for ControlCenter installation CD #4 (unless you are installing from a shared folder) to install the main ECC Server program.

- e. Enter information about the ECC Server installation in the ECC Server Data Entry screen, using Table 51 as a guide.

Table 51 ECC Server Installation Notes

Required Field	Description
<i>Enter Server Port Number</i>	Listening port number of the ECC Server. <i>Default: 5799</i>
<i>Enable LDAP for User Authentication</i>	Determines if LDAP will be used for user authentication. If you select YES, the installation wizard prompts for values shown in Table 48, <i>LDAP Installation Notes</i> on page 103. <i>Default: NO</i>
The following fields appear only when the target host is multihomed.	
<i>Select Primary Network Name for ECCServer</i>	An option list of resolved hostnames or IP addresses assigned to the available network interfaces on the ECC Server host. Select the hostname or IP address that is to be the default channel at the ECC Server host for communication to all other hosts.
<i>Select Alternative Network Names for Console Communications</i>	An option list of resolved hostnames or IP addresses assigned to the available network interfaces on the ECC Server host. Select the list entries that are to be alternate channels for communication to all other hosts from the ECC Server host.

- f. Click **Next**.

The installation wizard installs the ECC Server. When the progress bar reaches 100 percent, the ECC Server installed successfully. The installation wizard displays a screen that asks if you want to make EMC Solutions Enabler available for remote deployment.

The procedure for installing the ECC Server is now complete.



Quick check: Installation status

Before continuing with the installation, review the items in this section to verify the installation status. You might want to click the **Installed Components** button in the installation wizard to check the list of installed components and products.

◆ Components installed to this point:

- *Repository*, from the ControlCenter installation CDs (or a shared folder).
- *ECC Server*, from the ControlCenter installation CDs (or a shared folder).

◆ What's next?

Make EMC Solutions Enabler available for remote deployment, using the ControlCenter Console.

◆ What *required* tasks are ahead?

- Install at least one Store (the component that writes persistent data, collected by agents, to the Repository).
- Install other components or products, such as the Master Agent and WebConsole Server, on using the ControlCenter installation CDs (or a shared folder).
- Install at least one ControlCenter Console (a Java-based application that allows you to monitor and control the storage infrastructure from a central point).
- Deploy Master Agents on *all hosts* to be monitored and managed through ControlCenter.
- Push agents to agent hosts, using the ControlCenter Console.
- Finish setting up application agents (required only for a subset of agents).
- Perform initial discovery.
- Optionally back up ControlCenter.

30.5 Make Solutions Enabler available for remote deployment

EMC Solutions Enabler Version 6.0.2 is a product included with ControlCenter that can manage and retrieve configuration, status, and performance information from Symmetrix arrays, as well as information about databases and filesystems to be monitored by certain ControlCenter agents. EMC Solutions Enabler components include SYMCLI, Solutions Enabler SYMAPI, and Solutions Enabler SYMAPI Server.

Important: When implementing Storage Agent for SMI, you must install EMC Solutions Enabler directly on the agent host, using the Solutions Enabler CDs (or a shared folder). You cannot make Solutions Enabler available through the ControlCenter install wizard for eventual deployment to support Storage Agent for SMI. Refer to *Deploying Solutions Enabler* on page 213 for details.

Follow these steps to make Solutions Enabler 6.0.x available for remote installation.

- a. Click **Yes** (the default) to indicate that you want to package Solutions Enabler to make it available for deployment.
- b. Ensure that at least one of the following is true:
 - You have Solutions Enabler CD #1 (included in the ControlCenter package or as a separately purchased product).
 - If you are performing ControlCenter installation using a shared folder, you have copied the contents of Solutions Enabler CD #1 to that same shared folder.

EMC recommends that you use `configure_install_source.bat` (refer to *Changing the Media Source for ControlCenter Installation* on page 123 for details) to check the current installation source drive before making Solutions Enabler available for deployment. Depending on the previous setting, you might have to change the source drive letter to accommodate deployment through CD or a shared folder.

- c. At the prompt that asks to package Solutions Enabler to make it available for remote deployment, do *one* of the following:
 - Click **I have EMC Solutions Enabler**. The installation wizard does the following:

- Prompts you to insert the most current Solutions Enabler CD (if you did not indicate that you are installing ControlCenter from a shared folder). Insert Solutions Enabler CD #1 in the CD-ROM drive and click OK. Then the install wizard copies the source files for Solutions Enabler to the *Media Repository* so it will be available for remote installation through the ControlCenter Console.
- Starts copying the source files for Solutions Enabler to the *Media Repository* so it will be available for remote installation through the ControlCenter Console, if you were previously installing ControlCenter from a shared folder *and* the current installation drive (obtained from running `configure_install_source.bat` —refer to *Changing the Media Source for ControlCenter Installation* on page 123 for details) is set to the shared folder.
- Click **I DO NOT Have EMC Solutions Enabler**, the ECC Server installation continues without making Solutions Enabler available. If you wish, you can return to the installation wizard later (after obtaining the Solutions Enabler CDs) and make Solutions Enabler available for installation.

The installation wizard displays a message asking if you want to install more components.

Distributed infrastructure

If the ECC Server is the only ControlCenter component to be installed on the target host, and Solutions Enabler is now available in the Media Repository, click **No** to exit the installation (you can restart the installation program later, if you decide to install other components or products on the ECC Server host).

- d. Click **Yes** to continue the installation.

The installation wizard displays the Available Components list.

Refer to the *Solutions Enabler Installation Guide*, Host Specific Issues section for additional set up requirements that might be needed to insure successful use of Solutions Enabler.

The procedure for making Solutions Enabler available is now complete. Later you can deploy Solutions Enabler through the ControlCenter Console, using the Agent Administration Wizard. You can now go on to the next step, *Install one or more Stores*.

30.6 Install one or more Stores

One or more Stores can exist within a ControlCenter implementation. However, only one Store can exist on a single host. Hence, if you are installing ControlCenter as part of a *single-host infrastructure* configuration, in which all infrastructure components reside on one host, you can install only one Store.

Note: If you are installing the Store in a *single-host infrastructure* configuration, the Store installation will proceed very quickly because code is shared with other components. In a *distributed infrastructure* configuration, the Store installation takes more time because the installation wizard cannot share as much code with other already installed components.

Distributed infrastructure

To install the Store in a distributed infrastructure configuration, you will need to provide the Repository hostname and port number during the installation procedure. Be sure to download the Installation Tools to the target host. Then start the ControlCenter installation and select *Specify Existing Repository*.

Do the following to install a Store:

- a. Select **Store** from the Available Components list. Click **Add** to add the Store to the Selected Components list.
- b. Click **Next**.

The installation wizard prompts for ControlCenter installation CD #4 (unless you are installing from a shared folder).

- c. Insert ControlCenter installation CD #4 in the CD-ROM drive. Then click **OK**.

Multihomed host only: The installation program requests the *ECC Server Network Name for ECC Store Communications*. Select the hostname of the NIC on the ECC Server host that is to handle communications with the Store (as described in Table 52).

Important: Be aware that the Store typically installs very quickly if you are installing it as part of a single-host infrastructure configuration.

Table 52 Store Installation Notes (for a Multihomed Host Only)

Required Field	Description
The following field appears only when the ECC Server host is multihomed.	
Select ECC Server Network Name for ECC Store communications	The ECC Server network name to be used for communication with the Store.

The installation wizard installs the Store. When the progress bar reaches 100 percent, the Store installation is complete. The installation program displays a message that asks if you would like to install more components (on this host).

- d. Do one of the following:
- Click **Yes** to continue installing components on the target host.
The installation program displays a list of components (which does not include the components previously installed).
 - Click **No** to exit the installation. Continue with *Step 34: Start Infrastructure Components* on page 160.

The Store installation is now complete. The installation wizard presents you with a list of additional components and products for installation.



Quick check: Installation status

Before continuing with the installation, review the items in this section to verify the installation status. You might want to click the **Installed Components** button in the installation wizard to check the list of installed components and products.

◆ Components installed to this point:

- *Repository*, from the ControlCenter installation CDs (or a shared folder).
- *ECC Server*, from the ControlCenter installation CDs (or a shared folder).
- *EMC Solutions Enabler* (made available for remote deployment, from the Solutions Enabler CDs or a shared folder).
- *Store*, from the ControlCenter installation CDs (or a shared folder).

◆ What's next?

- Install other components or products (such as the Master Agent and WebConsole Server) on infrastructure hosts, using the ControlCenter installation CDs (or a shared folder).
- Finish the ControlCenter infrastructure installation and start infrastructure components.

◆ What required tasks are ahead?

- Install at least one ControlCenter Console (a Java-based application that allows you to monitor and control the storage infrastructure from a central point).
 - Deploy Master Agents on *all hosts* to be monitored and managed through ControlCenter.
 - Push agents to agent hosts, using the ControlCenter Console.
 - Finish setting up application agents (required only for a subset of agents).
 - Perform initial discovery.
-

30.7 Install other components and products on the infrastructure host

You can optionally install the components and products listed in Table 53 on infrastructure hosts.

Table 53 Components Optionally Installed on Infrastructure Hosts

Component	Description
<i>Master Agent</i>	EMC recommends installing the Master Agent on infrastructure hosts to monitor those hosts through ControlCenter (the Master Agent is required on each host to be monitored and managed through ControlCenter). Refer to <i>Step 45: Deploy and Start Master Agents</i> on page 192. You must also install Host Agent for Windows—see <i>Plan for Host Agents</i> on page 76 for details.
<i>Performance Manager</i>	Install Performance Manager (be sure your installation has licensed the application) on the infrastructure host if you want to displays historical performance data for hosts, file systems, Oracle databases, connectivity switches, and EMC storage arrays (all generated by the Workload Analyzer Archiver agent—see <i>Plan for Workload Analyzer Archiver</i> on page 58 for details) from the infrastructure host. Refer to <i>Step 40: Install Performance Manager (Optional)</i> on page 177 for details. When installing Performance Manager no license key is required. Later you will be required to enter the license key through the Console (see <i>Step 37: License the Desired Applications</i> on page 171 for details).
<i>StorageScope</i>	Install StorageScope on the infrastructure host if your installation considers it beneficial for performance and scalability. Refer to <i>Step 41: Install StorageScope (Optional)</i> on page 182. Important: When installing StorageScope, you must enter the StorageScope license key. Later you must enter the license key a second time through the Console (refer to <i>Step 37: License the Desired Applications</i> on page 171 for details).
<i>StorageScope API</i>	Optionally install StorageScope API (be sure your installation has licensed StorageScope) on the infrastructure host if your installation wants to create reporting functionality in addition to that offered by StorageScope. Important: StorageScope API is useful only to advanced users. Most installations should skip installing StorageScope API. Refer to <i>Step 42: Install StorageScope API (Optional)</i> on page 185 for details.
<i>WebConsole Server</i>	Install the WebConsole Server component on the infrastructure host if you want to provide server resources for the Web Console on the infrastructure host. Refer to <i>Step 31: Install the WebConsole Server (Optional)</i> on page 145 for details.

Distributed infrastructure

The SupportTools will also be available for installation. Refer to *Step 43: Install the SupportTools (Optional)* on page 187 for details.

30.8 Finish the infrastructure installation

Do the following after installing ControlCenter components and products on the infrastructure host(s).

- a. Click **Exit** to exit the installation wizard.

The installation program displays a dialog box asking you to confirm that the installation is complete.

- b. Do one of the following in the displayed dialog box:

- Click **OK** to indicate the installation is complete.

The installation program displays a screen indicating the installation is complete, along with the summary of the next steps in the ControlCenter implementation process.

You can select the **Installed Components** button to view a list of installed components or select **Exit** to exit the installation.

Important: After exiting the installation, reboot the target host(s) if the installation program displayed, at any time, a message indicating that a reboot is necessary (be sure to save all your work first). If the installation program did not display such a message, optionally reboot the target host(s) to start services for all the installed components and products (if you do this, you can skip *Step 34: Start Infrastructure Components* on page 160).

- Click **Cancel** to return to the installation wizard and continue installing components and products.

**Helpful Hint: Updating Java Memory Settings**

To optimize performance, you can update the maximum Java memory size, Java memory stack size, initial heap size, and maximum heap size for the ECC Server and Store. The default heap size is 512 MB.

On ECC Server and Store hosts, run the following batch file:

```
<ECC_INSTALL_ROOT>\tools\utils\alter_startup_params.bat
```

The program asks you to enter *JavaMaxHeap* (maximum heap size), *MaxPermSize* (maximum Java memory size), *JavaStackSize* (stack size), and *JavaStartHeap* (the starting heap size). You can enter new values for each or accept the defaults.

Refer to the *EMC ControlCenter Performance and Scalability Guidelines* on Powerlink for more information.

Step 31 Install the WebConsole Server (Optional)

The *WebConsole Server* is a program that controls communications for the *WebConsole*, a Web-based interface through which you can perform a limited number of ControlCenter functions, like monitoring, reporting, and alert management. To launch the WebConsole and login, the WebConsole Server must be installed and running on a host that can access the ControlCenter Repository and ECC Server and is reachable by hosts that are to run the WebConsole.

Follow these steps to install and run the WebConsole Server.

- ◆ 31.1 *Ensure your account has the proper privileges* on this page.
- ◆ 31.2 *Verify the host setup* on this page.
- ◆ 31.3 *Install the WebConsole Server* on page 146.

31.1 Ensure your account has the proper privileges

When installing the WebConsole Server:

- ◆ If the target host is running Windows XP, you must logon as *Administrator*.
- ◆ If the target host is running any other supported Windows operating system (refer to *EMC ControlCenter Support Matrix* on Powerlink for details), you must logon to an account with administrative privileges (an account in the Administrators group).

31.2 Verify the host setup

Verify the following on the target host for the WebConsole Server:

- ◆ Is running the Windows operating system (refer to *EMC ControlCenter Support Matrix* on Powerlink for supported versions).
- ◆ Has access to the ControlCenter Repository host through TCP/IP.
- ◆ Uses DNS to resolve names and IP addresses.
- ◆ Has the ControlCenter installation tools installed. Refer to *Step 26: Install the Installation Tools on the Target Host* on page 116 for details.

31.3 Install the WebConsole Server

You will need the ControlCenter installation CDs to complete this procedure (unless you are installing from a shared folder).

- a. If the installation wizard is already running, skip this step and continue with step b.
 1. Double-click the **Start ECC Install** desktop icon to start the ControlCenter installation wizard.

The installation wizard displays a warning about disabling antivirus software that might be running on the target host. Disable antivirus software, if necessary. Then click **OK**.
 2. Select **Specify existing ECCRepository**.
 3. Enter the Repository host name and port number.
 4. Click Next.
- b. Select **WebConsole Server** from the Available Components list. Click **Add** to add it to the Selected Components list.
- c. Click **Next** to begin the installation.

If you are using the installation CDs, the installation wizard prompts you to insert ControlCenter installation CD #1 (if it is not already in the CD-ROM drive) to continue the installation.
- d. Insert ControlCenter installation CD #1 (if it is not already in the CD-ROM drive). Then click **OK**. (If you are installing from a shared folder, this action is not necessary, because the installation program automatically locates the necessary installation files in the shared folder.)

When the progress bar reaches 100 percent, the WebConsole Server installation is complete. The installation program displays a message that asks if you would like to install more components on the target host.
- e. Do one of the following:
 - Click **Yes** to continue installing components on the target host.
 - Click **No** to exit the installation.

The installation of the WebConsole Server is now complete. You can now start the WebConsole Server using the procedure in *Step 34: Start Infrastructure Components* on page 160.

Step 32 Configure SSL for Web Applications (Optional)

The *Secure Sockets Layer* (SSL), a commonly used protocol for managing data security on the Internet, is included with the Microsoft Internet Explorer and Netscape browsers and the Tomcat Web server, which is used to manage the Web Console and StorageScope. SSL uses sockets to pass data between client and server programs, and verifies the transmitted data with a public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

You can configure SSL to protect the data transmitted to and from the Web Console (refer to *Know when to use the Web Console* on page 44 for details) and StorageScope, using the following procedure:

- ◆ 32.1 Log on with the proper authority on this page.
- ◆ 32.2 Stop services for the WebConsole Server, API Server, or StorageScope Server on page 148.
- ◆ 32.3 Generate a keystore certificate on page 148.
- ◆ 32.4 Enable SSL Communications on page 150.
- ◆ 32.5 Disable non-SSL Communications (Optional) on page 152.
- ◆ 32.6 Restart services for the WebConsole Server, API Server, or StorageScope Server on page 153.
- ◆ 32.7 Publicize the URL of the secure Web Console or StorageScope on page 153.

Web applications include Web Console and StorageScope. The following instructions apply to either web application except where noted. Use the instructions depending on what application you are configuring. For example if you are configuring StorageScope ignore the instructions for WebConsole.

32.1 Log on with the proper authority

Ensure that you are logged on to the web application Server host with an account that is a member of the local Administrators group and that the host is running the Windows operating system (refer to *EMC ControlCenter Support Matrix* on Powerlink for supported versions).

32.2 Stop services for the WebConsole Server, API Server, or StorageScope Server

If it is not already stopped, stop the services that control WebConsole, API Server, or StorageScope communications, as follows:

- a. From the Windows **Start** menu, select **Settings, Control Panel, Administrative Tools, Services**.

For WebConsole:

- b. In the **Services** window, ensure that the **Status** of the **EMC ControlCenter WebConsole Server** service is **Stopped**. If necessary, right-click the service name and select **Stop**.
- c. In the **Services** window, ensure that the **Status** of the **EMC ControlCenter API Server** service is **Stopped**. If necessary, right-click the service name and select **Stop**.

For StorageScope:

- d. In the **Services** window, ensure that the **Status** of the **EMC ControlCenter StorageScope Server** service is **Stopped**. If necessary, right-click the service name and select **Stop**.

32.3 Generate a keystore certificate

To implement SSL, a Web server must have a keystore certificate for each IP address that accepts secure connections. You can use a *self-signed certificate* generated by your installation and optionally verify the certificate using a certificate authority (a third-party organization that issues digital certificates).

Do the following to generate a self-signed certificate:

- a. In a command window on the WebConsole Server or StorageScope Server host, change to the following directory:

```
<ECC_INSTALL_ROOT>\tools\JRE\Nt\1.4.2\bin
```

- b. Enter the following command:

```
keytool -genkey -alias tomcat -keyalg RSA -keystore  
<path_to_keystore_file>
```

In the command, *path_to_keystore_file* is the name of the default directory for user settings. For example:

```
keytool -genkey -alias tomcat -keyalg RSA -validity
350 -keystore "C:\Documents and Settings\Default
User\.keystore"
```

Important: The default expiration for a self-signed certificate is 90 days. EMC recommends that you specify a longer time period for expiration. For example, to specify a 350 day expiration, specify the following on the keytool command: `-validity 350`

Note: To change the default path and filename for `.keystore`, specify the `-add` parameter in the `keytool` command.

The program prompts for a *keystore password*.

- c. Enter the default password used by Tomcat (which is case-sensitive): `changeit`

The program prompts for your first and last name.

- d. Instead of entering your first and last name, enter the network name of the WebConsole Server or StorageScope Server host.

The program prompts for information about your organizational unit.

- e. Enter information about your organizational unit, organization, city or locality, state or province, and two-letter country code. Press Enter after answering each question.

The program displays a summary of the entered information and prompts you to indicate if it is correct.

- f. Enter **yes** to indicate the information is correct, or **no** (the default) to make changes.
- g. Enter the key password for Tomcat (which is case sensitive), or press Enter to make it the same as the default password (`changeit`) specified in step c above.

The program creates the following file:

```
C:\Documents and Settings\<username>\.keystore
```

- h. Optionally enter the following command to create a Certificate Signing Request (CSR), which allows you to obtain a certificate from the Certificate Authority of your choice:

```
keytool -certreq -keyalg RSA -alias tomcat -file
certreq.csr -keystore <your_keystore_filename>
```

The program creates a file encoded in PEM format, called `certreq.csr`.

- i. Optionally submit `certreq.csr` to a Certificate Authority. The following are some possible Certificate Authorities:
- **Verisign:** <http://www.verisign.com/support/install/intermediate.html>
 - **Trustcenter:** <http://www.trustcenter.de/certservices/cacerts/en/en.htm#server>
 - **Thawte:** <http://www.thawte.com/certs/trustmap.html>

The Certificate Authority will return to you a *chain certificate*.

- j. Optionally (if you performed step i) enter the following command to import the chain certificate into your keystore.

```
keytool -import -alias root -keystore
<your_keystore_filename> -trustcacerts -file
<filename_of_the_chain_certificate>
```

32.4 Enable SSL Communications

To enable SSL communications, uncomment a section in the server configuration file on the WebConsole Server or StorageScope Server host, as follows.

- a. Open the following file in a text editor:

```
For WebConsole:
<ECC_INSTALL_ROOT>\ECCWebConsole\tomcat\conf\server.xml
```

```
For StorageScope:
<ECC_INSTALL_ROOT>\StorageScope\appserver\conf\server.xml
1
```

- b. In `server.xml`, *remove* the XML comment characters shown in **bold** below.

For WebConsole:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443
-->
<!--
<Connector
className="org.apache.coyote.tomcat4.CoyoteConnector"
  port="8443" minProcessors="5" maxProcessors="75"
  enableLookups="true"
  acceptCount="100" debug="0" scheme="https"
  secure="true">
<Factory
className="org.apache.coyote.tomcat4.CoyoteServerSocket
Factory"
                                clientAuth="false" protocol="TLS"/>
</Connector>
-->
```

For StorageScope:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector
className="org.apache.catalina.connector.http.HttpConne
ctor"
  port="8443" minProcessors="5" maxProcessors="75"
  enableLookups="true"
  acceptCount="10" debug="0" scheme="https"
  secure="true">
<Factory
className="org.apache.catalina.net.SSLServerSocketFacto
ry"
                                clientAuth="false" protocol="TLS"/>
</Connector>
-->
```

- c. Save `server.xml`, but leave it open for editing—the next step entails further edits to `server.xml`.

32.5 Disable non-SSL Communications (Optional)

ECC Console cannot launch StorageScope reports if non-SSL communication is disabled.

To optionally disable non-SSL communications, comment out a section in the server configuration file on the WebConsole Server or StorageScope Server host, as follows:

- a. If not already editing this file, open it in a text editor.

For WebConsole:

```
<ECC_INSTALL_ROOT>\ECCWebConsole\tomcat\conf\server.xml
```

For StorageScope:

```
<ECC_INSTALL_ROOT>\StorageScope\appserver\conf\server.xml
1
```

- b. Comment out (add the characters `<!--` and `-->` as shown in **bold below**) the section of `server.xml` that defines a non-SSL connection.

For WebConsole:

```
<!-- Define a non-SSL Coyote HTTP/1.1 Connector on port 7070->
<!--
<Connector
className="org.apache.coyote.tomcat4.CoyoteConnector"
port="7070" minProcessors="5" maxProcessors="75"
enableLookups="true" redirectPort="8443"
acceptCount="100" debug="0" connectionTimeout="20000"
useURValidationHack="false" disableUploadTimeout="true"/>
-->
```

For StorageScope:

```
<!-- Define a non-SSL HTTP/1.1 Connector on port 8080->
<!--
<Connector
className="org.apache.catalina.connector.http.HttpConnector"
port="8080" minProcessors="5" maxProcessors="75"
enableLookups="true" redirectPort="8443"
acceptCount="10" debug="0" connectionTimeout="60000"
<!-- Define a non-SSL Coyote HTTP/1.1 Connector on port 7070->
-->
```

- c. Save `server.xml` and exit the file.

32.6 Restart services for the WebConsole Server, API Server, or StorageScope Server

Restart the services that control Web Console communications on the WebConsole Server or StorageScope Server host, as follows.

- a. From the Windows Start menu, select **Settings, Control Panel, Administrative Tools**, then **Services**.

For WebConsole:

- b. In the **Services** window, right-click the **EMC ControlCenter API Server** service and select **Start**.
- c. In the **Services** window, right-click the **EMC ControlCenter WebConsole Server** service and select **Start**.

For StorageScope:

- d. In the **Services** window, right-click the **EMC ControlCenter StorageScope Server** service and select **Start**.

32.7 Publicize the URL of the secure Web Console or StorageScope

Inform users about the URL of the Web Console and StorageScope.

For WebConsole:

`https://<ECCServerHostname-OR-IPAddress>:xxxx/eccweb`

For StorageScope:

`https://<ECCServerHostname-OR-IPAddress>:xxxx/sts`

where `xxxx` is an available port number.

Step 33 Configure Agent Load Balancing (Optional)

When a ControlCenter configuration contains multiple agents of a particular type (for example, two Storage Agents for Symmetrix), ControlCenter balances (distributes evenly) the processing load between those agents, by assigning top-level managed objects (storage arrays, databases, switches, hosts, etc.) to specific agents. Load balancing can greatly improve the overall performance of agents and agent hosts.

If desired, your installation can turn load balancing “off” for one or more agent types, or select the types of load balancing (described in this section) to be performed. If load balancing is turned “off” for one or more agent types, the agents of those types monitor and manage the objects that they initially discover—ControlCenter does not periodically evaluate agent processing load and reassign objects to agents accordingly.

This section describes how to optionally update a configuration file on the ECC server host to specify the following.

- ◆ The types of agents that are to perform load balancing.
- ◆ Which types of agent load balancing ControlCenter is to perform (*full* and/or *partial*, described below).
- ◆ The frequency at which ControlCenter performs full agent load balancing.

Use the following procedure to configure load balancing for your ControlCenter installation:

- ◆ 33.2 *Understand primary agent status* on this page.
- ◆ 33.2 *Understand the types of load balancing* on page 155.
- ◆ 33.3 *Know the configuration parameters for load balancing* on page 156.
- ◆ 33.4 *Update your load balancing configuration* on page 159.

33.1 Understand primary agent status

When a ControlCenter configuration contains multiple agents of a particular type, ControlCenter designates one agent as *primary* for each object that is common to (discovered by) multiple agents. The *primary agent* monitors and manages an object. The other agent(s) can take over processing of that object in the event of a failover or load balancing situation.

ControlCenter uses the following criteria to determine which agent of a particular type is primary. If ControlCenter cannot determine primary status based on the first criterion, it considers the second, then the third, and so on.

1. The agent that has the highest version level (for example, 5.2). The primary agent should have version equal or higher than the version of the agent that last reported data on the managed object to ControlCenter.
2. The agent that has the shortest logical distance to the managed object.
3. The agent that has the lowest processing load.
4. The first agent located by the ECC Server.

33.2 Understand the types of load balancing

ControlCenter can utilize the following two types of load balancing:

- ◆ **Partial load balancing:** This type of load balancing is performed each time agents report the lists of objects they can manage to the ControlCenter infrastructure. ControlCenter analyzes changes to the number of managed objects and adjusts the distribution of managed object information to the affected agents. Partial load balancing is faster than *full load balancing*, but it often cannot resolve situations that create imbalance across all ControlCenter agents of the same type.

Consider the following simple example:

1. Two Storage Agents for Symmetrix (S1 and S2) each discover 10 managed objects. Five of those objects are common to both agents, indicating there are 15 total discovered managed objects (10 managed objects discovered by the two agents, minus 5 that are common to both).
2. ControlCenter determines that S1 is *primary* for 7 of the 15 managed objects, and S2 is primary for 8 of the 15.
3. A third Storage Agent for Symmetrix (S3) is started. It discovers 5 managed objects that are in common with S2.
4. Partial load balancing reallocates 4 of S2's 8 objects to S3, which becomes *primary* for those 4 moved objects, balancing the load (each agent is primary for 4 objects) between the agents. However, partial load balancing cannot resolve imbalance with agent S1 (full load balancing is required).

- ◆ **Full load balancing:** This type of load balancing is activated periodically, based on a time period specified in the load balancing configuration file on the ECC Server host (described in the next step). It balances load across all ControlCenter agents of the same type (not just agents affected by managed object changes, as with partial load balancing) and their managed objects. It requires more resources than *partial load balancing* and generally runs less frequently.

Consider the example described previously in *Partial load balancing*. When full load balancing is enabled (as it is by default), the following additional steps take place:

1. ControlCenter sees the following distribution of managed objects between Storage Agents for Symmetrix, based on the results of partial load balancing.
 - S1 is primary for 7 managed objects
 - S2 is primary for 4 managed objects
 - S3 is primary for 4 managed objects
2. To balance the load, ControlCenter moves primary status for one object from agent S1 to agent S2, and a second object from agent S1 to agent S3.
3. The resulting distribution from full load balancing is as follows.
 - S1 is primary for 5 managed objects
 - S2 is primary for 5 managed objects
 - S3 is primary for 5 managed objects

33.3 Know the configuration parameters for load balancing

You can configure load balancing for ControlCenter agents by updating parameters in the following file on the ECC Server host.

```
<ECCRootDirectory>\ecc_inf\data\<ECC_Server_Host
name>\class\AgentManager.properties
```

Before you configure load balancing, you must understand the default settings for the configuration fields in `AgentManager.properties` (described below) and determine if they are appropriate for your installation.

The following fields in `AgentManager.properties` apply to load balancing.

- ◆ `LoadBalancer.CountBasedLB.EnableFullLB`

When set to `true`, this field enables full load balancing for all agent types, except those that are specifically *disabled* in `LoadBalancer.CountBasedLB.EnableFullLBPerAgentType`. When set to `false`, this field disables full load balancing for all agent types (regardless of any values on any other parameters).

Default: `true`

- ◆ `LoadBalancer.CountBasedLB.FullLBActivationPeriod`
Specifies the interval at which the ECC Server performs full load balancing, in milliseconds. This field is valid only if full load balancing is enabled for at least one agent type.

Default: `3600000` (one hour)

- ◆ `LoadBalancer.CountBasedLB.EnableFullLBPerAgentType`
Disables full load balancing for specific agents. Agents are specified according to their three-letter prefixes, which are listed in Table 62 on page 320.

Default: Full load balancing is enabled for all agents.

For example, the following enables full load balancing for all agents *except* those associated with the acronyms EGS (Storage Agent for Symmetrix) and EGZ (Common Mapping Agent).

```
LoadBalancer.CountBasedLB.EnableFullLB=true
LoadBalancer.CountBasedLB.EnableFullLBPerAgentType=EGS:false|EGZ:false
```

Syntax note: Spaces are not allowed between agent acronyms, the “or bar” (`|`), and the boolean value.

- ◆ `LoadBalancer.CountBasedLB.EnablePartialLB`
When set to `true`, this field enables partial load balancing for all agent types, except those that are specifically *disabled* on `LoadBalancer.CountBasedLB.EnablePartialLBPerAgentType`. When set to `false`, this field disables partial load balancing for all agent types (regardless of any values on any other parameters).

Default: `true`

- ◆ `LoadBalancer.CountBasedLB.EnablePartialLBPerAgentType`
Disables partial load balancing for specific agents. Agents are specified according to their three-letter prefixes, which are listed in Table 62 on page 320.

Default: Partial load balancing is enabled for all agents.

For example, the following enables partial load balancing for all agents *except* those associated with the acronyms EGS (Storage Agent for Symmetrix) and EGZ (Common Mapping Agent).

```
LoadBalancer.CountBasedLB.EnablePartialLB=true
LoadBalancer.CountBasedLB.EnablePartialLBPerAgentType=EGS:false|EGZ:false
```

Syntax note: Spaces are not allowed between agent acronyms, the “or bar” (|), and the boolean value (false).

- ◆ `LoadBalancer.CountBasedLB.AgentOverloadedThreshold`
Specifies the number of managed objects under the management of agents specific agent types that, when exceeded, indicates that the agents of that type are overloaded. When the “overloaded condition” occurs, the ECC Server sends an alert to ControlCenter Console interfaces. When the agent's load returns to a level that is equal to or beneath the threshold, the ECC Server clears the alert. Agents are specified according to their three letter prefixes, which are listed in Table 62 on page 320.

Default: EGS:2 | EGZ:100 | EGN:100 | CNN:10

- ◆ `LoadBalancer.CountBasedLB.LBActivationThreshold`
Specifies the threshold for load balancing activation. When the number of managed objects managed by an agent exceeds the value specified in this field, ControlCenter changes the primary status for the associated managed object to a less loaded agent. Agents are specified according to their three-letter prefixes, which are listed in Table 62 on page 320.

Default: EGS:2 | EGZ:1 | EGN:1 | CNN:5

33.4 Update your load balancing configuration

If the default load balancing configuration is not appropriate for your installation, follow these steps to update the configuration.

- a. From the Windows Start menu, select **Settings, Control Panel, Administrative Tools**, then **Services**.
- b. In the **Services** window, ensure that the **Status** of the **EMC ControlCenter Server** service is **Stopped**. If necessary, right-click the service name and select **Stop**.
- c. If necessary, update the following file, using the parameter descriptions in the previous step as a guide:

```
<ECCRootDirectory>\ecc_inf\data\<ECC_Server_Host  
name>\class\AgentManager.properties
```
- d. Save the file you updated in the previous step.
- e. Start the **EMC ControlCenter Server** service and any other ControlCenter services that need to be started. Refer to *Step 34: Start Infrastructure Components* on page 160 for details.

Step 34 Start Infrastructure Components

To start the ControlCenter infrastructure components:

- ◆ 34.1 *Reboot the Repository host* on this page.
- ◆ 34.2 *Verify that the Repository has started* on this page.
- ◆ 34.3 *Start the ECC Server, Store(s), and WebApplications Server* on this page.
- ◆ 34.4 *Start other installed products* on page 161.

Important: If you previously rebooted the infrastructure host(s) after installing all desired ControlCenter components and products, the services for those components and products are automatically started—therefore there is no need to perform the steps in this section.

34.1 Reboot the Repository host

Before you start ControlCenter components and products (or verify that they have started automatically after reboot), you must reboot the host on which the Repository resides.

34.2 Verify that the Repository has started

The Repository starts up automatically as a service. The Repository must be running to continue installing other components.

Do the following on the Repository host to verify the Repository is running:

- a. Select **Start, Settings, Control Panel**, and then open **Administrative Tools**.
- b. Open **Services** and then scroll to locate and verify that Oracle database services have started.

The following services are configured to start automatically during install time (it might take 2 to 5 minutes for them to start):

```
OracleServiceRAMBDB
OracleECCREP_HOMETNSListener
```

34.3 Start the ECC Server, Store(s), and WebApplications Server

Follow these steps to start the ECC Server, Store(s), and WebApplications Server, or verify that those components have

started if they reside on a host that was rebooted after the components were installed.

Distributed infrastructure

If you installed the ECC Server and Store(s) on different hosts, start these services *in order* on the separate hosts (start the ECC Server on the ECC Server host, then start the Store(s), and so on).

- a. Select **Start, Settings, Control Panel**, then **Administrative Tools**.
- b. Open **Services**. Right-click the names of the services associated with the products and select **Start** (or verify that **Start** is already selected), in the order shown below:
 1. EMC ControlCenter Server
 2. EMC ControlCenter Store
 3. EMC ControlCenter WebApplications Server

34.4 Start other installed products

If you installed the Master Agent, StorageScope, WebConsole Server, or Performance Manager on the infrastructure host(s), start the services associated with those products (or verify that they have started, if they reside on hosts that were rebooted after the components were installed), as follows:

- a. From the **Start** menu, select **Settings**, then **Control Panel**.
- b. Open **Administrative Tools** and then select **Services**.
- c. Right-click the names of the services associated with the products and select **Start** (or verify that **Start** is already selected):
 - EMC ControlCenter Master Agent
 - EMC ControlCenter StorageScope
 - EMC ControlCenter ECCAPI Server (required to run the WebConsole Server and the Storage Provisioning Services Command Line Interface)
 - EMC ControlCenter WebConsole Server
 - EMC ControlCenter Performance Manager Reports
- d. If you installed Performance Manager on an infrastructure host, you need to deploy Workload Analyzer Archiver agent before using Performance Manager. Refer to *Step 40: Install Performance Manager (Optional)* on page 177 for details.



Quick check: Installation status

Before continuing with the installation, review the items in this section to verify the installation status. You might want to click the **Installed Components** button in the installation wizard to check the list of installed components and products.

◆ Components installed to this point:

- *Repository*, from the ControlCenter installation CDs (or a shared folder).
- *ECC Server*, from the ControlCenter installation CDs (or a shared folder).
- *EMC Solutions Enabler* (made available for remote deployment, from the Solutions Enabler CDs or a shared folder).
- *Store*, from the ControlCenter installation CDs (or a shared folder).
- Optional components (Master Agent, WebConsole Server, StorageScope, Performance Manager) on infrastructure hosts.

◆ What's next?

- Install at least one ControlCenter Console (a Java-based application that allows you to monitor and control the storage infrastructure from a central point).
- Tell remote users (and local users that don't require full ControlCenter Console capabilities) how to access ControlCenter through the Web Console.

◆ What required tasks are ahead?

- Deploy Master Agents on all hosts to be monitored and managed through ControlCenter.
 - Push agents to agent hosts, using the ControlCenter Console.
 - Finish setting up application agents (required only for a subset of agents).
 - Perform initial discovery.
-

Now that you have installed the ControlCenter infrastructure, you can install the *ControlCenter Console* and optionally the *WebConsole* to monitor and manage the ControlCenter environment, and install applications to perform your required business functions.

- ◆ Step 35: Install the ControlCenter Console..... 164
- ◆ Step 36: Launch the ControlCenter Console and Log In..... 168
- ◆ Step 37: License the Desired Applications..... 171
- ◆ Step 38: Launch the Web Console and Log In (Optional) 172
- ◆ Step 39: Install the Integration Packages (Optional)..... 175
- ◆ Step 40: Install Performance Manager (Optional) 177
- ◆ Step 41: Install StorageScope (Optional)..... 182
- ◆ Step 42: Install StorageScope API (Optional)..... 185
- ◆ Step 43: Install the SupportTools (Optional) 187
- ◆ Step 44: Install the EACLI Client (Optional) 189

Step 35 Install the ControlCenter Console

The *ControlCenter Console* is a Java-based application that is installed through Microsoft Internet Explorer or Netscape (refer to *EMC ControlCenter Support Matrix* on Powerlink for supported versions) and launched from a desktop icon or from the command line. ControlCenter applications are implemented as plug-ins to the ControlCenter Console and use the common collection of services provided by the ECC Server.

- ◆ Be sure to read *Step 9: Plan for Console Interfaces* on page 40 before performing the steps in this section.
- ◆ Do not install the Console more than once on any particular host. If you need additional Console sessions, you can invoke one instance of the program multiple times.
- ◆ Put the installation CDs aside for now. You will use a Web browser (Internet Explorer or Netscape) to install the Console.
- ◆ If users require only a limited set of functions, consider using the Web Console (refer to *Know when to use the Web Console* on page 44 for details) instead.

Follow these steps to download the ControlCenter Console installation program and install one or more Consoles:

- ◆ 35.1 *Verify setup of the ControlCenter infrastructure* on this page.
- ◆ 35.2 *Ensure your account has the proper privileges* on page 165.
- ◆ 35.3 *Download the ControlCenter Console* on page 165.
- ◆ 35.4 *Install the ControlCenter Console* on page 166.

Firewall Consideration

Consider using Terminal Services, Citrix, or VNC if you plan to provide secure access to the ControlCenter Console from outside a firewall. Refer to *Step 23: Consider Services for Remote Access* on page 105 for details.

35.1 Verify setup of the ControlCenter infrastructure

The Console is downloaded from the ECC Server and communicates with the ECC Server to monitor your environment. Before installing the ControlCenter Console, the ControlCenter infrastructure must be installed and running. Specifically, verify that the **EMC ControlCenter WebApplications Server** service is running on the ECC Server host.

35.2 Ensure your account has the proper privileges

When installing the ControlCenter Console:

- ◆ If you want to make the Console available to all users that log on to the target host, you must log on to an account with administrative privileges (in other words, an account in the Administrators group).
- ◆ If you want to make the Console available only to a specific user (one that does not have administrative privileges) on the target host, log on to that user's account.

35.3 Download the ControlCenter Console

Do the following to download the ControlCenter Console:

- a. In your Web browser, enter the URL for Console download:

`http://<ECCServerHostname-OR-IPAddress>:30000`

For example, if the ECC Server host name is `eccsvrhost` and the IP address is 123.45.4.321, use either of the following.

`http://eccsvrhost:30000`
`http://123.45.4.321:30000`

- If your browser *has* a Java virtual machine (JVM) that can run the installation program, the installation program displays the *Console installation home page*. Continue with the next step.
- If your browser *does not have* a JVM that can run the installation wizard, the Web page displays a message panel that explains how to download and install a valid JVM:
 1. Download a JVM from `http://java.sun.com` by clicking on the *Sun's Java website* link in the message panel. EMC recommends that you install the latest version of a generally available JVM (in other words, *not* one that is currently available for testing, for example a beta version).
 2. After the JVM is downloaded and installed:
 - If using Internet Explorer, click on the link *EMC ControlCenter Download Page* in the message panel. Then continue with the next step.
 - If using Netscape, stop and restart the Web browser session. Then enter the URL for Console download again (as described in step a above).

- b. Click the **Installation** option. Then click **Console 5.2**.

If desired, click the **Documentation Library** link to view documentation that can help with ControlCenter Console installation.

If this is the first time you have installed the ControlCenter Console on this host, the Security Warning dialog box appears.

- c. Click **Yes** to continue.

A progress bar appears indicating that the ControlCenter Console installation is downloading to the host. When the progress bar reaches 100 percent, the ControlCenter Console installation wizard launches automatically (this may take a few moments).

35.4 Install the ControlCenter Console

- a. Click **Next** in the ControlCenter Console Installation Welcome message screen.

If the Welcome screen does not open, minimize other open windows and wait for the screen to appear. If you receive a warning indicating that the InstallShield Certificate has expired, you can safely ignore this message and continue the download.

- b. Select the destination directory where you want to install the ControlCenter Console, as shown in Table 54.

Table 54 Console Installation Notes

Field	Description
<i>Console download location</i>	The directory you intend to install the ControlCenter Console. <i>Windows default:</i> C:\Program Files\ecc\console <i>UNIX default:</i> /opt/ecc/console

If the installation program detects a previous version of the ControlCenter Console on the host, it displays a message indicating the actions to be taken before continuing. After resolving the issues with the previous installation, click **Next** again to continue.

A progress bar appears indicating that the ControlCenter Console installation is taking place. When the progress bar reaches 100 percent, the Installation Summary message appears indicating that the installation was successful.

- c. Click **Finish** to exit the Console installation and close any unneeded web browser windows.

**Further information**

Refer to *EMC ControlCenter 5.2 Performance and Scalability Guidelines* on Powerlink for performance and scalability guidelines relating to ControlCenter Console installation.

Step 36 Launch the ControlCenter Console and Log In

Follow these steps to launch the ControlCenter Console and log in.

- ◆ 36.1 *Launch the Console application* on this page.
- ◆ 36.2 *Log in to the ControlCenter Console* on page 170.
- ◆ 36.3 *Remove or restrict use of the first ControlCenter Administrator account (recommended)* on page 170.

Terminal Emulation (Terminal Services/Citrix/VNC)

Terminal Services, Citrix, or VNC server configurations determine how many ControlCenter Console sessions can run concurrently.

Note: You can launch both the ControlCenter Console and Web Console on the same host at the same time.

Important: Before starting a Console interface, ensure that the ECC Server and Repository have been running for an adequate amount of time (approximately five minutes).

36.1 Launch the Console application

Windows

- a. Click the **Start ECC Console** icon on the desktop, or from a command line, run:

```
<Console_install_directory>\bin\launch.bat
```

The system displays the ControlCenter Launch Utility screen.

- b. If not already entered, enter the following:
 - ECC Server hostname, IP address, or fully qualified hostname
 - ECC Server host port number for Console communications
- c. Optionally select the **Enable Console Logging** checkbox to save extended debugging information from the Console (which can be useful in troubleshooting) to the following location:

```
%USERPROFILE%\ecc\data\<servername>\console.trc
```

where %USERPROFILE% is the root directory for ControlCenter Console logging information and <servername> is the ECC Server hostname, IP address, or fully qualified hostname (whichever you specified at logon).

ControlCenter always saves standard output from the ControlCenter Console to the `consoleLaunch.log` file in the same location (regardless of whether the **Enable Console Logging** checkbox is selected).

- d. Click **Submit**.

The user logon screen is displayed.

Solaris

- a. From the command line, run:

```
<Console_installation_directory>/bin/launch.csh
```

The system displays the ControlCenter Launch Utility screen.

- b. If not already entered, enter the following:
 - ECC Server hostname, IP address, or fully qualified hostname
 - ECC Server host port number for Console communications
- c. Optionally select the **Enable Console Logging** checkbox on the user logon screen to save extended debugging information from the ControlCenter Console (which can be useful in troubleshooting) to one of the following locations:
 - If \$HOME is defined:

```
$HOME/ecc/data/<servername>/consoleLaunch.trc
```

where \$HOME is the root directory for ControlCenter installation.

- If \$HOME is *not* defined:

```
<install_dir>/data/ecc/<servername>/consoleLaunch.trc
```

where \$HOME is the root directory for ControlCenter installation.

ControlCenter always saves standard output from the ControlCenter Console to the `console.trc` file in the same location (regardless of whether the **Enable Console Logging** checkbox is selected).

- d. Click **Submit**. The user logon screen is displayed.

36.2 Log in to the ControlCenter Console

- a. Enter your **User Name**. Use one of the following the first time you log in, until the ControlCenter Administrator adds other users through the ControlCenter Console.
 - `eccadmin` (if using Windows authentication)
 - The username to which you assigned ControlCenter administrative privileges in *Step 25: Create the eccadmin Account* on page 114 (if using LDAP).
- b. Enter your password.
- c. Click **OK**. The ControlCenter Console user interface appears.

36.3 Remove or restrict use of the first ControlCenter Administrator account (recommended)

EMC recommends that you remove `eccadmin` or limit its capabilities, once you have successfully installed a ControlCenter Console and implemented at least one other account with the same capabilities.

Further information

- ◆ Refer to *EMC ControlCenter 5.2 Performance and Scalability Guidelines* on Powerlink for performance and scalability guidelines relating to ControlCenter Consoles.
- ◆ For details on creating and maintaining ControlCenter user accounts, refer to *EMC ControlCenter 5.2 Administration/User Guide*.



Performance and Scalability Guidelines: Active Consoles

Limit the number of active Consoles to ten during peak ControlCenter use.

Limiting the number of active Consoles to ten helps maintain performance. Consoles are considered active if they are running user commands, even for views that update real-time information.

Important: If the number of active ControlCenter Consoles should exceed ten, contact EMC Customer Support for additional guidelines.

Step 37 License the Desired Applications

To enable all product functionality in the ControlCenter Console, know the products that require licenses, and enter the license keys as needed. This function is available only from the ControlCenter Console (it is not available from the Web Console).

Important: License each application once from only one Console. Subsequent Console launches on other hosts will have all licenses enabled (so there is no need to enter the licenses more than once).

- a. From the ControlCenter Console, select **ECC Administration** in the task bar.
- b. From the **Install** menu, select **Edit Licenses**.
- c. Enter the appropriate license keys from your license key card into the text fields and click **OK**.
- d. Exit the ControlCenter Console.
- e. Restart the ControlCenter Console to enable the licenses.

Important: Even if you entered the StorageScope license through the install wizard, you must enter this license again through the Edit Licenses... dialog box or agents associated with this license will not be installable.

Step 38 Launch the Web Console and Log In (Optional)

The *Web Console* is a Web-based interface through which you can perform a limited number of ControlCenter functions, like monitoring, reporting, and alert management. Unlike the Console Java application, no installation of the Web Console is necessary—users can simply launch it through a Web browser. The Web Console is best suited to users who are to monitor ControlCenter remotely, or local users that require only limited ControlCenter functions.

- ◆ 38.1 *Verify setup of the ControlCenter infrastructure* on page 164.
- ◆ 38.3 *Understand potential issues with pop-up blockers* on page 173.
- ◆ 38.4 *Log Into the Web Console* on page 173.

Note: You can launch both the Web Console and the ControlCenter Console (refer to *Step 36: Launch the ControlCenter Console and Log In* on page 168 for details) on the same host.

38.1 Verify setup of the infrastructure and WebConsole Server

Before launching the Web Console, ensure the following ControlCenter components are installed and running:

- ◆ OracleECCREP_HOMETNSListener
- ◆ OracleServiceRAMBDB
- ◆ EMC ControlCenter Server
- ◆ EMC ControlCenter API Server
- ◆ EMC ControlCenter Store (at least one must be installed—none have to be running)
- ◆ EMC ControlCenter WebConsole Server

38.2 Verify the host setup

Do the following to verify setup of the host where the Web Console is to run in a Web browser.

- a. Verify that Java VM 1.4.2_03 or higher is installed as a plug-in and is activated on the host where the Web Console is to run.
 - If using Internet Explorer, under **Tools, Internet Options**, ensure that *Use Java 1.4.2 for <applet> (requires restart)* under Java(Sun) appears and is checked. If that option does not appear, download Java VM 1.4.2 from

`http://java.sun.com`. Then restart Internet Explorer, access **Internet Options** as described above, and ensure the option is checked.

- If using Netscape, under **Edit, Preferences, Advanced**, ensure the option *Enable Java* is checked. When you download and install Java VM 1.4.2 from `http://java.sun.com`, the install wizard asks you which browsers to plug into. When you specify the Netscape browser that you are using to access the Web Console, the Java VM is enabled by default.
- b. Verify that the host has a 500 MHz processor or higher, 256 MB RAM or higher, and 50 MB available disk space.
- c. Verify that one of these operating systems is installed.
 - AIX 5.1, 5.2, or 5.3
 - HP-UX 11.0, 11.11, or 11.23
 - Red Hat Enterprise Linux AS 3.0
 - Solaris 8, 9, or 10
 - Windows Server 2003
 - Windows 2000 SP2, SP3, or SP4
 - Windows XP SP1 or SP2

38.3 Understand potential issues with pop-up blockers

Like any Web application, display of the Web Console could be prevented by *popup blocker* software that resides on a local host. In addition, online help for the Web Console, which is displayed in a separate browser window, could be blocked (not displayed).

In this situation, users can do one of the following to allow display of the Web Console:

- ◆ Disable the pop-up blocker software while using the Web Console.
- ◆ Use the pop-up blocker's *unblocking mechanism* to access the Web Console and its online help. Usually this involves holding the CTRL key down while clicking the Refresh button in the browser or a hyperlink.

38.4 Log Into the Web Console

Do the following to login to the Web Console:

- a. Open the Web browser and enter the URL as follows.

- For non-secure communications:

`http://<ECCServerHostname-OR-IPAddress>:7070/eccweb`

For example, if the ECC Server host name is `eccsvrhost` and the IP address is `123.45.4.321`, use either of the following:

`http://eccsvrhost:7070/eccweb`

`http://123.45.4.321:7070/eccweb`

- For secure communications (if implemented using *Step 32: Configure SSL for Web Applications (Optional)* on page 147):

`https://<ECCServerHostname-OR-IPAddress>:8443/eccweb`

For example, if the ECC Server host name is `eccsvrhost` and the IP address is `123.45.4.321`, use either of the following:

`https://eccsvrhost:8443/eccweb`

`https://123.45.4.321:8443/eccweb`

Important: If you have previously logged in to a ControlCenter Web application, the steps that follow might not be necessary because login information is stored from the previous access. If this is the case, ControlCenter skips the login screen and displays the WebConsole interface.

- Enter your username. Use `eccadmin` (or, if using LDAP, the User Name associated with the initial ControlCenter Administrator account) the first time you log on, until the ControlCenter Administrator (`eccadmin` user) adds other users through the ControlCenter Console.
- Enter your password.
- Click **OK**. The Web Console user interface appears.
- Optionally bookmark the Web Console URL as a favorite site in your Web browser.

Step 39 Install the Integration Packages (Optional)

The Integration Packages application integrates ControlCenter into management framework applications such as HP OpenView Network Node Manager, HP OpenView Vantage Point Operations, Micromuse Netcool/OMNIBus, Tivoli NetView, and Tivoli Enterprise Console.

Each third-party Integration Package expands the functionality of these frameworks by providing support for ControlCenter-managed storage resources. By processing EMC-specific events in the form of SNMP traps, Integration Packages provides the ability to launch available EMC-specific tools.

For details about the Integration Packages application, see *EMC ControlCenter Integration Packages Product Guide*.

To install the Integration Packages application, follow these steps:

- ◆ 39.1 *Verify the host setup* on this page.
- ◆ 39.2 *Download and install the Integration Packages application* on this page.

39.1 Verify the host setup

Verify that the target host has a supported third-party Framework installed. The Framework does not have to be running.

39.2 Download and install the Integration Packages application

Download the application as follows:

- a. Enter the following URL in a Web browser window:

`http://<ECCServerHostname-OR-IPAddress>:30000`

- If your browser *has* a Java virtual machine (JVM) that can run the installation program, the installation program displays the *Console installation home page*.

Continue with the next step.

- If your browser *does not have* a JVM that can run the installation wizard, the Web page displays a message panel that explains how to download and install a valid JVM. Do the following:
 1. Download a JVM from <http://java.sun.com> by clicking on the link **Sun's Java website** on the message panel. EMC recommends that you install the latest version of the JVM.
 2. After the JVM is installed, click the link **EMC ControlCenter Download Page** in the message panel.
 3. Continue with the next step.
- b. Click the **Installation** option. Then click **Integration Packages**.

If this is the first time installing the Integration Packages on this host, the Security Warning dialog box appears.
- c. Click **Yes** to continue.
- d. Click **Next** in the welcome screen.
- e. Select the destination directory where you want to install the Integration Packages (the default is `C:\ecc\InstallIntPkg`). Then click **Next**.

When the progress bar reaches 100 percent, the Installation Summary message indicates if the installation was successful.
- f. Click **Finish** to exit the installation and close any unneeded Web browser windows.

Refer to *EMC ControlCenter 5.2 Integration Packages Product Guide* for detailed information on starting and configuring the application.

Step 40 Install Performance Manager (Optional)

To install and run Performance Manager, follow the steps in this section.

Be sure to read the overview of *Plan for Workload Analyzer Archiver* on page 58 before you install Performance Manager.

- ◆ 40.1 *Ensure your account has the proper privileges on this page.*
- ◆ 40.2 *Ensure the Performance Manager license key is enabled on this page.*
- ◆ 40.3 *Verify the host setup on this page.*
- ◆ 40.4 *Install Performance Manager on page 178.*
- ◆ 40.5 *Prepare to start Performance Manager on page 179.*
- ◆ 40.6 *Start Performance Manager on page 179.*
- ◆ 40.7 *Connect additional Repositories to Performance Manager (optional) on page 179.*

40.1 Ensure your account has the proper privileges

When installing Performance Manager:

- ◆ If the target host is running Windows XP, you must log on as *Administrator*.
- ◆ If the target host is running any other supported Windows operating system (refer to *EMC ControlCenter Support Matrix* on Powerlink for details), you must log on to an account with administrative privileges (an account in the Administrators group).

40.2 Ensure the Performance Manager license key is enabled

Ensure the Performance Manager license key was entered through the Console (this must be done only once, using one Console). Refer to *Step 37: License the Desired Applications* on page 171 for details.

40.3 Verify the host setup

Verify that the target host:

- ◆ Is running the Windows operating system, and has the required amount of memory and processor speed (refer to *EMC ControlCenter Support Matrix* on Powerlink for details).

- ◆ Has access to the ControlCenter Repository host through TCP/IP.
- ◆ Uses DNS to resolve names and IP addresses.
- ◆ Has the ControlCenter installation tools installed. Refer to *Step 26: Install the Installation Tools on the Target Host* on page 116 for details.

40.4 Install Performance Manager

You will need the ControlCenter installation CDs to complete this procedure unless you are installing from a shared folder.

- a. If the installation wizard is already running, skip this step and continue with step b.
 1. Double-click the *Start ECC Install* desktop icon to start the ControlCenter installation wizard.
The installation wizard displays a warning about disabling antivirus software that might be running on the target host. Disable antivirus software, if necessary. Then click **OK**.
 2. Select **Specify existing ECCRepository**.
 3. Enter the Repository host name and port number.
 4. Click **Next**.
- b. Select **Performance Manager** from the Available Components list. Click **Add** to add it to the Selected Components list.
- c. Click **Next** to begin the installation.
If you are using the installation CDs, the installation wizard prompts you to insert ControlCenter installation CD #4.
- d. Insert ControlCenter installation CD #4, and then click **OK**. (If you are installing from a shared folder, there is no need to perform this action because the installation program automatically locates the necessary installation files in the shared folder.)

When the progress bar reaches 100 percent, the Performance Manager installation is complete.

If there are additional components to install, the installation program displays a message that asks if you would like to install more components on the target host.

- e. Do one of the following:
 - Click **Yes** to continue installing components on the target host. The installation program displays a list of components, based on the components previously installed.
 - Click **No** to exit the installation.

40.5 Prepare to start Performance Manager

Before starting Performance Manager, do the following:

- a. Ensure that you have installed Workload Analyzer Archiver (refer to *Plan for Workload Analyzer Archiver* on page 58 for details), which processes and stores data for Performance Manager.
- b. Ensure that the **EMC ControlCenter Performance Manager Automated Reports** service is started on the ECC Server host.

40.6 Start Performance Manager

Do one of the following to start the application on the host where Performance Manager is installed:

- ◆ From Windows Start menu, select **Programs, EMC, EMC ControlCenter, Performance Manager**.
- ◆ If the Console is also installed on the host:
From the Console **File** menu, select **Launch, Performance Manager**.

40.7 Connect additional Repositories to Performance Manager (optional)

If your installation has more than one ControlCenter Repository, you can have Performance Manager connect to multiple Repositories (even though its original installation allows only one Repository connection).

On the host where Performance Manager is installed, do the following to add Repository connections:

- a. From the Windows **Start** menu, select **Oracle, Home, NetworkAdministration, Net8 Assistant**.
The system displays the Net8 Assistant main window.
- b. Expand **Local**. Then select **Service Naming**.

- c. From the **Edit** menu, select **Create**.

The system displays the Net Service Name Wizard Welcome screen.

- d. Enter a meaningful name for the Repository connection (such as the Repository hostname). Then click **Next**.

The system displays the Net Service Name Wizard Page 2 of 5: Protocol screen.

- e. Accept the default selection, TCP/IP (Internet Protocol). Then click **Next**.

The system displays the Net Service Name Wizard Page 3 of 5: Protocol Settings screen.

- f. Enter the fully qualified hostname for the Repository host and accept the default port number. Then click **Next**.

The system displays the Net Service Name Wizard Page 4 of 5: Service screen.

- g. Select **(Oracle8 or Previous) SID** and enter `rambdb` in the text box. Then click **Next**.

The system displays the Net Service Name Wizard Page 5 of 5: Test screen.

- h. Click **Finish** (without running a test, because if you run a test from here, it will fail due to password incompatibility — you can test the connection later in this procedure).

The Net Service name for the Repository appears in the Service Naming folder of the Net8i Assistant.

- i. From the **File** menu, select **Save Network Configuration**.

- j. From the **File** menu, select **Exit** to close the Net8i Assistant.

- k. Right-click the `WLA.ini` file icon in one of the following locations and select **Properties**:

- Windows NT:

`C:\WINNT\<username>\Application Data\WLA`

- Windows 2000, XP, and 2003:

`C:\Documents and Settings\<username>\Application Data\WLA`

where *<username>* is the Windows user ID.

Note: If you do not see Application Data folder at the above location then enable “Show hidden files and folders” field in Windows Explorer -> Tools -> Folder Options -> View tab.

- l. Clear the **Read-only** file attribute. Then click **OK**.
- m. Open the `WLA.ini` file in a text editor.
- n. Copy the `Alias` and `UserId` lines and paste them directly under the last `UserId` line.
- o. Replace the `Alias` host with the same Net Service Name that you added to the Net8i Assistant.
- p. Repeat the last two steps for each Repository to be added.
- q. Save and close `WLA.ini`.
- r. Right click the icon for `WLA.ini` and select **Properties**.
- s. Select the **Read-only** file attribute (so it appears checked). Then click **OK**.
- t. Open Performance Manager.
If the connection to the additional Repositories was successful, the **Select Repository** dialog box opens, which contains a list of all the Repositories you have added.
- u. Select the Repository to use for this session. Then continue using Performance Manager.

Step 41 Install StorageScope (Optional)

To install StorageScope, follow these steps:

- ◆ 41.1 *Verify the host setup* on this page.
- ◆ 41.2 *Install StorageScope* on this page.
- ◆ 41.3 *Start StorageScope Service* on page 184.

41.1 Verify the host setup

Verify that the host:

- ◆ Has access to the ControlCenter Repository host through TCP/IP.
- ◆ Uses DNS to resolve names and IP addresses.
- ◆ Has the ControlCenter installation tools installed. Refer to *Step 26: Install the Installation Tools on the Target Host* on page 116 for details.

Firewall Requirement

If one or more StorageScope sites are to access StorageScope through a firewall, ensure that the default port 8080 is left open so StorageScope communications can occur through the firewall.

41.2 Install StorageScope

You will need the ControlCenter installation CDs to complete this procedure unless you are installing from a shared folder.

- a. If the installation wizard is already running, skip this step and continue with step b.
 1. Double-click the **Start ECC Install** desktop icon to start the installation wizard.
 2. Select **Specify existing ECCRepository**.
 3. Enter the Repository hostname and port number.
 4. Click **Next**.
- b. Select **StorageScope** from the Available Components list. Click **Add** to add StorageScope to the Selected Components list.
- c. Click **Next** to begin the installation.

The installation program displays the data entry screens for StorageScope.

- d. Enter the StorageScope installation data shown in Table 55.

Table 55 StorageScope Installation Notes

Required Field	Description
<i>Select Primary Network Name for StorageScope Server</i>	The default channel at the StorageScope server host for communication with other hosts.
<i>Enter StorageScope Server Port Number</i>	The StorageScope server listening port number. <i>Default: 8080</i>
<i>Enter License Key for StorageScope Component</i>	The license key provided with your purchase of StorageScope.
The following fields appear only when the target host is multihomed.	
<i>Select ECC Server Network Name for StorageScope Communications</i>	Alternate channels at the StorageScope server host for communication with other hosts.

- e. Click **Next**.

The installation wizard prompts you to insert ControlCenter installation CD #1 (unless you already have ControlCenter installation CD #1 in the CD-ROM drive).

- f. Insert ControlCenter installation CD #1 (unless it is already in the CD-ROM drive) then click **OK**.

When the progress bar reaches 100 percent, the StorageScope installation is complete.

If there are additional components to install, the installation program displays a message that asks if you would like to install more components on the target host.

- g. Respond to the prompt as follows:

- Click **Yes** to continue installing components on this host. The installation program displays a list of components, based on the components previously installed.
- Click **No** to exit the installation.

41.3 Start StorageScope Service

Do the following to start StorageScope.

- a. Ensure that the ECC Server and Repository are installed and running.
- b. From the **Start** menu, select **Settings, Control Panel**.
- c. Open **Administrative Tools**, and then select **Services**.
- d. Right-click **EMC ControlCenter StorageScope** and select **Start**.

41.4 Launch StorageScope

To access StorageScope by using your browser, enter one of the following sites:

`http://<storagescope_host_name>:<storagescope_port_number>`

or

`http://<storagescope_host_name>:<storagescope_port_number>/sts`

Where:

- ◆ `storagescope_host_name` is the name of the host on which StorageScope is installed.
- ◆ `storagescope_port_number` is the number of the port on the StorageScope host through which you communicate with StorageScope. The default port number is 8080.

To launch StorageScope from the ControlCenter:

1. Select ECC Administration in the task bar.
2. On the Reports menu, select Launch StorageScope. StorageScope launches in a browser window.

Performance and Scalability Guidelines: Active StorageScope Sessions

Limit the number of active StorageScope sessions to 5 during peak ControlCenter use.

A StorageScope session is considered “active” if it is being used by the user to request reports, chart, and so on. If you must have more than 5 StorageScope sessions active during peak usage, contact EMC Customer Support for assistance.

Step 42 Install StorageScope API (Optional)

Using StorageScope API, users can create applications (such as reporting tools) that use the StorageScope interface. Install StorageScope API only if you plan to create such applications. For information about how to use StorageScope API, refer to the *EMC ControlCenter StorageScope API* book.

Important: StorageScope API is useful only to advanced users who want to create additional reporting functionality. Most users should skip this step.

Important: StorageScope API can only be installed on the Repository host. StorageScope API will not appear in the *Available Components* list on a host that does not have the Repository installed.

Follow these steps to install StorageScope API:

- a. If the installation wizard is already running, skip this step and continue with step b below.
 1. Double-click the **Start ECC Install** desktop icon.
 2. Select **Specify existing ECCRepository**.
 3. Enter the Repository hostname and port number.
 4. Click **Next**.
- b. Select **StorageScope API** from the Available Components list. Click **Add** to add it to the Selected Components list.
- c. Click **Next** to begin the installation.

The installation program displays a message that asks you to insert ControlCenter installation CD #2 into the CD-ROM drive.

- d. Insert ControlCenter installation CD #2. Then click **OK**.

When the progress bar reaches 100 percent, the installation is complete.

If there are additional components to install, the installation program displays a message that asks if you would like to install more components on the target host.

- e. Respond to the prompt as follows:
- Click **Yes** to continue installing components on this host. The installation program displays a list of components based on the components previously installed.
 - Click **No** to exit the installation.

Step 43 Install the SupportTools (Optional)

The ControlCenter SupportTools component contains the EMC ControlCenter Log Utility (ELU), a Windows-based stand-alone utility that provides centralized, logical access for ControlCenter log files, and other files related to monitoring ControlCenter operations.

You can install the SupportTools component on any host *except* the host where the ECC Server resides (because the SupportTools are already downloaded to the ECC Server host as part of the ECC Server installation).

The ELU's *expert mode* allows you to view, analyze, and distribute information from the following *managed files*:

- ◆ ControlCenter log files on the ECC Server, Store, ControlCenter Console, and agent hosts
- ◆ ControlCenter Repository log and backup files
- ◆ StorageScope configuration application and logs
- ◆ SYMAPI logs
- ◆ ESNAPI logs
- ◆ Host information files
- ◆ Installation log files
- ◆ Agent log files
- ◆ Workload Analyzer Archiver log files

With the Log Utility, you can also generate host information (on Windows machines) and collect host information generated outside the Log Utility. Additionally, you can execute remote predefined commands for EMC's Solutions Enabler and PowerPath.

For information on using the Log Utility, see the *Log Utility Online Help*.

You will need the ControlCenter installation CDs to complete this procedure unless you are installing from a shared folder.

- a. If the installation wizard is already running, skip this step and continue with step b.
 1. Double-click the **Start ECC Install** desktop icon to start the installation wizard.
 2. Select **Specify existing ECCRepository**.
 3. Enter the Repository host name and port number.
 4. Click **Next**.

- b. Select **SupportTools** from the Available Components list and click **Add** to add SupportTools to the Selected Components list.
- c. Click **Next**.
- d. Insert ControlCenter installation CD #4 into the CD-ROM drive.

A progress bar appears. When the progress bar reaches 100 percent, the component installed successfully.

Important: At this point, the installation wizard might display a warning indicating you must reboot the target host to complete the installation. If this is the case, EMC recommends that you reboot the target host as soon as possible.

Step 44 Install the EACLI Client (Optional)

The EACLI client provides the framework for all ControlCenter command line interfaces (CLIs). You install and invoke the EACLI client to access Storage Provisioning Services (SPS) CLI commands (refer to *EMC ControlCenter Storage Provisioning Services CLI Reference Guide* for details on using SPS CLI commands).

To install the EACLI client:

1. Ensure that the ECC Server is running.
2. Ensure that you have entered the Automated Resources Manager (ARM) license key (refer to *Step 37: License the Desired Applications* on page 171 for details). If you must enter the ARM license key, stop and restart the **EMC ControlCenter ECCAPI Server** service after entering the key, to enable functions associated with the license.
3. On the host where you plan to run the CLI, ensure that Java runtime environment (JRE) version 1.4.2 or later is installed and included in the PATH.
4. Insert ControlCenter installation CD #1 (unless it is already in the CD-ROM drive).
5. Change to the following directory (which resides in the root directory of CD #1):

```
ControlCenterCLI
```

6. Do one of the following to install the EACLI client:
 - **Windows:** Run the following batch file:
`eacli_install.bat`
 - **UNIX:** Run the following C shell script at the xhost Console:
`eacli_install.csh`

You are now ready to access SPS CLI commands on the target host.

Uninstalling EACLI

To uninstall the EACLI client:

- ◆ **Windows:** From Add/Remove Programs, select **EMC ControlCenter EACLI Client**.
- ◆ **UNIX:** Change to the root directory (`cd /`) and run the following command:
`java -jar <EACLI_INSTALL_DIR>/_uninst/uninstall.jar`



Quick check: Installation status

Before continuing with the installation, review the items in this section to verify the installation status. You might want to click the **Installed Components** button in the installation wizard to check the list of installed components and products.

◆ Components installed to this point:

- *Repository*, from the ControlCenter installation CDs (or a shared folder).
- *ECC Server*, from the ControlCenter installation CDs (or a shared folder).
- *EMC Solutions Enabler* (made available for remote deployment, from the Solutions Enabler CDs or a shared folder).
- *Store*, from the ControlCenter installation CDs (or a shared folder).
- *Other components or products*, such as the Master Agent and WebConsole Server, using the ControlCenter installation CDs (or a shared folder).
- *At least one ControlCenter Console*, using the the ControlCenter installation CDs or the Console Install Wizard in Internet Explorer or Netscape.

◆ What's next?

- Deploy Master Agents on *all hosts* to be monitored and managed through ControlCenter.

◆ What *required* tasks are ahead?

- Deploy agents on agent hosts, using the ControlCenter Console.
 - Finish setting up application agents (required only for a subset of agents).
 - Perform initial discovery.
-

ControlCenter *agents* are programs that run on hosts to control, collect data from, and monitor the health of resources in your storage network. ControlCenter commands are passed from the Console to the ECC Server, and then for execution to the agents through TCP/IP.

This section describes how to deploy ControlCenter agents on hosts and perform initial discovery of your storage environment.

Refer to *EMC ControlCenter 5.2 Planning and Installation Guide, Volume 2 (MVS Agents)* for information about planning and deploying MVS agents.

◆ Step 45: Deploy and Start Master Agents	192
◆ Step 46: Deploy Open Systems Agents	210
◆ Step 47: Finish Setting Up Agents	223
◆ Step 48: Enable Access to Symmetrix Arrays	224
◆ Step 49: Allow Automatic Discovery to Complete	227
◆ Step 50: Perform Assisted Discovery	228
◆ Step 51: Discover connectivity devices	237
◆ Step 52: Back Up ControlCenter (Optional)	238

Step 45 Deploy and Start Master Agents

You must deploy a Master Agent on each host to be monitored by other ControlCenter agents. A Master Agent must be deployed and running on a target host before any other agents can be deployed on that host.

Perform the following steps to deploy and start the Master Agent:

- ◆ 45.1 *Log on with the proper privileges* on this page.
- ◆ 45.2 *Deploy Master Agents* on this page.
- ◆ 45.3 *Ensure Master Agents have the required rights (Windows only)* on page 206.
- ◆ 45.4 *Start Master Agents* on page 207.

45.1 Log on with the proper privileges

Ensure that you are logged on to the target host for Master Agent installation with the necessary privileges:

- ◆ *Windows*: Log on with an account that is a member of the local Administrators group.
- ◆ *UNIX*: Log on with an account that has `root` privileges.

45.2 Deploy Master Agents

Use one of the following methods to deploy the Master Agent on each host where ControlCenter agents are to be deployed.

Important: EMC highly recommends using a shared folder (or, in the case of UNIX, an NFS-mountable disk) to deploy the Master Agent, especially if you plan to run ControlCenter agents on many hosts. Instead of moving the installation CDs from host to host, you can map a drive to the shared location on each host and deploy the Master Agent from there.

- ◆ Deployment from a shared folder:
 - For Windows, perform the steps in *Step 27: Set Up Shared Folder Installation (Recommended)* on page 120.
 - For UNIX systems (AIX, HP-UX, Linux, and Solaris), copy the contents of ControlCenter installation CD #1 to a directory on an NFS-mountable disk. Instead of using the CD mount point, specify the NFS mount point.

- ◆ Local deployment on Windows using the ControlCenter installation wizard (refer to *Deploy the Master Agent on Windows (GUI)* on this page).
- ◆ Local deployment on Windows using the command line (refer to *Deploy the Master Agent on Windows (Command Line)* on page 195).
- ◆ Local deployment on AIX, HP-UX, Linux, or Solaris with shell scripts, using the procedure in *Deploy the Master Agent on UNIX (Command Line)* on page 196.
- ◆ Download and deployment from a web site for use with BMC Software Common Install. Refer to *Deploy the Master Agent with BMC Software Common Install* on page 201.

Deploy the Master Agent on Windows (GUI)

Follow the steps in this section to deploy the Master Agent on Windows using a graphical interface. If the installation wizard is already running, you can skip steps a and b.

- a. Ensure that the ControlCenter Installation Tools are installed on the host (refer to *Step 26: Install the Installation Tools on the Target Host* on page 116 for details).
- b. Double-click the **Start ECC Install** desktop icon to start the installation wizard.
- c. In the installation wizard, select **Specify existing ECCRepository**.

If the target host can connect to the Repository, or if the Repository was connected at any previous ControlCenter installation on the target host, the installation wizard automatically gathers required information about the Repository (such as the host name and port number).

No Repository Connection?

The installation wizard displays the *Warning* dialog box to indicate that the installation program could not connect to the Repository host. Click **Continue** in the *Warning* dialog box. Then enter the **Repository Hostname** and **Port Number**.

- d. Click **Next**.

The installation wizard displays the Available Components list.

- e. Select **MasterAgent** from the Available Components list. Click **Add** to add it to the Selected Components list.

- f. Click **Next**.

The installation wizard displays the Data Entry screen.

- g. Enter the **Master Agent Port Number**, using information from *Enter information required for Master Agent deployment, using the field descriptions in Table 11 as a guide* on page 55.

No Repository Connection?

If the target host does not have connectivity to the Repository, the installation wizard also requests the following (enter values from): *Enter information required for Master Agent deployment, using the field descriptions in Table 11 as a guide* on page 55.

- ◆ ECC Server Component Name
- ◆ ECC Server Port Number
- ◆ ECC Server Network Name for Master Agent Communications

- h. Click **Next**.

When deploying the Master Agent from CD, the installation wizard prompts you to insert ControlCenter installation CD #1 in the CD-ROM drive. When deploying from a shared folder, the wizard skips the prompt and begins deployment.

When the progress bar reaches 100 percent, the Master Agent has installed successfully. A message appears asking if you want to install more products on the target host.

- i. Respond to the prompt as follows:

- Click **Yes** to continue installing components on this host. The installation program displays a list of components based on the components previously installed.
- Click **No** to exit the installation.

The values entered during this installation procedure, as well as in previous ControlCenter installations on this host, will persist for future installations if the Repository was connected to the host when the values were entered.

Deploy the Master Agent on Windows (Command Line)

Use the command line to deploy the Master Agent on a Windows host if the display cannot support a minimum of 256 colors, which is required to run the EMC ControlCenter installation GUI.

Note that this program does not add the Master Agent to the **Add/Remove Programs** menu in the Windows Control Panel (as is done with the GUI installation procedure described in *Deploy the Master Agent on Windows (GUI)* on page 193). To uninstall the Master Agent after installing it through the command line, refer to *Uninstall Only the Master Agent (Using the Command Line)* on page 283.

- a. Do one of the following:
 - If you are deploying the Master Agent from CD, insert ControlCenter installation CD #1 in the CD-ROM drive.
 - If you are deploying the Master Agent from a shared folder, ensure that a drive is mapped to the root directory for the shared folder (refer to *Step 27: Set Up Shared Folder Installation (Recommended)* on page 120 for details).
- b. In a command window, change the current directory to the CD-ROM drive (for example, D:) or the drive that is mapped to the shared folder, depending on your original installation method.
- c. Enter the following command:

```
install_master.bat
```

The program prompts you for the ControlCenter root directory and indicates that C:\ECC is the default.

- d. Enter the directory where you intend to deploy ControlCenter agents. Accept the default of C:\ECC or enter another directory, bearing the following in mind:
 - Do not include spaces in the path (for example, the following directory path is *not* valid: C:\Program Files\ecc).
 - Do not specify universal naming convention (UNC) paths (for example, the following directory path is *not* valid: \\hostX\ECC).
 - Do not specify only the root directory of a drive (for example, the following directory path is *not* valid: C:\).
- e. Enter the requested system data.

```
ECC Server's Hostname or IP address[]:
```

- If you enter the hostname, the IP address is not required. EMC recommends that you enter the hostname.
- If you enter an IP address, you will be prompted to enter the ECC Server hostname (refer to Table 51 on page 136 for the value).

Important: The ECC Server hostname *must match exactly* the hostname, minus the `svr` prefix, specified on the `ECCSERVER_NAME` parameter in the following file on the ECC Server host:

```
Install_Root\installIGS520.answers
```

For example, the correct value in the following entry is `myHost`:
`ECCSERVER_NAME=svrmyHost`

- f. Accept the defaults for the following prompts, or provide alternate information if you customized the ports originally.
 - ECC Server Port [5799]:
 - Master Agent's listening port [5798]:

The program displays the following message:

```
Are these values acceptable [Y|N|Q]:
```

- g. Enter **Y** to accept the entries. (If you enter **N**, the program will repeat the prompts for installation values. If you enter **Q**, the program will exit without performing any further actions.)
 The installation extracts files and writes configuration files.
- h. Press **ENTER** to exit the installation.
- i. Continue deploying Master Agents on all hosts that are to be monitored and managed through ControlCenter.

Deploy the Master Agent on UNIX (Command Line)

Follow these steps when deploying the Master Agent on UNIX systems (AIX, HP-UX, Linux, and Solaris).

Important: If deploying from a shared location, copy the contents of ControlCenter installation CD #1 to an NFS-mountable disk. Then create the mount point for that disk.

- a. Create the mount point for deployment and mount the install media as follows.
 - **Linux:** Insert ControlCenter installation CD #1 into the CD-ROM drive. If the CD does not automount, enter the following commands in sequence to create the mount point for the CD and mount it:

```
mkdir <mount_point_directory>
```

Example: `mkdir /mnt/cdrom`

```
mount <cdrom_device> <mount_point_directory>
```

Example: `mount /dev/cdrom /mnt/cdrom`

If you get the following error message:

- **Solaris:** Ensure that the `vold` daemon is running so the CD-ROM will be automounted when inserted in the CD-ROM drive. Then insert ControlCenter installation CD #1 into the CD-ROM drive.
- **AIX:** If not already created, create the mount point for the installation CD-ROM.

```
mkdir /cdrom
```

Then insert ControlCenter installation CD #1 into the CD-ROM drive. Mount the CD-ROM using the following command.

```
mount -v cdrfs -p -r <device_name> <mount_point>
```

Example: `mount -v cdrfs -p -r /dev/cd0 /cdrom`

- **HP-UX:**

Because the standard mount and unmount HP-UX commands do not support Rockridge extensions, EMC suggests using the portable file system (PFS) to create the CD-ROM mount point.

1. Create the following file: `/etc/pfs_fstab`

2. Enter the following line in the `pfs_fstab` file:

```
/dev/dsk/cXtYdZ /cdrom pfs-rrip xlat=unix,soft 0 0
```

In the line above, replace X, Y, and Z with the controller, target, and LUN of the CD-ROM device.

3. Start the following daemons.

```
pfs_mountd &
pfsd &
```

If the daemon locations are not in the path, they might be located in the following subdirectory:

```
/usr/sbin
```

4. Create the mount point.

```
mkdir /cdrom
```

5. Insert ControlCenter installation CD #1 into the CD-ROM drive.
6. Mount the CD-ROM, using the following command:

```
pfs_mount /cdrom
```

An alternate method to creating a `pfs_fstab` entry is to mount the CD as follows: `pfs_mount -t rrip /dev/dsk/cXtYdZ /cdrom`

- b. While logged in as root, enter the following command, specifying the mount point as an argument.

```
install_master.sh <mount_point>
```

For example:

```
./install_master.sh /cdrom
```

The installation script prompts for the root ControlCenter installation directory.

```
Please enter ECC root directory[]:
```

- c. Enter the directory where you intend to install all ControlCenter agents. Accept the default of `/usr/ecc` or enter another directory path and name, bearing the following in mind:

- Do not include spaces in the path (for example, the following directory path is not valid: `/EMC Software/ecc`).
- Do not specify only the root directory (for example, the following directory path is not valid: `/`).

- d. Press ENTER. The program prompts you to create native installable images. If you want to deploy the Master Agent on more than one UNIX host, you can distribute the image to other hosts and use it to deploy the Master Agent on those hosts.

```
Do you want to create native installable images [Y|N]:
```

- e. Respond with one of the following:

- Enter **N** to continue the installation without creating images.

- Enter **y** to create the images. The program displays the following prompt:
Enter package output destination (enter full absolute path):
Enter the output path. Press ENTER. The program installs the package in the specified output destination.

f. Enter the requested system data.

ECC Server's Hostname or IP address[]:

- If you enter the hostname, the IP address is not required. EMC recommends that you enter the hostname.
- If you enter an IP address, you will be prompted to enter the ECC Server hostname (refer to Table 51 on page 136).

ECC Server's Hostname[]:

Important: The ECC Server hostname *must match exactly* the hostname, minus the `svr` prefix, specified on the `ECCSERVER_NAME` parameter in the following file on the ECC Server host:

`Install_Root\installIGS520.answers`

For example, the correct value in the following entry is `myHost`:

`ECCSERVER_NAME=svrmyHost`

g. Accept the default values for the following prompts (if correct):

ECC Server Port [5799]:

Master Agent's listening port [5798]:

The installation program does not validate the provided ECC Server hostname and port numbers. Ensure that you enter the correct values.

The program displays the following message:

Are these values acceptable [Y|N|Q]:

h. Respond with one of the following:

- **y**, to tell the installation program to write the configuration files with the specified values.
- **n**, to tell the installation program *not* to write the configuration files. The program will prompt you for new values.

- **q**, to quit the program without writing configuration files or prompting for new data.

If you enter **y**, and the operating system is HP-UX, Linux, or Solaris, the installation program displays the following:

```
Do you want EMC ControlCenter Master Agent to start on
reboot [Y|N]:
```

Because “autostart on reboot” for the Master Agent is not supported on AIX, the installation program does not display this question on AIX.

Respond with one of the following:

- **y**, to tell ControlCenter to start the Master Agent on reboot (ControlCenter updates the `rc.d` entries with the `eccmad` script, which starts and stops the Master Agent).
- **n**, to tell ControlCenter *not* to start the Master Agent on reboot.

If the following output is seen:

```
Step 1: Copy init script (eccmad) to /etc/init.d
+ done
```

```
Step 2: Create symbolic links for start scripts
ln: creating symbolic link `/etc/init.d/rc5.d/S99eccmad' to `/etc/init.d/eccmad':
No such file or directory
+ Add link /etc/init.d/rc5.d/S99eccmad ... ERROR rc=1
```

```
Step 3: Create symbolic links for stop scripts
ln: creating symbolic link `/etc/init.d/rc5.d/Kcmad' to `/etc/init.d/eccmad': No
such file or directory
+ Add link /etc/init.d/rc5.d/Kcmad ... ERROR rc=1
```

```
Done: error count = 2
```

```
Warning: Failed to configure start-on-reboot.
```

Then do the following:

1. Copy the EMC ControlCenter 5.2 installation CDs to a shared folder as described on Page 120.
2. Copy `setuprc.csh` from the V 5.2 SP4 ECC Server host `Install_Root/LinuxMA/` folder.
3. Paste `setuprc.csh` into the shared folder in which you copied the installation CDs.
4. On the Linux host, create the mount point for the NFS-mountable disk and continue from Step b of this section.

The Master Agent is now installed.

- i. Continue installing the Master Agent on all hosts that are to be monitored and managed through ControlCenter.

Deploy the Master Agent with BMC Software Common Install

The Master Agent is available for use with BMC software in the form of a BMC Software Common Install package. The ControlCenter Master Agent Common Install package can be installed locally or deployed using BMC Software's Distribution Server product.

1. Download the following from BMC's software or FTP web site.
 - The BMC Software Common Install Engine (version 7.4.40) for the target platform. Each install engine is contained in an Electronic Product Download (EPD) that includes a self-extracting executable for Windows or a .tar file for UNIX.

Download this engine only if you plan to install the Master Agent on a local machine. The BMC Software Distribution Server has the capability to perform the installation on remote machines.

- The EMC ControlCenter Master Agent EPD (self extracting executable or .tar file).

Important: If you use WinZip to uncompress .tar files, use WinZip version 9.0 (other versions cannot uncompress the file correctly).

2. Extract the downloaded file to a local directory on the target host. The extracted contents should have the directory structure:

```
./bmc_products
  /Index
  /Install
  /Products
```

3. Move the downloaded Master Agent self-extracting executable or .tar file to the directory shown in step 2 and extract it. The extracted files and directories will overlay the install engine's Index and Products directories.
4. Run one of the following to start the install.
 - Microsoft Windows operating systems: setup.exe
 - UNIX operating systems: setup.sh

The Common Install engine requires a web browser to display its installation wizard. If no supported web browser is installed, you must start the installation in *Server Only* mode and connect to the install engine's web server from a machine with a supported web browser. Start the installation in *Server Only* mode with `setup.exe -serveronly` or `setup.sh -serveronly` and follow the on-screen instructions.

5. Click **Next** in the Welcome to the Installation Utility screen.
6. Select **Accept**, click **Next** in the Review License Agreement screen.
7. Select **Install products on this computer now** and click the **Next** button in the Selection Installation option screen.
8. Select **Typical**, click **Next** in the Select Type of Installation screen.
9. Enter or browse to the BMC Software Product Installation directory where PATROL is currently installed in the Specify Installation Directory screen.
10. In the Select the Products and Components to Install screen, expand the EMC ControlCenter folder, select **EMC ControlCenter Master Agent**. Then click **Next**.
11. In the ECC Root Directory screen, enter or browse to the root directory for ControlCenter installation. Then click **Next**.
12. In the Identify the ECC Server screen, enter the hostname or IP address of the host where the ECC Server resides. If you enter the IP address, you must enter the hostname on the next screen. Then click **Next**.
13. In the ECC Server Hostname screen, enter the network name of the host where the ECC Server resides. This screen displays only when you enter the IP address of the ECC Server host in the previous screen. Then click **Next**.
14. In the Identify the ECC Master Agent Listening Port screen, enter the Master Agent listening port number or accept the default. Then select a radio button indicating whether the Master Agent should automatically start on reboot or accept the default. Then click **Next**.

The Master Agent *start up on reboot* option is not available on AIX.

15. Review the Selections and Install screen, then click **Start install**.

The wizard displays the Installation Progress screen. Click the View Log button to display the install log. Click the Finish button to exit the installation.

16. Allow the installation to complete. Then click **Next**.

The wizard displays the Install Finish screen.

17. Ensure that the following prerequisites for ControlCenter Master Agent deployment are met.
 - BMC Distribution Manager is installed and configured for deployment on hosts where the Master Agent is to reside. Refer to the BMC documentation for details.
 - BMC Distribution Client is deployed to the target host(s).
 - Connection accounts and privileged account are created on the target host(s).
 - Distribution Profiles are in place for Windows and Unix on the target host(s).
 - System groups that contain the target host(s) are in place.
 - At least one of the following is installed on target host(s): PATROL 3.5 Agent, PATROL 3.5 Classic Console, PATROL 7 Central Operator for Windows, PATROL 7 RT Server, or PATROL 7 Console Server.
18. Extract the Master Agent EPD file to a directory on the host where Distribution Manager is installed (for example, C:\ecc_ma).

Important: If you use WinZip to uncompress .tar files, use WinZip version 9.0 (other versions cannot uncompress the file correctly).

The next steps will import the ControlCenter Master Agent components into the Distribution Manager Repository.

19. Click the Components tab in the Distribution Manager main screen.
20. Select the Components link and click **Import**. The Import Components dialog box appears.
21. Enter the full path (or browse) to the `bmc_products` directory created the .tar file was extracted (for example: C:\ecc_ma\bmc_products).

A tree of components that can be imported displays.

22. Expand the EMC ControlCenter folder and select **EMC ControlCenter Master Agent for <operating_system>** (5.2). Then click **OK**.
23. Click **Import** to import the selected component. When the import completes, click **Close**.
24. Click the **Collections** tab on the main Distribution Manager screen.
25. Click the **Selections** link and click **Add**. The Add Collection dialog box appears.
26. Enter a Collection name (for example: *ControlCenter Master Agent*) and click **Add**. A new link appears under the Collections list with the specified name.
27. Click the link with the collection name you specified. The program displays a collection screen in the right panel.
28. Click the **Components** tab on the collection screen. A list of components selected for this collection appears (it should be empty).
29. Click **Add**. A tree of all components that have been imported into the Distribution Manager appears.
30. In the component tree expand the EMC ControlCenter folder, select **EMC ControlCenter Master Agent for <Operating System>** (5.2), and then click **OK**. The component is added to the collection's component list.
31. Click the **Configurations** tab on the collection screen to display the collection Configurations screen.
32. Click **Add** to open the Add Configuration screen.
33. Enter a configuration name and description. Click **Next**.
34. Click **Next** on the following screen to begin answering questions specific to EMC ControlCenter Master Agent deployment.

There are no uninstall screens/questions for the Windows Master Agent.

35. Schedule the ControlCenter Master Agent distribution by first selecting the Distribution tab in Distribution Manager.
36. Click **Add**. The Add Distribution Set dialog box appears.

37. Enter a Distribution set name (for example, EMC ControlCenter Distribution) and click **Add**. This causes the newly added distribution set's properties to display in the right panel.
38. Click the **Distribution's Items** tab in the right panel.
39. Click **Add Item** to display the Add distribution Item dialog box.
40. Select the name of the collection you created from the Collection menu.
41. Select the name of the configuration you created from the Configuration menu.
42. Select the name of the System group where you want to deploy your collection/configuration.
43. Click **Add** to finish creating the distribution set.
44. Click the **Distribution's Schedule** tab in the right panel to display the Schedule screen.
45. Click **Add Schedule**.
46. Select either **Distribute immediately** or **Schedule distribution** and enter start date and start time information for when to distribute.
47. Click **Install**.
48. Click **Add** to complete the scheduling of the distribution.
49. Review deployment status and history by clicking the **Distribution Manager's Reports** tab.
50. Click the **Active** tab to view the status of scheduled deployments currently under way.
51. Select a distribution name from the Distribution menu to view that active distribution's status. The status of the distribution for each host will be displayed.
52. Click the **History** tab to view the status of distributions that have completed.
53. Select a distribution name from the Distribution menu to view the completed distribution's status. The status of the distribution for each host will be displayed.
54. Click **installation.log links** to view the installation log file for specific hosts.

Deploy the Master Agents with Sudo

To install the Master Agent with sudo:

1. Create a new file named `instMA.sh`. This shell script should contain two lines:

```
----
#!/usr/bin/sh
<CD MOUNT POINT>/install_master.sh <CD MOUNT POINT>
----
```

Where `<CD MOUNT POINT>` is the directory to which you have mounted ControlCenter 5.2.0 CD1.

For security, `instMA.sh` should be owned by root, and have `-rwxr-xr-x (755)` permission settings.

2. Grant sudo permission to this script.
3. To deploy the master agent, run this script with sudo. The Master Agent install should proceed.

45.3 Ensure Master Agents have the required rights (Windows only)

When a Master Agent is deployed, the **EMC ControlCenter Master Agent** service inherits the security settings of the user account that is used to start the service. In turn, all ControlCenter agents that run on the same host inherit those security settings. Because some functions performed by those agents require administrative privileges, you must ensure that the Master Agent starts with administrative privileges (for example, using the *Administrator* or *Domain Administrator* account) so they can be propagated other agents, using the following procedure.

Be aware that there are security risks associated with running applications under accounts with administrator privileges.

- a. Select **Start, Settings, Control Panel, Administrative Tools, Services**.
- b. Ensure that all application agents running on the host are stopped (using the ControlCenter Console).
- c. Stop the **EMC ControlCenter Master Agent** service (if it is not already stopped).
- d. Right-click the **EMC ControlCenter Master Agent** service and select **Properties**.

- e. Click the **Log On** tab and select **This account**.
- f. Enter the username and password required to grant the Master Agent administrative privileges. Ensure that the account has the privileges *Act as part of the operating system* and *Back up files and directories*.
- g. Stop and restart the Master Agent and all other agents running on the host, to activate the new security settings.

45.4 Start Master Agents

Important: A Master Agent must be deployed and running on a target host before any other agents can be deployed on that host.

Depending on the operating system, do one of the following to start the Master Agent:

Windows

Ensure that you are logged on to a user account that is in the Administrators group. Then, do the following from the Windows GUI:

1. From the **Start** menu, select **Settings, Control Panel**.
2. Open **Administrative Tools, Services**.
3. Right-click **EMC ControlCenter Master Agent** and select **Start**.

Although the Master Agent service is set to Automatic for Startup Type at reboot, you must manually start this service after its initial deployment (the service will start automatically at the next reboot after the Master Agent is deployed).

UNIX

Ensure that you are logged on to an account with `root` privileges.

Then, enter the following command:

```
<Install_Root>/exec/start_master.csh
where, <Install_Root> is the ECC infrastructure install
directory.
```

When you can see the target host in the Console *tree panel*, the Master Agent deployment is successful. You can now go on to install other agents on that host.

Sudo

1. To start the Master Agent with sudo, grant sudo permission to the `<MA_INSTALL_DIR>/exec/start_master.csh` script.
2. Run the `start_master.csh` script with sudo.

Once the Master Agent is running as root, all processes/agents it spawns inherit the root permissions, and run normally.



Quick check: Installation status

Before continuing with the installation, review the items in this section to verify the installation status. You might want to click the **Installed Components** button in the installation wizard to check the list of installed components and products.

◆ Components installed to this point:

- *Repository*, using the ControlCenter install CDs or a shared folder.
- *ECC Server*, using the ControlCenter install CDs or a shared folder.
- *EMC Solutions Enabler* (made available for remote deployment, using the Solutions Enabler CDs or a shared folder).
- *Store*, using the ControlCenter install CDs or a shared folder.
- *Other components or products* (such as the Master Agent and WebConsole Server), using the ControlCenter installation CDs (or a shared folder).
- *At least one ControlCenter Console*, using the Console installation program in Internet Explorer or Netscape.
- *Master Agents* on all hosts to be monitored and managed through ControlCenter.

◆ What's next?

- Push application agents to agent hosts, using the ControlCenter Console.

◆ What *required* tasks are ahead?

- Finish setting up ControlCenter agents (required only for a subset of agents).
 - Perform initial discovery.
-

Step 46 Deploy Open Systems Agents

This section describes how to deploy open systems agents and EMC Solutions Enabler (required for some agents to function properly—refer to *Deploying Solutions Enabler* on page 213 for details) using the Agent Administration Wizard in the ControlCenter Console.

Tip: View the “Using the Console” tutorial in the Documentation Library to learn about the Agent Administration Wizard.

The *Master Agent*, which controls the deployment, starting, and stopping of other ControlCenter agents, is required on each agent host. Before you begin, ensure that you have deployed the Master Agent on all hosts that require it, using *Step 45: Deploy and Start Master Agents* on page 192.

Using the Agent Administration Wizard

The Agent Administration Wizard guides you through the process of deploying agents. The wizard checks target hosts for:

- ◆ *Free disk space:* Determines if enough free disk space is available to deploy selected agents. This check is performed for all agents.
- ◆ *Prerequisite software:* Ensures that target hosts have the following (refer to *EMC ControlCenter Support Matrix* on Powerlink for version information):
 - EMC Solutions Enabler 6.0.x, for Common Mapping Agent, Storage Agent for Symmetrix, and Symmetrix SDM Agent
 - NaviCLI for Storage Agent for CLARiiON
 - Oracle for Database Agent for Oracle (Windows only)
 - ESSCLI for Storage Agent for ESS
 - EDM for Backup Agent for EDM
 - Java Runtime Environment (JRE) 1.4.2_01, for Storage Agent for CLARiiON MetaLUN support
 - Java Runtime Environment (JRE) 1.4.1 or higher, for Storage Agent for Invista support

Deploying Agents on Infrastructure Hosts

When deploying agents, keep in mind that only the following agents are supported for deployment on ControlCenter infrastructure hosts. The total number of these agents that can be deployed on an infrastructure host in combination depends on the number and size of managed objects and the host configuration.

- ◆ Common Mapping Agent
- ◆ Fibre Channel Connectivity (FCC) Agent
- ◆ Host Agent for Windows
- ◆ Integration Gateway
- ◆ Master Agent

- ◆ Storage Agent for CLARiiON (CLARiiON MetaLUNs are not supported when the agent is deployed on the ControlCenter Repository host)
- ◆ Storage Agent for HDS
- ◆ Storage Agent for HP StorageWorks
- ◆ Storage Agent for NAS
- ◆ Storage Agent for Symmetrix
- ◆ Symmetrix SDM Agent
- ◆ Workload Analyzer Archiver

Entering Required Licenses for Agents

To deploy certain agents, you must enter license keys using the ControlCenter Console (refer to *Step 37: License the Desired Applications* on page 171 for details), as shown in Table 56.

Table 56 License Key Requirements for ControlCenter Agents

Agent	Available with These License Keys
<i>Backup Agent for <system></i>	Automated Resource Manager or StorageScope
<i>Common Mapping Agent</i>	Open Integration Components (no license required), StorageScope
<i>Database Agent for Oracle</i>	Open Integration Components (no license key required)
<i>Fibre Channel Connectivity Agent</i>	SAN Manager or StorageScope
<i>Host Agent for <platform></i>	Open Integration Components (no license required), StorageScope
<i>Host Agent for Novell</i>	Automated Resource Manager or StorageScope
<i>Integration Gateway</i>	Open integration components (no license key required)
<i>Storage Agent for Centera</i>	Centera
<i>Storage Agent for CLARiiON</i>	CLARiiON Agent, SAN Manager, or Performance Manager
<i>Storage Agent for ESS</i>	StorageScope
<i>Storage Agent for HDS</i>	SAN Manager or StorageScope
<i>Storage Agent for HP StorageWorks</i>	SAN Manager or StorageScope
<i>Storage Agent for NAS</i>	Celerra Agent or StorageScope,
<i>Storage Agent for SMI</i>	StorageScope

Table 56 License Key Requirements for ControlCenter Agents (continued)

Agent	Available with These License Keys
<i>Storage Agent for Symmetrix</i>	Performance Manager, StorageScope, Symmetrix Manager or Optimizer
<i>Symmetrix SDM Agent</i>	SAN Manager or StorageScope
<i>Workload Analyzer Archiver</i>	Performance Manager

Checking Agent Disk Space

Use Table 57 to calculate required disk space for agent hosts.

Table 57 ControlCenter Agent Disk Space Requirements

Agent	Windows	AIX	HP-UX	Solaris	Linux
<i>Master Agent</i>	150 MB	102 MB ^a	119 MB ^a	124 MB ^a	102 MB ^a
<i>Backup Agent for EDM</i>				5 MB	
<i>Backup Agent for Legato NetWorker</i>	11 MB	21 MB	11 MB	6 MB	
<i>Backup Agent for TSM</i>	13 MB	33 MB	29 MB	8 MB	
<i>Backup Agent for VERITAS NetBackup</i>	11 MB	21 MB	11 MB	6 MB	
<i>Common Mapping Agent</i>	12 MB			6 MB	
<i>Database Agent for Oracle</i>	14 MB	40 MB	25 MB	18 MB	
<i>Fibre Channel Connectivity Agent^b</i>	21 MB	40 MB	23 MB	12 MB	
<i>Host Agent for <platform> (except Novell: 10 MB on Windows only)</i>	22 MB	28 MB	21 MB	14 MB	28 MB
<i>Integration Gateway</i>	7 MB			106 MB	
<i>Storage Agent for Centera</i>	127 MB				
<i>Storage Agent for CLARiiON</i>	12 MB	22 MB	11 MB	6 MB	
<i>Storage Agent for ESS</i>	9 MB				
<i>Storage Agent for HDS</i>	11 MB	19 MB	10 MB	5 MB	
<i>Storage Agent for HP StorageWorks</i>	11 MB				
<i>Storage Agent for Invista</i>	11 MB				
<i>Storage Agent for NAS</i>	17 MB				
<i>Storage Agent for SMI</i>	12 MB				

Table 57 ControlCenter Agent Disk Space Requirements (continued)

Agent	Windows	AIX	HP-UX	Solaris	Linux
<i>Storage Agent for Symmetrix</i>	28 MB	34 MB	22 MB	13 MB	
<i>Solutions Enabler</i>	43 MB	107 MB	149 MB	112 MB	
<i>Symmetrix SDM Agent</i>	10 MB	18 MB	10 MB	5 MB	
<i>Workload Analyzer Archiver</i>	30 MB				

- a. Includes space required for the native installable images.
- b. ESNAPI, used by FCC Agent to manage switches, needs 40 MB on Windows, and 60 MB on Solaris, HP-UX, and AIX.

Deploying Solutions Enabler

Refer to the *Solutions Enabler Installation Guide*, Host Specific Issues section for additional set up requirements that might be needed to insure successful use of Solutions Enabler.

Use one of the two methods described in this section to deploy EMC Solutions Enabler on the following:

- ◆ Hosts that run Storage Agent for Symmetrix or Symmetrix Agent for SDM (required).
- ◆ Hosts with databases and file systems to be discovered by Common Mapping Agent (required).
- ◆ Hosts with databases and file systems to be discovered by Database Agent for Oracle (required).
- ◆ Hosts with Symmetrix device groups to be discovered (optional).
- ◆ Hosts that run Storage Agent for SMI to monitor Symmetrix or CLARiiON arrays (required, with additional libraries are required—you must use *Method 2: Deployment using the Solutions Enabler CDs* on page 214).

Specifying the Root Deployment Directory

You can specify the root deployment directory for Solutions Enabler during its deployment, as follows:

- ◆ If Solutions Enabler was previously deployed on the target host, EMC recommends that you specify the same root deployment directory as the previous version. This minimizes the impact on existing SYMCLI scripts—you will not have to modify the PATH in those scripts to reference a new location.

- ◆ If Solutions Enabler was *not* previously deployed on the target host, specify your preferred deployment directory or accept the default, which is:

Windows: \Program Files\EMC\SYMCLI\bin

UNIX: /opt/emc

Keep in mind that when upgrading to Solutions Enabler 6.0.x from a previous version, you might still have to modify existing SYMCLI scripts to account for changes in the product resulting from the upgrade.

Method 1: Remote deployment through ControlCenter

Deploy Solutions Enabler using the same procedure used to deploy Open Systems agents (*Procedure for Deploying Agents* on page 217). You cannot use this method to deploy Solutions Enabler for use with Storage Agent for SMI.

Before you begin: Before using the ControlCenter Console to deploy Solutions Enabler, you must make it available during infrastructure installation (refer to *Step 30.5: Make Solutions Enabler available for remote deployment* on page 138 for details), stop all applications that use Solutions Enabler on the target host, and ensure that the `sympisrv` service is not running on the target host.

Important: If Solutions Enabler is already deployed on the target host and has a version that is less than the version to be deployed through ControlCenter, the existing copy will be removed and the new copy deployed to the desired location. If the existing version of Solutions Enabler is greater than or equal to the version to be deployed through ControlCenter, Solutions Enabler will not be listed as available for deployment.

Method 2: Deployment using the Solutions Enabler CDs

You must use this procedure when deploying Storage Agent for SMI to monitor Symmetrix or CLARiiON arrays. Components of Solutions Enabler required for monitoring those arrays with SMI Agent are not included when deploying Solutions Enabler through the ControlCenter Console.

Do the following to deploy Solutions Enabler using the Solutions Enabler CDs or a shared folder. See the Solutions Enabler documentation for details.

1. Insert the appropriate EMC Solutions Enabler CD (included with your ControlCenter package) in the CD-ROM drive on the host where Storage Agent for SMI is installed.

If you copied the Solutions Enabler CDs to a shared folder (refer to *Step 27: Set Up Shared Folder Installation (Recommended)* on page 120 for details), you can skip this step.

2. Start the Solutions Enabler installation wizard.
3. Select the installation folder for the `db`, `log`, and `config` directories, or accept the default. Then click **Next**.

`C:\Program Files\EMC\SYMAPI`

4. Select the installation folder for Solutions Enabler or accept the default. Then click **Next**.

`C:\Program Files\EMC\SYMCLI`

5. Select all the EMC Solutions Enabler library options. Click **Next**.
6. Select all the EMC Solutions Enabler deployment options. Then click **Next**.
7. Select **No** when prompted with the question: "Install shared libraries that will ONLY allow monitoring capability?" Then click **Next**.
8. Select **Yes** when prompted with the question: Please confirm, the EMC Full Solutions Enabler kit will be installed. Continue?
9. Select **Yes** when prompted with the question: The SIU Service will now be installed. Do you want to start the service?
10. Select **Yes** when prompted with the question: The SYMAPI server can be installed and started now or it can be installed from a command line at a later time. Install and start the SYMAPI server now?
11. Select **Yes** when prompted with the question: The storapid server can be installed and started now or it can be installed from a command line at a later time. Install and start the storapid server now?
12. Select **Yes** when prompted with the question: The cimserver server can be installed and started now or it can be installed from a command line at a later time. Install and start the cimserver server now?

13. Click **Finish** to complete the setup.

Tip: Simplifying Agent Deployment

To simplify agent deployment, especially for larger ControlCenter configurations, you can create user-defined groups that organize your hosts into more manageable units.

For example, if you create a user-defined group that contains all the hosts in a particular business unit, you can install agents on all those hosts with one Console operation (such as, right click on the folder that represents the group, and then select the menu option to install agents). You can also create subfolders, or subgroups, within your user-defined groups. You cannot create subgroups under any other folder type. All user-defined groups are distinguished by an orange dot in the folder icon.

This section describes only one example of how to organize managed objects through the Console to simplify agent deployment. For more information, refer to the information about creating user-defined objects and groups in the *Console Online Help*.

The following is an example of how to create a user-defined group and add members:

- a. Select the tree panel by clicking either an empty space in the tree panel (if you want to create a new group at the root directory) or on an existing group (if you want to create a new sub-group).

- b. Select **New** from the **Edit** menu, or right-click and select **New**, and then **Group**.

The Console displays a highlighted **New Group** folder in the tree panel.

- c. Type the name of the new group.
- d. Add members to the group (for example, hosts from the **Hosts** folder), without removing them from their current location, by copying and pasting them into the new group folder, dragging and dropping their objects into the folder, or using the CTRL and SHIFT keys while dragging a group or group object into the folder.

You can now run agent operations (such as install, upgrade, start, stop, patch deployment, and uninstall) on all hosts in that folder by selecting menu options from the folder in the Console tree panel.

Procedure for Deploying Agents

During this procedure for deploying agents with the Agent Administration Wizard, the wizard displays the following buttons, which you can select at any time.

Table 58 Agent Administration Wizard Buttons

Button	Function
Next	Proceeds to the next page
Cancel	Aborts the agent deployment
Finish	Remains greyed out until you reach the final wizard page
Help	Displays a help panel

Follow this procedure when deploying ControlCenter agents:

- Ensure that the Repository, ECC Server, and Store(s) are running.
- Launch and log in to the ControlCenter Console, using an account in the Administrators group.
- Right-click any managed object (for example, the **Hosts** tree folder) in the Console tree panel and select **Install** from the **Agents** submenu.

The Agent Installation page launches. The wizard displays a list of one or more hosts that are running the selected platform and their status, operating system version, release, and level.

If platforms with different operating system types and versions are selected, the wizard displays a list of all platforms available for agent deployment (in other words, platforms with Master Agents installed) in the Host tree folder. You can select only one platform type.

- Click the checkmark at the top of the host information table to select all hosts, or individually click the checkbox next to each host to select them individually. You can also click the eraser to clear the selection of one or more hosts.
- Click **Next**.

The wizard displays a list of all agents (and their versions) available for deployment on the previously selected host(s).

- f. Individually click the checkbox next to each agent to be installed. Click the eraser to clear the selection of one or more agents.

Important: Deploy only the required agents (use *Plan for Agents* on page 49 as a guide).

- g. Click **Next**. The wizard displays the Prerequisite Checks screen, which contains a table that lists agent/host compatibility.
 - If the Status field indicates **Passed** for all agents, the selected agents are ready for deployment. Continue with the next step.

Note that the agent checks might issue warnings about agent deployment. Warnings will not by themselves keep agent checks from passing—however, EMC recommends that you consider taking actions to resolve conditions stated in warning messages to avoid potential error situations in the future.

- If the Status field indicates that *not all* agent checks returned a status of **Passed**, some or all of the selected agents are *not* ready for deployment. Check that the agent configuration is correct, make any necessary updates, then re-try the operation. Continue with the next step when all agents indicate a status of Passed or Failed. (If you continue when one or more agents indicate a status of Failed, the Passed agents will be deployed, but not the Failed agents.) Correct or make updates to the Failed agents, then install those agents again.
- h. Click **Next**.

If deploying Solutions Enabler, the wizard prompts for the root Solutions Enabler directory. Refer to *Specifying the Root Deployment Directory* on page 213 for details. After you enter the root deployment directory, the wizard displays the Review Install Agent Task screen (see below).

The wizard displays the Review Install Agent Task screen, which contains a table of information summarizing agent/host installation compatibility.

- i. Click **Finish** to complete the installation.

The installation wizard generates a log file and displays the agent deployment details, such as a time stamp, status, agent name, and autostart settings.

Verifying Solutions Enabler Installation

Storage Agent for Symmetrix requires EMC Solutions Enabler Version 6.0.2. Refer to *Deploying Solutions Enabler* on page 213 for details about installing a valid version of Solutions Enabler when it is necessary.

The deployment location for Solutions Enabler Version 5.3.x SYMCLI on Windows was:

```
\Program Files\EMC\WideSky\bin
```

If you previously deployed Solutions Enabler Version 5.3.x, ensure that you modify the PATH for any SYMCLI scripts to the location for Solutions Enabler version 6.0.2 SYMCLI on Windows:

```
\Program Files\EMC\SYMCLI\bin
```

If Storage Agent for Symmetrix does not find a valid version of Solutions Enabler, Storage Agent for Symmetrix logs the error condition in `<Install_Root>\exec\EGS520\EGS.log`, and tries to send an alert to ControlCenter Console interfaces indicating the condition. Then Storage Agent for Symmetrix shuts down.

Creating Native Install Images for UNIX Host Agents

To create native installable images for the Host Agents for AIX, HP-UX, LINUX, and for Solaris:

- a. On the target host, ensure that the only ControlCenter agent installed is the Master Agent. No ControlCenter application agents should be installed—if necessary, uninstall application agents on the target host before proceeding.
- b. Using the ControlCenter Console, push only the desired host agent (AIX, HP-UX, LINUX, or Solaris) to the target host.
- c. Log on to the target host. Then change the directory to:

```
<Master_agent_install_directory>/exec/M*R520
```

- d. Run the following script:

```
package_agents.sh
```

Example: `./package_agents.sh`

- e. Specify the output directory for the created packages. Then press Enter.

The program creates the installable image file, where `<host_os_identifier>` is a unique identifier for the operating system installed on the target host:

```
magent-5.2.00-1<host_os_identifier>
```

If you receive the following message while running `package_agents.sh`, other agents (in addition to the host and Master Agent) could still reside on the host and possibly cause errors in creating the images:

Caution: Only ControlCenter Master and Host Agents should be installed to `/usr/ecc/exec`. Other Agents have been detected on this system.

The images are now available for use with your local scripts or commands for pushing the host agent to the desired hosts. The native installable images can be uninstalled with the same package manager that is used to install them.

Deploying Windows Agents from the Command Line

You can now use a Windows executable to deploy Host Agent for Windows and/or the Windows Master Agent from the command line. To deploy Host Agent for Windows or the Windows Master Agent (or both) on a host:

- Change to the following directory on the ECC Server host:
`<inst_root>\media_rep\remoteinstall\WinNativeInstall`
Example:
`cd C:\ecc\media_rep\remoteinstall\WinNativeInstall`
- Copy **setup.exe** from the directory accessed in the previous step to a location on the host where the agents are to reside.
- Change to the directory where you copied **setup.exe** and run it as follows:

```
setup.exe /s /v"/qn INSTALLDIR=<ecc_install_root>
SERVERHOSTNAME_ORIP=<eccserver_hostname_or_ip_addr>
[SERVERHOSTNAME_NAME=<ecc_server_hostname>]
[SERVER_PORT=<port_#>]
[MAPORT=<port_#>]
/Liwrmo!veacup+ <log_output_file>
[INSTALLHOSTAGENT=false]
Example (creates only the Windows Master Agent image):
```

```
setup.exe /s /v"/qn INSTALLDIR=C:\ecc
SERVERHOSTNAME_ORIP=ecchost INSTALLHOSTAGENT=false
/Liwrmo!veacup+ C:\temp\CmdLine.log"
```

In the command syntax:

- **INSTALLDIR** is the root directory where the agents are to be installed.
- **SERVERHOSTNAME_ORIP** is the ECC Server hostname or IP address. If you specify the IP address, you must also specify the hostname on the **SERVERHOSTNAME_NAME** parameter.
- **SERVERHOSTNAME_NAME** is the ECC Server hostname or IP address. This parameter is required only if you provided an IP address on the **SERVERHOSTNAME_ORIP** parameter. Do not specify this parameter if you specified a hostname on the **SERVERHOSTNAME_ORIP** parameter.
- **SERVER_PORT** is the ECC Server listening port number. This parameter is optional—if not specified, the default value (5799) is used.

- MAPORT is the Master Agent listening port number. This parameter is optional—if not specified, the default value (5798) is used.
- [/Liwrmo!veacup+] indicates that setup.exe is to create a log file (<log_output_file>) that describes its progress.
- <log_output_file> is the location of the log file for setup.exe. The directory must exist in the file system before you enter the command. Messages that would normally appear in dialog boxes during interactive installation will be prefixed with the following string:
ECC_LOG_MESSAGE
For example:
C:\ecc\ecc_testing.log
- INSTALLHOSTAGENT indicates that only the Windows Master Agent image is to be created (not the host agent image). This parameter is optional—if not specified, the default value (true) is used.

If setup.exe completes successfully, the log output file specified in the command contains a message indicating completion. If the command contains syntax errors, setup.exe will attempt to invoke its GUI version to request additional command input.

Step 47 Finish Setting Up Agents

If you are running any of the following agents, you might need to perform steps in this section to complete agent deployment:

- ◆ **Common Mapping Agent**—Refer to the *Configuration* section of *Common Mapping Agent Quick Summary* on page 67.
- ◆ **Database Agent for Oracle**—Refer to the *Configuration* section of *Database Agent for Oracle Quick Summary* on page 74.
- ◆ **Storage Agent for NAS**—Refer to the *Configuration* section of *Storage Agent for NAS Quick Summary* on page 86.
- ◆ **Storage Agent for Symmetrix**—Refer to the *Configuration* section of *Storage Agent for Symmetrix Quick Summary* on page 92.
- ◆ **Symmetrix SDM Agent**—Refer to the *Configuration* section of *Symmetrix SDM Agent Quick Summary* on page 73.

Step 48 Enable Access to Symmetrix Arrays

Symmetrix access controls (available in Enginuity 5567 or higher) can restrict access to ControlCenter functions such as SRDF, TimeFinder, SDR, and Optimizer for an entire Symmetrix array or a subset of Symmetrix devices.

You can use the Symmetrix command line interface (SYMCLI) to configure Access Controls that allow Symmetrix systems to work with ControlCenter. Because SYMCLI is a component of EMC Solutions Enabler, ensure you have Solutions Enabler installed on the target host before you begin. Then, perform the following procedure on every host that is to run Storage Agent for Symmetrix:

- a. Set up an *accgroup* for the ControlCenter application, for each Symmetrix system that has Access Control enabled, with the ControlCenter PIN added as a user ID. For example, you could enter the following SYMCLI command to set the access permissions:

```
symacl -sid <symm_serial_#> commit -file setUpCC.txt
```

where *symm_serial_#* is the serial number of the Symmetrix system that has Access Control enabled. In the following example, the Symmetrix serial number is 1166:

```
symacl -sid 1166 commit -file setUpCC.txt
```

In the command, *setUpCC.txt* contains the following Access Control commands, which create a group for the ControlCenter application, add an access PIN for ControlCenter applications, and grant ALL or BASE access to the ControlCenter application group. For example:

```
create accgroup ECC_APP;
add user accid ECCPIN name ECC_PIN to accgroup ECC_APP;
grant access=ALL to accgroup ECC_APP for ALL DEVS;
```

- b. Set up an access group that contains all Symmetrix agent hosts. Give BASE and ECC access rights to that group. Enter the following SYMCLI command to set the access permissions:

```
symacl -sid <symm_serial_#> commit -file setCCHost.txt
```

where *symm_serial_#* is the serial number of the Symmetrix system that has Access Control enabled. In the following example, the Symmetrix serial number is 1166:

```
symacl -sid 1166 commit -file setCCHost.txt
```

In the command, *setCCHost.txt* contains the following Access Control commands, which create an access group for hosts running ControlCenter agents, add an access ID for a ControlCenter agent host to the group where *UNIQUE ID* is the unique ID of the host returned by running *symacl -unique* on that host and *HOST NAME* is the name of the host, and grant ALL or BASE access to the ControlCenter application group. For example:

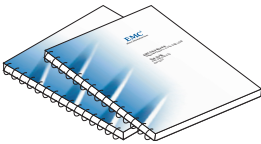
```
create accgroup ECC_HOST;
add host accid <UNIQUE ID> name <HOST NAME> to accgroup ECC_HOST;
grant access=BASE,ECC to accgroup ECC_HOST for ALL DEVS;
```

After you run the commands, the system displays the entries in the access database.

Further information

For details about how to install, configure, and use SYMCLI for Symmetrix Access Controls, refer to *EMC Solutions Enabler Symmetrix Access Control CLI Product Guide*.

For details about installing, configuring, and using Symmetrix Access Controls with ControlCenter, refer to the ControlCenter Console online help.





Quick check: Installation status

Before continuing with the installation, review the items in this section to verify the installation status. You might want to click the **Installed Components** button in the installation wizard to check the list of installed components and products.

◆ Components installed to this point:

- *Repository*, from the ControlCenter installation CDs (or a shared folder).
- *ECC Server*, from the ControlCenter installation CDs (or a shared folder).
- *EMC Solutions Enabler* (made available for remote deployment, from the Solutions Enabler CDs or a shared folder).
- *Store*, from the ControlCenter installation CDs (or a shared folder).
- *Other components or products* (such as the Master Agent and WebConsole Server), using the ControlCenter installation CDs (or a shared folder).
- *At least one Console*, using the Console installation program in Internet Explorer or Netscape.
- *Master Agents on all hosts* to be monitored and managed through ControlCenter.
- *Application agents*, using the agent installation wizard in the Console.

◆ What's next?

- Perform initial discovery (automatic discovery, assisted discovery, and connectivity device discovery).
-

Step 49 Allow Automatic Discovery to Complete

Discovery is the process of identifying the resources to be managed by ControlCenter, which include hosts, storage arrays, connectivity devices, adapters, switch ports, zones, groups, and so on, and the relationships between those resources. *Initial discovery* refers to the first discovery of those resources that occurs after you finish installing ControlCenter components and products. Initial discovery must occur before you can begin managing those objects through ControlCenter.

Automatic discovery of hosts and Symmetrix systems is performed by the related ControlCenter agents after they are up and running. No action is required from ControlCenter users, other than to optionally define and assign each agent's discovery data collection policy (refer to *EMC ControlCenter 5.2 User/Administration Guide* for details). Once ControlCenter automatically discover objects, it continues to monitor them.

Follow this procedure to ensure that automatic discovery successfully completes as part of ControlCenter initial discovery:

- ◆ 49.1 *Allow automatic discovery to complete* on this page.
- ◆ 49.2 *Verify that managed objects are automatically discovered* on this page.

49.1 Allow automatic discovery to complete

Before beginning Assisted Discovery and Connectivity Device discovery (the next two steps in initial discovery), allow sufficient time for ControlCenter to automatically discover hosts and Symmetrix arrays.

49.2 Verify that managed objects are automatically discovered

In the ControlCenter Console or WebConsole tree panel, verify that managed objects representing automatically discovered resources appear.

Step 50 Perform Assisted Discovery

Follow these steps when using *Assisted Discovery* to discover storage arrays, hosts, and database objects were not discovered with Automatic Discovery:

- ◆ 50.1 *Understand Assisted Discovery for SMI-enabled arrays* on this page.
- ◆ 50.2 *Ensure agents are running* on page 229.
- ◆ 50.3 *Enter Assisted Discovery settings* on page 229.
- ◆ 50.4 *Review the results of Assisted Discovery* on page 235.
- ◆ 50.5 *Start managing objects discovered with Assisted Discovery* on page 235.
- ◆ 50.6 *Stop managing objects discovered with Assisted Discovery* on page 236.

50.1 Understand Assisted Discovery for SMI-enabled arrays

Storage Agent for SMI can discover any SMI-enabled storage array supported by an available SMI provider. The Discovery Settings for SMI Arrays panel lets you discover all SMI-enabled arrays, of any type, that are known to the SMI provider you specify. The Discovery Settings for Symmetrix panel and the SMI Provider tabs on the CLARiiON, ESS, HDS, and StorageWorks panels allow you to use the Storage Agent for SMI to discover only arrays of a specific type.

For example, to discover only CLARiiON arrays known to the SMI provider, use the SMI Provider tab on the CLARiiON panel. To discover only the Symmetrix arrays known to the SMI provider, use the Symmetrix panel. You must provide the following information on the panels for Assisted Discovery of SMI-enabled arrays.

The following are Assisted Discovery Settings for SMI-enabled arrays.

- ◆ *Provider Host Name*—The network name of the host where Storage Agent for SMI resides.
- ◆ *Provider Port*—The port through which ControlCenter is to connect to the SMI provider host. The default is 5988.
- ◆ *Provider Namespace*—The namespace of specified SMI provider. The namespace of EMC's provider is `root/cimv28`. This is built-in information and is always shipped with the product. If this is not an EMC storage array, then contact the provider directly.
- ◆ *User Name*—Username for the SMI provider. See *Password* for

more information.

- ◆ *Password*—Password for the SMI provider. Once you have installed the provider (EMC calls the CIM Agent: Common Information Model Agent), you must perform a series of steps to configure and validate the installation, including adding the username/password.

For example, in order to discover an IBM ESS array, install the ESS CIM Agent; then, follow the `postinstall.txt` file, which will instruct you on how to configure and validate the installation. These instructions include a step to add the username/password. The SMI agent uses this username/password to connect to the CIM Agent.

- ◆ *Timeout*—Time-out for attempts to connect to SMI provider host, in seconds. The default is 60.

50.2 Ensure agents are running

Table 59 on page 230 lists the objects and agents that participate in Assisted Discovery. To perform discovery for objects, you must ensure the associated agents are running, or if you have implemented an SMI Provider, ensure that Storage Agent for SMI is running and has access to the managed objects to be discovered.

50.3 Enter Assisted Discovery settings

Follow this procedure to provide information about the objects to be discovered and, if necessary, information about an SMI provider:

- a. From the Console menu bar, display the **Discover** Console menu and select **Other**.

The **Discover Other Objects** dialog box appears.

- b. Select one of the object types to discover in the **Discover Type** field in the **Discover Other Objects** dialog box on the left-hand side. In each case, the **Discovery Settings** portion of the dialog box changes according to the selected resource.
- c. Use *Objects and Agents Participating in Assisted Discovery* on page 230 to enter information in the **Discovery Settings** area of the dialog. Table 59 on page 230 uses the following abbreviations.
 - *During AD*: Objects that are discovered during Assisted Discovery.

- *After AD*: Objects that are discovered after Assisted Discovery is complete.

Table 59 **Objects and Agents Participating in Assisted Discovery**

Objects	Discovery Settings
Centera (<i>Storage Agent for Centera</i>)	
<i>During AD</i>: EMC Centera Content Addressed Storage. <i>After AD</i>: Access nodes, application profiles, licenses, pools, and services.	Provide the following information in the Discover Other Objects dialog box. ◆ <i>Primary Access Node</i>—IP address or hostname of the node to be used in discovering Centera arrays. ◆ <i>Access Node, Failover 1-3 (Optional)</i>—Secondary access nodes, to be used only if access failed through the primary access node listed above. ◆ <i>Path to Authorization File (Optional)</i>—By default, Storage Agent to Centera connects to Centera arrays using the Anonymous profile, which has monitoring capability enabled (so no authentication is required). To provide authentication, you must create a profile for monitoring Centera, copy the corresponding pool entry authorization (PEA) file to a directory that the agent can access, and specify the location of that PEA file as an absolute or a relative (to the agent installation directory) path.
CLARiiON (<i>Storage Agent for CLARiiON</i>)	

Table 59 Objects and Agents Participating in Assisted Discovery (continued)

Objects	Discovery Settings
<i>During AD:</i> EMC CLARiiON arrays. <i>After AD:</i> Storage processors, storage groups, mapped LUNs, and unmapped LUNs.	The discovery settings depend on the CLARiiON model. Click one of the following tabs in the Discover Other Objects dialog box: ◆ FC4500/FC5300—The hostname of the node that is connected to the SP on the CLARiiON array to be discovered. ◆ CX200—Name of storage processor (SP) A, name of storage processor (SP) B (not required if only one SP is used), and the global username and password that Storage Agent for CLARiiON will use to access the array. ◆ FC4700/CX except CX200—Name of storage processor (SP) A, name of storage processor (SP) B, and the global username and password that Storage Agent for CLARiiON will use to access the array. ◆ SMI Provider—Provider hostname, port, namespace, global username and password, time-out interval, and optionally the SSL certificate store path (the full path, including file name, of the file containing the SMI Provider's client certificate, used for authentication by Storage Agent for SMI). If you specify an incorrect username/password combination in the Discover Other Objects dialog, Storage Agent for CLARiiON will not discover metaLUNs. In this situation, do the following to enable metaLUN discovery. 1. Select the partially discovered CLARiiON from the tree panel in the Console. 2. Select Discover, Remove Permission to Manage to open the Remove Permission to Manage CLARiiON dialog box. 3. Uncheck the correct CLARiiON agent from the Remove Permission to Manage CLARiiON dialog box and click OK. 4. Discover the CLARiiON again through ADA by using correct username/password.
Database (<i>Common Mapping Agent tab</i>)	
<i>During AD:</i> Database and host objects. <i>After AD:</i> Other database and host objects (depends on the database or host type) are automatically discovered after assisted discovery completes.	Provide the following information in the Discover Other Objects dialog box: ◆ <i>Host Names</i>—Host network names where databases to be monitored reside. ◆ <i>Host IPs</i>—IP addresses of hosts where databases to be monitored reside. ◆ <i>Host Ports</i>—Host port numbers used by the SYMAPI Server component of EMC Solutions Enabler. ◆ <i>DB Instances</i>—Name(s) of the databases to be monitored. ◆ <i>DB User, DB Password</i>—User database login name(s) and password(s). Note: The user name that is supplied does not need to have any admin rights. ◆ <i>DB Type</i>—SQL Server, Sybase, Informix, or DB2 Universal Database. ◆ <i>DB Home</i>—Home directories of databases to be monitored. ◆ <i>SYBASE OCS (Optional)</i>—Sybase Open Client Server library installation path.

Table 59 Objects and Agents Participating in Assisted Discovery (continued)

Objects	Discovery Settings
Database (<i>Database Agent for Oracle tab</i>)	
<i>During AD:</i> Database objects on the agent host or on remote, accessible hosts. <i>After AD:</i> Oracle database files, schemas, and tablespaces. Important: When discovering a remote Oracle instance, file properties will not be fully populated. The database will appear in the Agent Host folder in the Console.	Provide the following information in the Discover Other Objects dialog box: ◆ <i>Database Kind</i>—The value in this field is always <code>Oracle</code>. ◆ <i>Host Name</i>—Name or IP address of the host on which the database resides—the agent host must be able to resolve the provided value. You might need to manually enter this value when discovering a remote Oracle instance because the menu includes only hosts that are known to ControlCenter. If the database is to be monitored through a cluster address, enter the cluster DNS name or IP address. ◆ <i>Oracle Base</i>—The value of the <code>ORACLE_BASE</code> environment variable, which indicates the base Oracle database installation directory. ◆ <i>Oracle Home</i>—The value of the <code>ORACLE_HOME</code> environment variable, which indicates the base Oracle database home directory. ◆ <i>Oracle SID</i>—The Oracle system identifier (the name of the Oracle database instance to be discovered). The agent host must be able to resolve the provided value. Can be an Oracle SID (for a database on the specified host) or a TNS service name (specified in <code>tnsnames.ora</code> on the agent host). ◆ <i>Listener Port Number</i>—The port number where Database Agent for Oracle connects to the database to be discovered. The value is typically 1521. ◆ <i>SYS User Password</i>—Oracle administrative password used to create an account for Database Agent for Oracle, so it can access the database to be discovered. ◆ <i>Oracle Agent User Name and Password</i>—User ID and password that Database Agent for Oracle uses to access the database to be discovered. Important: If the host on which the remote database resides is also running VERITAS File System, your initial Assisted Discovery attempt may appear to succeed but no objects may initially appear in the Console. This may be caused by unsynchronized metadata on disk in VERITAS File System. This issue is easily resolved by one of two methods: - Mounting the VERITAS file system with the <code>-o convosync=direct</code> option, and then attempting Assisted Discovery. - Setting the Oracle Agent Data Collection policy (after Assisted Discovery) to collect data after VERITAS File System metadata synchronization has occurred.
ESS	
<i>During AD:</i> IBM ESS arrays. <i>After AD:</i> Devices, controllers, and ports	The following input is required on the ESS Agent tab: ◆ <i>Server IP/Server Name</i>—IP address or hostname of the ESS Specialist Server. ◆ <i>User Name</i>—Username for the ESS Specialist Server. ◆ <i>Password</i>—Password for the ESS Specialist Server. Refer to <i>Understand Assisted Discovery for SMI-enabled arrays</i> on page 228 for descriptions of the input required on the SMI Provider tab.

Table 59 Objects and Agents Participating in Assisted Discovery (continued)

Objects	Discovery Settings
HDS	
<i>During AD:</i> StorageWorks XP and HP HDS storage arrays. <i>After AD:</i> Devices, controllers (FEAdapter), ports, groups (LUN, WWN, host, StorageDomains), Performance Manager data (optional).	The following input is required on the HP XP Series tab: ◆ <i>Server Type</i>—IP address or hostname of the ESS Specialist Server. ◆ <i>User ID</i>—The CommandView user ID (Active commands require administrator access, but discovery requires user-level access only). ◆ <i>Password</i>—The CommandView password. ◆ <i>Command View CLI Path</i>—Path and filename for CommandView command line interface file, on the host where Storage Agent for HDS is running. For example: C:\HPSS\cvcli.bat The following input is required on the HDS Series tab: ◆ <i>Server Type</i>—For HDS arrays, this is always HiCommand. ◆ <i>Server IP</i>—IP address of the HiCommand server. ◆ <i>Server Port</i>—Port where ControlCenter is to connect to the HiCommand server. ◆ <i>User ID</i>—Username for the HiCommand server. ◆ <i>Password</i>—Password for the HiCommand server. ◆ <i>HiCommand Tuning Manager Host</i>—Network name of host running HiCommand Tuning Manager. You must enter a value to enable collection of HDS statistics for Performance Manager by Storage Agent for HDS. ◆ <i>HiCommand Tuning Manager Port</i>—Port to connect to the HiCommand Tuning Manager server. You must enter a value in this field to enable collection of HDS statistics for Performance Manager by Storage Agent for HDS.
Host (<i>Discovered by Common Mapping Agent, through SYMAPI Server</i>)	
Hosts	Provide the following information in the Discover Other Objects dialog box: ◆ <i>Host Name</i>—Network name of the host to be discovered. ◆ <i>Host IP</i>—IP address of the host to be discovered. ◆ <i>Host Port</i>—Port for connection to the host to be discovered. Default: 2707
NAS Container (<i>Discovered by Storage Agent for NAS</i>)	
<i>During AD:</i> EMC Celerra Network Servers and Network Appliance Filers. <i>After AD:</i> For Celerra, NAS devices, Data Mover, file systems, and volumes. For Network Appliance, NAS devices, filer, file systems, and volumes.	Provide the following information in the Discover Other Objects dialog box: ◆ <i>IP Addr</i>—Network name of the host to be discovered. ◆ <i>Port</i>—Port for connection to the host to be discovered. Default: 8000 ◆ <i>Username</i>—Username that Storage Agent for NAS uses to access the NAS container to be discovered. ◆ <i>Password</i>—Password that Storage Agent for NAS uses to access the NAS container to be discovered. ◆ <i>Type</i>—NAS device type you want to discover. Choices are Celerra and NetApp. To discover Network Appliance systems, you must enable <code>rsh</code> on those systems, and ensure that the username/password specified in the Discovery Settings dialog box is a valid administrative user on those systems (to allow access through <code>rsh</code>).

Table 59 Objects and Agents Participating in Assisted Discovery (continued)

Objects	Discovery Settings
SMI Arrays (<i>Discovery by Storage Agent for SMI through an SMI Provider</i>)	
<i>During AD:</i> SMI-enabled storage arrays. <i>After AD:</i> Objects depend on array discovered.	Refer to <i>Understand Assisted Discovery for SMI-enabled arrays</i> on page 228 for descriptions of the input required on the SMI Provider tab.
StorageWorks (<i>Discovery by Storage Agent for SMI through an SMI Provider</i>)	
<i>During AD:</i> HP StorageWorks HSG80 (EMA) and HP StorageWorks XP arrays <i>After AD:</i> Controllers and mapped LUNs <i>Note:</i> After discovering StorageWorks arrays, Console interfaces will not display relationships between those arrays and hosts until the next host agent discovery occurs.	• <i>Serial port (for serial connections only)</i>—The communication port for a serial connection. The default is: COM1 • <i>Baud rate (for serial connections only)</i>: 4800, 9600, or 19200. The default is: 9600 • <i>Parity (for serial connections only)</i>: NONE, ODD, or EVEN. The default is: none • <i>Stop bit (for serial connections only)</i>: 1.0, 1.5, or 2.0. The default is: 1.0 • <i>Bits (for serial connections only)</i>: 7 or 8. The default is 8. • <i>Host name (for network connections only)</i>: Hostname (preferred) or IP address of the host where the StorageWorks Command Console Agent or the SANworks Management Appliance is running. The default is: mysteam • <i>Host port (for network connections only)</i>: TCP port through which Storage Agent for HP StorageWorks communicates with the StorageWorks Command Console Agent or the HSG Element Manager Agent. The default is 4999. • <i>Password (for network connections only)</i>: Password for accessing either the StorageWorks Command Console Agent or the HSG Element Manager Agent. There is no default. • <i>Timeout (for network connections only)</i>: Number of seconds that a socket read call and the connect call will wait for a response before failing. The default is 6.
Symmetrix (<i>Discovery by Storage Agent for SMI through an SMI Provider</i>)	
<i>During AD:</i> EMC symmetrix storage arrays.	Refer to <i>Understand Assisted Discovery for SMI-enabled arrays</i> on page 228 for descriptions of the input required on the Discovery by SMI Agent, via SMI Provider tab.

- d. Select an agent from the **Send To** list or use the default setting ***all relevant agents***.

If you want to send the access data to more than one agent, but do not want to send the access data to all relevant agents, click the **Select Agents** button to launch the **Select Agents** dialog box. In this dialog box, you can select the exact subset of active agents to which the server will send the access data.

- e. Click **Apply**.

The **Access Info Confirmation** dialog box appears.

- f. Click **OK** after confirming that the information presented in the dialog box is correct.

The command is sent to the ECC Server. The object appears in the ControlCenter tree panel when it is discovered.

- g. Click **Cancel** to close the **Discover Other Objects** dialog box.

50.4 Review the results of Assisted Discovery

To review the results of assisted discovery:

- a. Click the **Discover** drop-down menu and select **Review Progress**.

The **Review Discovery Results** dialog box appears.

- b. Select a command or access information row in the Result Summaries table.

The command or access information details appear in the Assistance Result Details panel.

You cannot delete rows in the Results Summaries tables for commands sent by your Console. You can delete rows for stored access data if there are no managed objects associated with that access data (if the **object #** column has a zero). In this case, the **Delete** button is enabled.

If the **object #** column is nonzero for stored access data, and you want to delete the access data, you must use the Stop Managing Object dialog box (refer to step 50.6 on page 236) to reduce the *object count* for that row.

50.5 Start managing objects discovered with Assisted Discovery

To start managing an object that has been discovered through Assisted Discovery:

- a. Right-click the object in the Console tree panel and select **Discover, Start Managing Object**.

The **Start Managing Object** dialog box appears.

- b. Select the checkbox beside the agent(s) that you want to start managing the object.

Grayed-out, checked items represent agents that are currently managing the selected object.

- c. Click **OK**.

ControlCenter sends a command to the ECC Server to add the selected agent(s) to the set of agents that currently manage the selected object. You can check the status of the command in the **Review Discovery Results** dialog box.

50.6 Stop managing objects discovered with Assisted Discovery

To stop managing an object that has been discovered through Assisted Discovery:

- a. Right-click the object in the tree panel and select **Discover, Stop Managing Object**.

The **Stop Managing Object** dialog box appears.

- b. Clear the checkbox beside the agent(s) that you want to stop managing the object.

Grayed-out, unchecked items represent agents that are not currently managing the selected object.

- c. Click **OK**.

ControlCenter sends a command to the ECC Server to remove the selected agent(s) from the set of agents that currently manage the selected object. You can check the status of the command in the **Review Discovery Results** dialog box.

A discovered object remains in the Repository even if no agent is currently managing it.

Step 51 Discover connectivity devices

Connectivity device discovery is a one-time-user-initiated discovery of connectivity devices launched through the Discover menu in the ControlCenter Console. It is a two-stage process that includes finding connectivity devices in the SAN, and then, in a separate operation, discovering the topology and fabric information for the switches that were discovered. These steps can be taken simultaneously or in sequence.

Do the following to discover connectivity devices:

- a. Gather needed connection information for the switches to be discovered—IP address (of the service processor or DSM Connect host for McDATA, switch proxy for Brocade and CNT), username, password, and so on.

- b. Click the **Monitoring** task and choose **Discover, Connectivity...**

The system displays the **Search for Connectivity Devices** dialog box.

- c. Specify the IP addresses of the devices in the **Search for Connectivity Devices** dialog box. Advanced options let you prompt for connection information as needed and discover full topology and fabric information for switches.

ControlCenter discovers connectivity devices in the SAN, including switches and fabrics, displaying the status of each device and adding it to the topology.

Planning, installation, and initial setup of ControlCenter are now complete. You are now ready to use ControlCenter to manage your storage environment. Refer to the *EMC ControlCenter 5.2 Administration/User Guide* for information about using ControlCenter for daily operations. You can now restart the antivirus software and Distributed Transaction Coordinator Service that you stopped before ControlCenter installation (if applicable).

Step 52 Back Up ControlCenter (Optional)

Do the following to completely back up ControlCenter:

- ◆ 52.1 *Prior to backing up* on this page.
- ◆ 52.2 *Stop Repository services* on page 239.
- ◆ 52.3 *Back up ControlCenter application files* on page 239.
- ◆ 52.4 *Start Repository services* on page 240.

52.1 Prior to backing up

If you have a requirement to backup the ControlCenter infrastructure server using third-party software, such as NetBackup, EDM, etc., the following should be considered:

Backups should be scheduled around the following automatic tasks:

- ◆ Hotbackup database job that runs daily at 2:00 a.m.
- ◆ Export Backup that runs daily at 10:00 p.m.
(ramdb_export_db.bat)
- ◆ Both backup jobs are stored in the RAMBBACKUPDIR environment variable directory.

For example, scheduling third-party backup after 3:00 a.m. or 11:00 p.m. (after the automatic tasks end) allows backup of the latest files from RAMBBACKUPDIR. You can determine the exact completion time of hot backup or export backup by looking at the timestamps of %RAMBOH%\Repository\admin\Ramb_Scripts\ramb_hotback.log and %RAMBBACKUPDIR%\exp\rambdb_exp.log.

When backing up the database components, the following open files need to be excluded from the backup process:

```
%RAMBOH%\Repository\oradata\rambdb\*.CTL
%RAMBOH%\Repository\oradata\rambdb\*.LOG
%RAMBOH%\Repository\oradata\rambdb\*.DBF
```

This also applies to any third-party monitoring tools, such as BMC Patrol, as the external locks that this tool places on files are intrusive to Oracle (refer to the Oracle website, <http://www.oracle.com>, for additional information).

For recovery purposes, when backing up the database components, the following files need to be included in the backup process:

```
%RAMBBACKUPDIR%\hot\*.*
%RAMBBACKUPDIR%\exp\*.*
%RAMBOH%\Repository\oradata\rambdb\archive\*.*
%RAMBOH%\Repository\database\PWD*.*
%RAMBOH%\Repository\database\SP*.*
%RAMBOH%\Repository\admin\rambdb\bdump\*.*
%RAMBOH%\Repository\admin\rambdb\udump\*.*
%RAMBOH%\Repository\admin\rambdb\pfile\*.*
```

52.2 Stop Repository services

- From the Windows **Start** menu, select **Settings, Control Panel, Administrative Tools, Services**.
- In the **Services** window, ensure that the **Status** of the following services is **Stopped**. If necessary, right-click each service name and select **Stop**.

OracleECCREP_HOMETNSListener
OracleServiceRAMBDB

52.3 Back up ControlCenter application files

Before you begin this step, verify that you have enough disk space available for Repository backup in the backup location.

Do the following to back up the application files:

- Create a backup directory such as `<drive>\rollback`.
- Do the following on each host that has ControlCenter infrastructure components installed:
 - Insert ControlCenter installation CD #1 in the CD-ROM drive. If the Main Menu window displays, close the window.
 - In Windows explorer, double-click the following file.
`<install_drive>\utils\backup.bat`
 - Copy the original ControlCenter installation directory (`%ECC_INSTALL_ROOT%`) to the backup directory. Do not change the directory name.

The directory name is required if you need to restore the files.

52.4 Start Repository services

- a. From the Windows **Start** menu, select **Settings, Control Panel, Administrative Tools, Services**.
- b. In the **Services** window, right-click the following service names and select **Start**:

OracleECCREP_HOMETNSListener
OracleServiceRAMBDB

The backup of ControlCenter is now complete.



Quick check: Installation status

Your initial ControlCenter installation is complete, with the following installed components and products:

- ◆ *Repository*, from the ControlCenter installation CDs (or a shared folder).
- ◆ *ECC Server*, from the ControlCenter installation CDs (or a shared folder).
- ◆ *EMC Solutions Enabler* (made available for future installs, from the Solutions Enabler CDs or a shared folder).
- ◆ *Store*, from the ControlCenter installation CDs (or a shared folder).
- ◆ *Other components or products* (such as the Master Agent), using the ControlCenter installation CDs (or a shared folder).
- ◆ *At least one ControlCenter Console*, using the ControlCenter Console installation program in Internet Explorer or Netscape.
- ◆ *Master Agents on all hosts* to be monitored and managed through ControlCenter, using one or more of the Master Agent installation methods described in *Deploy and Start Master Agents* on page 192.
- ◆ *Application agents*, using the agent installation wizard in the ControlCenter Console.

- ◆ *Initial discovery* is complete and you have optionally backed up the installed ControlCenter components and products.
-

Set Up Cluster Support (Optional)

A *cluster* is a set of hosts (also referred to as *nodes* in this section) that can perform failover operations to reduce downtime in the event of a host failure. When a system-level failure requiring failover occurs on the active, primary host, a backup standby takes over. When the primary host is back online, you can manually perform failback to the primary host.

Before you begin: Read *Step 6: Plan for Cluster Support (Optional)* on page 24.

- ◆ Step 53: Install the ControlCenter Infrastructure in a Clustered Environment 244
- ◆ Step 54: Install ControlCenter Agents in an Application Clustered Environment 261
- ◆ Step 55: Troubleshoot Problems with Clusters 266

Step 53 Install the ControlCenter Infrastructure in a Clustered Environment

This section describes how to implement cluster support for the ControlCenter infrastructure, StorageScope, and Workload Analyzer Archiver agent, using these steps:

- ◆ 53.1 *Verify the hardware and software setup* on page 246.
- ◆ 53.2 *Create cluster node names* on page 247.
- ◆ 53.3 *Create ControlCenter resource groups* on page 247.
- ◆ 53.4 *Create the shared physical disk resource(s)* on page 248.
- ◆ 53.5 *Create the cluster IP address resource(s)* on page 249.
- ◆ 53.6 *Create a network name resource* on page 251.
- ◆ 53.7 *Bring the cluster resource group(s) online* on page 252.
- ◆ 53.8 *Install ControlCenter components and products* on page 252.
- ◆ 53.9 *Replicate ControlCenter Registry keys* on page 254.
- ◆ 53.10 *Add components and products to cluster control* on page 256.
- ◆ 53.11 *Enable failover for multiple Stores and Console refresh (optional)* on page 259.
- ◆ 53.12 *Bring the cluster(s) online* on page 260.

StorageScope and Workload Analyzer Archiver are the only non-infrastructure components that are supported for clustering on a ControlCenter infrastructure host.

EMC does not support installing host agents and infrastructure components on the same hosts in a cluster. Refer to *Install ControlCenter Agents in an Application Clustered Environment* on page 261 for instructions on installing host agents in a cluster.

Understand MSCS Cluster Support for ControlCenter

ControlCenter works with only certain features of MSCS:

- ◆ **Only active/passive clusters are supported.** In this type of cluster, a primary (active) host performs normal processing, and a secondary (passive) host restarts applications with full performance when a failure occurs on the active host. *Active/active* clusters, where both hosts run application software during normal operation and all the work is transferred to one host if a failure occurs, are not supported for ControlCenter.
- ◆ **Only two-node clusters are supported.** Although MSCS and EMC GeoSpan for MSCS support both two-node (one host failing over to another) and four-node (for up to three host failures) clusters, only two-node clusters are supported for ControlCenter.

Considerations for a Distributed Configuration

The steps in this section are tailored to a *single-host infrastructure* ControlCenter configuration (one in which all ControlCenter infrastructure components are installed on the same host). If you want to set up a cluster environment for a *distributed infrastructure* configuration, follow the steps in the gray boxes marked “Distributed Infrastructure.”

For a distributed configuration, it is possible to have one two-node cluster for each of the following ControlCenter components and products, although you can install any combination of the listed components on the same two-node cluster.

- ◆ Repository
- ◆ ECC Server (includes the Performance Manager Automated Reports service)
- ◆ Store (not required to be part of the cluster environment)
- ◆ WebConsole Server (includes the ECCAPI Server service)
- ◆ StorageScope
- ◆ Master Agent and Workload Analyzer Archiver

53.1 Verify the hardware and software setup

Ensure that the following are installed:

- ◆ **Two host machines:** Ensure that hosts meet the requirements specified in *EMC ControlCenter Support Matrix* on Powerlink.
- ◆ **Shared disk(s):** One or more that are 36 GB or larger.

Symmetrix users: To increase performance, ensure that your shared disk is configured as a metastriped device.

- ◆ **Software:** Install and configure the following on *both* host machines:
 - Microsoft Windows 2000 Advanced Server or Windows Server 2003 operating system; then set up MSCS as described in Microsoft's *Step-by-Step Guide to Installing Cluster Service*.
 - EMC GeoSpan for MSCS (optional), using the procedures in the *EMC GeoSpan for MSCS Product Guide*. GeoSpan allows you to create a cluster environment for disaster recovery by using SRDF for cluster failover.
- ◆ **IP Addresses:** Set up six unique static IP addresses (one for ControlCenter, and five as described in Microsoft's *Step-by-Step Guide to Installing Cluster Service*).

Important: Ensure that local user accounts being used for ControlCenter are set up identically on all cluster nodes.

Distributed Configuration

Set up as many clusters as desired. For example, you could set up one cluster each for the Repository, ECC Server, StorageScope, and ControlCenter agents. Repeat the above steps for each additional cluster.

53.2 Create cluster node names

GeoSpan: If you are implementing GeoSpan, skip this section— instead follow the steps in the *EMC GeoSpan for MSCS Product Guide* for implementing a two-node cluster (ControlCenter supports only two-node clusters), up to the point where you create a disk group for the quorum disk. The procedure in the *EMC GeoSpan for MSCS Product Guide* includes steps for creating cluster node names (for example, ECC1 and ECC2).

Use MSCS to create active and passive node names for the cluster environment, as described in Microsoft's *Step-by-Step Guide to Installing Cluster Service*.

For example, set up the following two nodes (these names will be used in the rest of this procedure):

- ◆ Cluster node #1: ECC1
- ◆ Cluster node #2: ECC2

Distributed Configuration

Use MSCS to set up the desired cluster nodes. For example:

- *Repository cluster:* ECCR1 , ECCR2
- *ECC Server cluster:* ECCS1 , ECCS2
- *StorageScope cluster:* ECCT1 , ECCT2
- *Master Agent/Workload Analyzer Archiver:* ECCA1 , ECCA2

Important: Ensure that cluster node names do not contain special characters such as underscores (this is an MSCS requirement).

53.3 Create ControlCenter resource groups

GeoSpan: If implementing GeoSpan, follow the steps in *EMC GeoSpan for MSCS Product Guide* for creating resource groups for a two-node cluster (skip the MSCS steps in this section). For example, use GeoSpan to create the ECCRG group for the two available cluster nodes (ECC1 and ECC2).

Create one or more resource groups for ControlCenter, using the MSCS Cluster Administrator, as follows:

- a. Start Cluster Administrator: Click **Start, Programs, Administrative Tools, Cluster Administrator**.

- b. Create a new Resource Group for ControlCenter: Right-click **Groups**, and select **New, Group** to open New Group wizard.
- c. Give a name (for example: ECCRG) and description to the new cluster group, and then click **Next**.

The Cluster Administrator displays the Preferred Owners screen with the available cluster nodes (for example, ECC1 and ECC2).

Distributed Configuration

Instead of creating only the ECCRG resource group, create as many resource groups as desired, for example:

- *Repository cluster*: ECCRR
- *ECC Server cluster*: ECCRS
- *StorageScope cluster*: ECCRT
- *Master Agent and Workload Analyzer Archiver*: ECCRA

- d. Select both nodes on the Preferred owners screen. Using the **Add** button, move them to the **Preferred owners** column. Click **Finish** to return to the Cluster Administrator window.
- e. Select the previously created resource group(s), then **Properties**. Select **Failback**, and then click the **Prevent Failback** radio button.

53.4 Create the shared physical disk resource(s)

GeoSpan: If implementing GeoSpan, create the shared physical disk resources using the procedure in the *EMC GeoSpan for MSCS Product Guide*, using the values shown in this procedure as a guideline (for example, ECCRGPhysicalDisk).

Use MSCS to create a new resource with attributes for the *shared physical disk*:

- a. Click and highlight the **Disk Group** menu tree icon to show the disk resource group.
- b. Drag the desired physical disk from the Disk Group to the ECCRG resource group (for our single-host infrastructure example). When asked to confirm that the resource should be moved and the group should be changed for the resource, reply **Yes**.

MSCS creates a resource for the shared physical disk.

Distributed Configuration

Instead of creating a resource with shared physical disk attributes for only the ECCRG resource group, create resources for all the groups in your cluster environment: ECCRR, ECCRS, ECCRT, and ECCRA.

- c. Right click the new entry for the shared physical disk resource in the ECCRG resource group. Then, select **Properties**.
- d. In the **Properties** screen, ensure that the checkbox labeled **Run the resource in a separate resource monitor** is *not* checked.
- e. Click the **Modify** button next to the **Possible Owners** box. MSCS displays the Possible Owners screen.
- f. If the listed nodes (for example, ECC1 and ECC2) are not already in the Possible Owners column, select both available nodes and move them to the Possible owners column, using the **Add** button. Then, click **OK**.

MSCS displays the Dependencies screen, which specifies the resources that must be brought online before the current resource.

- g. Ensure that no dependencies are specified in the Dependencies screen (since *Physical Disk* is the first resource to be brought online and therefore has no dependencies on other resources).
- h. In the **Properties**, screen click the **Parameters** tab.
MSCS displays the Parameters screen.
- i. Ensure that no disk parameters are specified in the Parameters screen. Then, click **OK**.

53.5 Create the cluster IP address resource(s)

GeoSpan: If implementing GeoSpan, create the IP address resources using the procedure in the *EMC GeoSpan for MSCS Product Guide*, using the values shown in this procedure as a guideline (for example, ECCRGIPAddress).

Using MSCS, create a new resource with attributes for the *cluster IP address*:

- a. Right-click ECCRG, and select **New, Resource**. MSCS displays the New Resource wizard.

- b. Enter a resource for the cluster IP address (you might have to ask your network administrator for the network name and IP address for the resource group):

Cluster Resource Group Resource —

Name: ECCRGIPAddress

Resource type: IP Address

Group: ECCRG

Distributed Configuration

Instead of creating a resource for only the ECCRG group, create resources for all groups in your cluster environment using the IP Address resource type. In our example, the resources are:

Name: ECCRRIPAddress, Group: ECCRR

Name: ECCRSIPAddress, Group: ECCRS

Name: ECCRTIPAddress, Group: ECCRT

Name: ECCRAIPAddress, Group: ECCRA

- c. Click **Next**. MSCS displays the Possible Owners screen, which lists the two available nodes for the cluster.
- d. Select both available nodes. Then use the **Add** button to move them to the Possible owners column. Then click **Next**.

MSCS displays the Dependencies screen, which specifies the resources that must be brought online before the current resource.

- e. On the Dependencies screen, since IP Address is dependent on Physical disk, select **Add**, then click **Next**.

Resource dependencies —

Disk E: Physical disk

MSCS displays the TCP/IP Address Parameters screen, which allows the IP address to be assigned to the resource.

- f. On the TCP/IP Address Parameters screen, enter the IP address for the resource (refer to example below).

In the Address field shown below, specify the IP address assigned to the ControlCenter cluster resource group. This is a mobile address.

TCP/IP Address Parameters —

Address: 1.22.33.111 *(fill in actual address)*

Subnet mask: 255.255.255.0

Network: *NetworkName* (fill in actual name)

Enable NetBIOS for this address: [*selected*]

- g. Click **Finish**.

53.6 Create a network name resource

GeoSpan: If implementing GeoSpan, create the network name resource using the procedure in the *EMC GeoSpan for MSCS Product Guide*, using the values in this procedure as a guideline (for example, ECCRGNetworkName).

Create a new resource with attributes for *Network Name*, using MSCS:

- a. Right-click the ECCRG resource group (example) and select **New, Resource**. This brings up the New Resource wizard. Enter the information, and then click **Next**. For example:

Cluster Resource Group Resource —

Name: ECCRGNetworkName

Resource type: Network Name

Group: ECCRG

Distributed Configuration

Instead of creating a resource for the ECCRG group, create resources for all groups in your cluster environment, using the *Network Name* resource type. In our example, the resources are:

Name: ECCRRNetworkName, Group: ECCRR

Name: ECCRSNetworkName, Group: ECCRS

Name: ECCRTNetworkName, Group: ECCRT

Name: ECCRANetworkName, Group: ECCRA

- b. In the New Resource wizard, click **Next**. MSCS displays the Possible Owners screen, which lists the two **Available nodes** for the cluster.
- c. Select both available nodes. Using the **Add** button, move them to the Possible owners column. Then, click **Next**.

MSCS displays the Dependencies screen, which specifies the resources that must be brought online before the current resource.

- d. On the Dependencies screen, since `NetworkName` is dependent on `IP Address`, select **Modify**, then move the `IP Address` resource from the Available Resources column to the Resource Dependencies column. Then, click **Next**.

This automatically establishes dependencies on all previously configured generic resources (in other words, since `IP Address` is dependent on `Physical Disk` and `Network Name` is dependent on `IP Address`, it follows that `Network Name` is also dependent on `Physical Disk`).

- e. Leave the Network Name Parameters screen blank and click **Finish**.

53.7 Bring the cluster resource group(s) online

In the MSCS tree panel, right click the cluster resource groups to be brought online (in our example, ECCRG is the only resource group) and click **Bring Online**.

53.8 Install ControlCenter components and products

You are now ready to install ControlCenter as part of a clustered environment, using the steps in this section.

Important: Install all ControlCenter components and products on the *shared disk* (not on the separate hosts). When specifying hostnames, use the *fully qualified domain name* (FQDN) for the host to ensure that different IP addresses correctly resolve to different hostnames.

- a. Install the Repository, using *Step 30.3: Install the Repository* on page 132, noting exceptions for the following fields:
 - *Choose Your Database Backup Directory:* Ensure that the directory resides on the shared disk (example: `E:\ECC_Backup`). The shared disk must be in the ControlCenter resource group(s).
 - *Select Primary Network Name for ECC Repository:* Enter the primary network FQDN assigned to the ControlCenter resource group (ECCRG).

Reminder: When you set up the Repository in a cluster environment, EMC highly recommends that you use network name for the target host (if DNS is properly configured, this will display automatically in the installation wizard) instead of the IP address.

- b. Install the ECC Server, using the step *Install the ECC Server* in *Step 29: Be Sure You are Ready to Install ControlCenter* on page 130, noting exceptions for the following installation fields:
 - *Select Primary Network Name for ECCServer*: Enter the primary network address for the cluster name.
 - *Select Alternative Network Names for Console Communications*: Do not enter a response.

Important: When specifying the hostname, use the FQDN for the host. This ensures that the different IP addresses correctly resolve to different hostnames.

- c. Install one or more Stores, using the procedure in *Install one or more Stores* on page 140.
- d. If you plan to include the WebConsole Server in the cluster environment, install the WebConsole Server, using the procedure in *Step 31: Install the WebConsole Server (Optional)* on page 145.
- e. Start the ControlCenter infrastructure, using the procedure shown in *Step 34: Start Infrastructure Components* on page 160.
- f. Install StorageScope, using the procedure in *Step 41: Install StorageScope (Optional)* on page 182, with the following exceptions:
 - *Select Primary Network Name for StorageScope server*: Enter the primary network address assigned to the cluster name.
 - *Select Alternative Network Name for Console Communication*: Do not enter a response.

Important: When specifying a hostname, use the FQDN for the host. This ensures that the different IP addresses correctly resolve to different hostnames.

- g. Optionally do the following, if you plan to include Workload Analyzer Archiver as part of your cluster environment:
 1. Install the Master Agent, using the procedure shown in *Step 45: Deploy and Start Master Agents* on page 192.

Important: When installing the Master Agent on a Windows multihomed host, select the network address that has connectivity to the ECC Server host.

2. Install and launch the ControlCenter Console (not as part of the clustered environment), using *Step 35: Install the ControlCenter Console* on page 164 to deploy Workload Analyzer Archiver.
3. Deploy Workload Analyzer Archiver, using the ControlCenter Console (refer to *Step 46: Deploy Open Systems Agents* on page 210 for details). After installing Workload Analyzer Archiver, edit the following file:

```
<Install_root>\exec\ctg.ini
```

where *<Install_root>* is the ECC infrastructure install directory.

Add to *ctg.ini* the line shown in **bold** immediately following the *autostart =* and *restart =* lines, as shown:

```
autostart = true (could also be false—do not modify)
restart = true (could also be false—do not modify)
cluster = true
```

4. Save and exit *ctg.ini*.

Important: Before deploying Workload Analyzer Archiver on an infrastructure host in a cluster environment, refer to *EMC ControlCenter Performance and Scalability Guidelines* on Powerlink for performance considerations.

53.9 Replicate ControlCenter Registry keys

For ControlCenter to run on both cluster hosts, you must transfer ControlCenter Registry keys, environment variables, and other settings from the primary host to the shared disk, and then from the shared disk to the secondary host, using the following utilities:

- ◆ *clustersave* — Copies Registry and environment variable settings from the primary host to the shared disk.
- ◆ *clusterload* — Reads Registry and environment variables settings from the shared disk and configures them on the secondary node.

To prepare the ControlCenter environment for the backup host:

- a. Ensure that all the previous steps in this procedure completed successfully.

- b. Ensure that the primary and backup nodes are live and connected.
- c. In a command window on the primary node, change to the following directory:

```
<install_root>\tools\utils
```

 where `<install_root>` is the ECC infrastructure install directory.
- d. Enter `clustersave` and press ENTER. The `clustersave` utility does the following:
 - Changes the online ControlCenter Windows services from Automatic to Manual on the backup node.
 - Copies registry and environment variable settings from the primary host to the ControlCenter installation area on the shared drive.
- e. Shut down the two Repository services: Click **Start**, and select **Programs, Administrative Tools, Services**. In the Services window, select the following services, right-click, and select **Stop**.

```
OracleServiceRAMBDB
OracleECCREP_HOMETNSListener
```

After installation of ControlCenter, the Repository is automatically started and online. The Repository must be shut down prior to performing the Move Group command in the next step.
- f. If not online, start Cluster Administrator: Click **Start, Programs, Administrative Tools, Cluster Administrator**.
- g. From the cluster monitor console, initiate a manual failover of the resource group ECCRG to the backup node: Right click on ECCRG and choose **Move Group**.

Distributed Configuration

Perform a manual failover of the desired resource groups to the backup node, by repeating the steps above for each resource group in the cluster environment. In our example, the resource groups are:

- *Repository cluster:* ECCRR
- *ECC Server cluster:* ECCRS
- *StorageScope cluster:* ECCRT
- *Agent cluster:* ECCRA

- h. In a command window on the backup node, change to the following directory:

```
<install_root>\tools\utils
```

 where *<Install_root>* is the ECC infrastructure install directory.
- i. Enter `clusterload` and press ENTER.
- j. Reboot the backup node.

 When the backup node is rebooted, the resource group(s) will automatically fail back to the primary node (main server).
- k. Before going on to the next step, verify that the resource group(s), shared disk resources, and IP address resources are online.

53.10 Add components and products to cluster control

Create, in the specified order, the applicable ControlCenter resources for the cluster service.

Important: *Most of the resources have dependencies on all resources preceding them, so all previous resources must be online before later resources can be activated. In some cases, however, listed resources do not depend on all resources preceding them—only a subset of those resources. The recommended order of resource dependencies will ensure that all resources are started in the proper order.*

- a. Verify that the cluster is online on the primary node, and the shared disk and IP address resources are online.

Distributed Configuration

Verify that all clusters are online on the primary node (ECCGR, ECCGS, ECCGT, and ECCGA in our example), and that the shared disk and IP address resources are online.

- b. Note that the following *generic services* are to be created in this procedure:
 - OracleECC_REPHOMETNSListener
 - OracleServiceRAMBDB
 - EMC ControlCenter Server
 - EMC ControlCenter WebApplications Server
 - EMC ControlCenter API Server
 - EMC ControlCenter WebConsole Server

- EMC ControlCenter Master Agent
- EMC ControlCenter Store
- EMC ControlCenter StorageScope
- EMC ControlCenter Performance Manager Reports

Distributed Configuration

For each cluster in our sample configuration, add the following resources (this is a sample only—your distributed cluster configuration might be different):

- *Repository cluster*: OracleServicerambdb, OracleECCREP_HOMETNSListener
- *ECC Server cluster*: EMC ControlCenter Server, EMC ControlCenter WebApplications Server, EMC ControlCenter Performance Manager Reports
- *StorageScope cluster*: EMC ControlCenter StorageScope
- *Agent cluster*: EMC ControlCenter Master Agent

- Right-click the cluster name(s) (ECCRG in our example) identified in the previous step, one at a time, from the top (OracleECC_REPHOMETNSListener) to the bottom. Select **New, Resource**.

MSCS displays the New Resource wizard main screen.

- In the New Resource wizard main screen, fill in the fields as follows, and then click **Finish**:

Cluster Resource Group Resource —

Name: ECCRGOracleServicerambdb

Resource type: Generic Service

Group: ECCRG

Run this resource... [unchecked]

When creating these resources, make sure the New Resource *Service Name* field exactly matches the component's Windows Service name.

MSCS displays the Possible Owners screen, which shows the two available nodes for the cluster.

- Select both nodes. Using the Add button, move the nodes to the Possible owners column. Then, click **Next**.

MSCS displays the Dependencies screen, which shows the resources that must be brought online before the current resource.

- f. For each resource, select the name of the *previous resource* that you entered as a dependency (so each resource will be dependent on its predecessor, the predecessor will be dependent on its predecessor, and so on).

Using the Add button, move the nodes to the Resource Dependencies column. The resources are shown in order below. Setting dependencies for each resource to the one listed before it establishes all the proper dependency relationships in MSCS. For OracleServiceRAMBDB, specify a dependency on ECCRGNetworkName (the previously entered resource, from step 53.6 *Create a network name resource* on page 251).

1. OracleServiceRAMBDB
2. OracleECC_REPHOMETNSListener
3. EMC ControlCenter Server
4. EMC ControlCenter Store
5. EMC ControlCenter StorageScope
6. EMC ControlCenter API Server
7. EMC ControlCenter WebApplications Server
8. EMC ControlCenter WebConsole Server
9. EMC ControlCenter Master Agent
10. EMC ControlCenter Performance Manager Reports

- g. Click **Next**.

MSCS displays the Generic Service Parameters screen.

- h. The Generic Service Parameters screen allows you to identify the parameters that need to be provided with the service. Fill in the service name, for example:

Generic Service Parameters —

Service name: OracleServiceRAMBDB

Start parameters: [none]

Leave the **Use Network Name for Computer name** box cleared.

- i. Click **Next**.

MSCS displays the Registry Replication screen, which does not need to be populated.

- j. Click **Finish**.

You should receive a pop-up acknowledgment that the resource was successfully created.

- k. Click **OK**.
- l. For each resource, right click and select **Properties**, then in the **Advanced** tab, select *Do not restart*.
- m. Repeat the steps in this procedure for each listed service.

53.11 Enable failover for multiple Stores and Console refresh (optional)

To enable more than one Store in a clustered environment, and to have remote ControlCenter Consoles refreshed when failover occurs:

- a. On the infrastructure host(s), shut down all ControlCenter Consoles, Stores, and the ECC Server.
- b. Copy the following file to a backup location:


```
<Install_Root>\ecc_inf\data\<hostname>\data\ecc_server.ini
```

 where *<Install_Root>* is the ECC infrastructure install directory.
- c. Open `ecc_server.ini` (the original file, not the backup) with a text editor.
- d. In `ecc_server.ini`, search for the line that contains the string:


```
name server aliases.
```
- e. Add to the `name server aliases` line a comma-separated list of hostnames that correspond to the physical IP addresses bound to the same network adapter as the server's virtual IP address. Ensure that host names in `name server aliases` do not contain the server's virtual name since it is already included in the `name server URL` property.
- f. Restart the ECC Server, Stores, and ControlCenter Consoles.

53.12 Bring the cluster(s) online

Bring the new cluster online as follows:

- a. In the Cluster Administrator window, right-click on the new group's icon (ECCRG for a single host infrastructure configuration). The group's resources appear.

Distributed Configuration

In the Cluster Administrator window, right-click the icons for clusters you want to bring online, then repeat this step for each cluster. In our example, the four clusters are ECCRR, ECCRS, ECCRT, and ECCRA.

- b. For each resource, right-click and select **Bring Online**. The State column for the resource will now show Online Pending.

You may continue to bring resources online while (any) resource status shows Online Pending.

Step 54 Install ControlCenter Agents in an Application Clustered Environment

Use the steps in this section to set up ControlCenter Host Agents in a cluster environment.

EMC does not support installing host agents and infrastructure components on the same hosts in a cluster. Refer to *Install the ControlCenter Infrastructure in a Clustered Environment* on page 244 for instructions on setting up ControlCenter infrastructure components and the Workload Analyzer Archiver in a clustered environment.

Unlike installation of ECC Infrastructure components in a cluster environment, ensure that ControlCenter host agents are installed on a local drive that is *not* a shared cluster resource.

Running ControlCenter host agents on clustered hosts is supported in the following environments (refer to the *ControlCenter SP4 Support Matrix* on Powerlink for the most up-to-date supported configuration information):

- ◆ Host Agent for Windows, on hosts running Windows 2000, 2003, Microsoft Cluster Service (MSCS), and VERITAS Volume Manager (VxVM) 3.1.
- ◆ Host Agent for Solaris, on hosts running Solaris 9 and VERITAS Cluster Server (VCS) 3.5, 4.0.
- ◆ Host Agent for HP-UX, on hosts running HP-UX 11.23 and HP Serviceguard A.11.14.
- ◆ Host Agent for AIX, on hosts running HACMP 5.1 on AIX 5.2.
- ◆ Database Agent for Oracle (Proxy only).
- ◆ Common Mapping Agent (Proxy only) tolerates discovering databases in a cluster environment via proxy through Solutions Enabler running on the clustered host.
 - An ODBC Connection must be made to the virtual database on all physical nodes hosting the cluster so that the locally installed Solutions Enabler can communicate to it.
 - Refer to the *EMC Solutions Enabler* documentation for host and database types supported by Solutions Enabler in proxy mode.

Understand MSCS Cluster Support for ControlCenter

ControlCenter works with only certain features of MSCS:

- ◆ **Only active/passive clusters are supported.** In this type of cluster, a primary (active) host performs normal processing, and a secondary (passive) host restarts applications with full performance when a failure occurs on the active host. *Active/active* clusters, where both hosts run application software during normal operation and all the work is transferred to one host if a failure occurs, are not supported for ControlCenter.
- ◆ **Only two-node clusters are supported.** Although MSCS and EMC GeoSpan for MSCS support both two-node (one host failing over to another) and four-node (for up to three host failures) clusters, only two-node clusters are supported for ControlCenter.

Installing and Setting Up Agents in a Cluster

Proceed with the following steps to set up your cluster environment, installing only the desired agents for your agent cluster and using the desired cluster software. You must install the Master Agent to allow all other ControlCenter agents to run as part of the cluster environment (just as in a standalone server environment).

54.1

Install ControlCenter Master and Host Agents

You are now ready to install ControlCenter Master and Host Agents as part of a clustered environment, using the steps in this section.

Important: Install all ControlCenter Host Agents on the local drive, not on a shared resource.

- a. Install the Master Agents, using the procedure shown in *Step 45: Deploy and Start Master Agents* on page 192.

Important: When installing the Master Agent on a Windows multihomed host, select the network address that has connectivity to the ECC Server host.

- b. Install the Host Agents, using the procedure shown in *Step 46: Deploy Open Systems Agents* on page 210.

54.2 Turn off quot command operations on SUN Cluster servers

When ControlCenter host agents are deployed on SUN servers running SUN Cluster software, you must do the following to turn off quot command operations on those hosts.

- a. 1. Edit the following file on each SUN Cluster host:

```
<Install_root>\exec\ctg.ini
```

where <Install_root> is the ECC infrastructure install directory.

- b. 2. Add the following lines to ctg.ini.

```
# The following fields determine the starting time,
# frequency, and retention time (in days) for the
# USER historical data collection
hist_user_start_hour   = 0
hist_user_start_min    = 0
hist_user_freq_hour    = 0
hist_user_freq_min     = 0
hist_user_retention    = 0
```

If you do not turn off quot command operations on Sun Cluster hosts, those hosts (especially ones with large file systems) could fail and write the following to the host message file: "Issues with the quorum disk."

54.3 Set up cluster support for Database Agent for Oracle

Important: ControlCenter 5.2 allows you to monitor Oracle databases that are part of cluster environments, with the limitations described in this section. Ensure that you read and understand those limitations before you configure and enable ControlCenter cluster support for Oracle databases.

When running Database Agent for Oracle on a cluster node or via proxy (not on a cluster node) to monitor Oracle instances on cluster nodes, keep the following in mind:

- ◆ Remote Oracle database discovery requires the following configuration on the remote host:
 - Oracle Client — Used to discover database information.
 - Solutions Enabler — Used to gather filesystem information about the host OS. Refer to the *EMC Solutions Enabler* documentation for host and database types supported by Solutions Enabler in proxy mode. An ODBC Connection must

be made to the Virtual Db on all physical nodes hosting the cluster so that the locally installed Solutions Enabler can communicate to it.

- ◆ Database Agent for Oracle does not support discovery of Oracle instances that are identified by multiple TNS service names or remote TNS service names.
- ◆ For OPS or 9i RAC, ControlCenter displays only one instance (the first one found by an agent DCP). EMC recommends that you do not run multiple Database Agents for Oracle against different instances in the OPS or 9i RAC setup (because it will produce duplicate storage space).
- ◆ In a cluster environment, StorageScope does not support databases that use raw devices or raw logical volumes:
 - In the Host Database DataFiles report, all datafiles on those raw logical volumes will have a value of *Unknown* in the *Resides On* column on the secondary (passive) node.
 - In the Host Database report, *database total* and *database used* capacities will display for the secondary (passive) node.
 - In the Host Chargeback and Host By Group reports, there will be double counting when databases on both the primary (active) and secondary (passive) nodes are assigned to the same group.

For all other types of databases, StorageScope will report statistics correctly (double counting is eliminated).

- ◆ After failover to a secondary node, logical volumes used in raw database creation are not removed from Relationship View in Console interfaces. The raw logical volumes will have a value of *Unknown* in StorageScope reports.
- ◆ Performance Manager will show performance statistics for both physical nodes, no indication of cluster relationship, and no data dependency between physical nodes.

Depending on your configuration, do one of the following when running Database Agent for Oracle in a cluster environment.

- ◆ *Proxy configuration (recommended)*—If Database Agent for Oracle is running on a host that is *outside* the cluster environment (in other words, not running on a cluster node) and monitoring Oracle instances that reside on cluster nodes, after failover to the secondary cluster node, you must allow the applicable DCPs to run before data for Oracle instances on the secondary node become available in ControlCenter Console interfaces.

The DCPs and alert definitions that applied to Oracle instances on the primary node will be applied to the Oracle instances on the secondary node (so you are not required to create new ones). If you decide to create new DCPs or alert definitions for the failed over Oracle instances, ensure that you delete the previous DCPs and alert definitions.

- ◆ *Local configuration (not recommended)*—If Database Agent for Oracle is running directly on a cluster node and monitoring Oracle instances that reside on one or more cluster nodes, and the cluster nodes are running UNIX (these steps are not necessary for cluster nodes running Windows and MSCS):

- a. Ensure that the Master Agent and Database Agent for Oracle are deployed in locations that are accessible to both the primary and secondary cluster nodes.

- b. Logon to the active physical node as `root`.

- c. Edit the following file:

```
$ECC_INSTALL/exec/start_master.csh
```

- d. Add the following line to `start_master.csh`, immediately following the line `setenv ESN_ROOT /ecc/exec/esn`.

```
setenv ORACLE_HOME <your_oracle_home>
```

For example:

```
setenv ORACLE_HOME /opt/oracle/product/8.1.7
```

- e. Save and exit `start_master.csh`. Start the Master Agent.

Step 55 Troubleshoot Problems with Clusters

The issues described in this section can arise when ControlCenter runs in a clustered environment:

- ◆ *Extraneous Event Log Messages* on this page.
- ◆ *Network Name Typo* on this page.
- ◆ *Multiple IP Addresses on Same Network Adapter* on page 267.

Extraneous Event Log Messages

Symptom: When ControlCenter services fail over to a passive node, the services might send extraneous messages to the event log, for example:

The description for Event ID (0) in Source (EMC ControlCenter Master Agent) cannot be found. The local computer may not have the necessary registry information or message DLL files to display messages from a remote computer. The following information is part of the event: Stop in progress.

Reason: These messages do not indicate an actual error condition. They instead reflect a problem with the way the newly started services access the Windows EventViewer.

Action: You can safely ignore the messages.

Network Name Typo

Symptom: When failing over to the second node, the listener services do not start up.

Reason: The network name of first node was incorrectly entered. The network name is associated with the first cluster node but not the second cluster node.

Action: The correct hostname (or IP address) is the mobile ControlCenter cluster resource group name. The cluster service will configure the mobile ControlCenter cluster resource group IP address and bring it online before the listener service is started. This will allow Oracle listener service to start up on either of the cluster nodes.

Reset the values in ControlCenter initialization files:

1. Check the `listener.ora` file. Determine the network name set in that file.
2. Run `ipconfig` to see if the IP address is active.

3. If the address is active, verify the resource starting order in the resource group. Below is the required order:
 - a. Shared disk
 - b. IP address, WebApplications Server
 - c. Repository
 - d. Listener
 - e. ECC Server
 - f. Store

If the IP address is after the listener startup, listener startup will fail because the address is not yet configured by cluster.

Multiple IP Addresses on Same Network Adapter

Description: The ECC Server installation allows the user to choose from among the ECC Server host's available IP addresses for supporting client (Console, Store, StorageScope) access. Special care needs to be taken if multiple IP addresses are bound to the same network adapter.

Suppose we have the following scenario:

- ◆ `ip_x1` and `ip_x2` are bound to the same network adapter and are on the same subnet.
- ◆ `ip_x1` is specified as the interface for subnet S in the routing table. (This can be identified by using `route print` on Windows.)

If you choose `ip_x2` as one of the serving IP addresses, you must also choose `ip_x1`. However, if you chose `ip_x1`, you do not necessarily have to chose `ip_x2`. Both addresses should instead be chosen together. You must choose all IP addresses intended for serving the above-mentioned clients, or a situation like the following could occur:

- ◆ A server has three IP addresses, `ip_x`, `ip_y` and `ip_z`. Each is assigned to a different network adapter.
- ◆ Server installation chooses `ip_x` and `ip_y` for serving the clients.
- ◆ You choose to install a console on subnet Z, which is also the subnet to which `ip_z` is assigned.
- ◆ A router interconnects subnet Z and subnet X.
- ◆ The user connects to `ip_x`.

There is an internal ControlCenter problem that can cause Event Manager to fail to connect for this scenario.

Action: Since the Console is attached to subnet Z directly, `ip_z` is a natural choice for serving clients on this subnet. ECC Server installation should then choose to listen on all, including `ip_z`.

Multiple IP Addresses on Same Network Adapter: Cluster Case

To perform this procedure you must download and install a specific patch. Contact Customer Support for availability.

Description: Cluster nodes are inherently multihomed, so the previous discussions apply here. Cluster nodes also support failover, so both nodes need to be considered together.

However, the installation GUI only shows IP addresses for the installation node. You will need to find all IP addresses on the other node by using `ipconfig`.

You need to create a virtual IP address to be included in the resource group in which the ECC Server will reside. This virtual IP address is normally bound to one of the active node's network adapters, which already has a physical IP address bounded.

Action: Do the following:

- ◆ Obtain and install the correct patch from EMC. Contact Customer Support for availability.

Suppose your virtual server has IP address `ip_v`, your active node has an IP of `ip_v1`, and your backup node has IP of `ip_v2`. Suppose also that the virtual and active IP addresses are bound to the same network adapter N1, and the backup IP is bound to another network adapter N2.

After failover, your virtual server's IP address (`ip_v`) will now be bound along with your backup node's IP (`ip_v2`) to your backup node's network adapter N2.

- ◆ Choose a virtual server IP address only during installation time. After the installation, change the name `server aliases` field in the following file to add the IP addresses for both nodes:
`<Install_Root>\ecc_inf\data\<hostname>\data\ecc_server.ini`
where, `<Install_Root>` is the ECC infrastructure install directory.

For example:

```
name server aliases = ip_v1, ip_v2
```

Uninstall ControlCenter

When uninstalling ControlCenter, ensure that you uninstall all components in the order shown in this section.

- ◆ Step 1: Removing Service Pack 4 272
- ◆ Step 2: Uninstall Agents 274
- ◆ Step 3: Uninstall ControlCenter Console(s) 276
- ◆ Step 4: Uninstall Integration Packages..... 278
- ◆ Step 5: Uninstall Other Components and Products 279
- ◆ Step 6: Uninstall ControlCenter Cluster Support..... 284

Step 1 Removing Service Pack 4

To remove Service Pack 4 and return to the version of a component that you were running before the Service Pack application (5.2x), you must manually uninstall agents, run uninstall from Add/Remove Programs, and then roll back the Repository using the backup you made before applying the SP.

1. Using the ControlCenter Console, stop and uninstall all ControlCenter agents that have been upgraded to 5.2 Service Pack 4 (version 5.2.0.4.0). (Refer to the EMC ControlCenter 5.2 Planning and Installation Guide, Volume 1, Uninstall Agents.)
2. On each applicable host, stop and uninstall the Master Agent.
3. Stop all services that begin with:
 - EMC ControlCenter
 - Oracle (Repository host only)

Stop any enabled virus-checking software. If your site policy does not allow this, the install proceeds but takes an extremely long time. Some antivirus software may be monitored by Services and restarted automatically. Refer to your antivirus vendor documentation to determine if additional Services need to be stopped.

4. Close the ControlCenter Console(s) on all applicable hosts, and then uninstall ControlCenter Console Service Pack 4 using **Add/Remove Programs**. This rolls back the Console to the previous version.
5. Do the following on all hosts where ControlCenter 5.2 Service Pack 4 components are installed.
 - a. Remove EMC ControlCenter 5.2 Service Pack 4 by using **Add/Remove Programs**.
 - b. Delete `<install_root>\Repository`.
 - c. Copy `<rollback_dir>\Repository` to `<install_root>\Repository`.
 - d. Restart Oracle services.
 - e. Run: `<install_dir>\repository\admin\ramb_scripts\ramb_mediarecovery.bat`
Wait for the restore to complete (script successful message), and then manually restart EMC ControlCenter services.

If the Repository recovery fails, contact Customer Support.

6. Install the previous 5.2.0 version of the Master Agent.
7. Install the previous 5.2x version of additional agents to which you originally applied Service Pack 4.

Step 2 Uninstall Agents

This procedure explains how to use the ControlCenter Console Agent Administration Wizard to uninstall agents.

Do the following in the ControlCenter Console:

- a. If you plan to uninstall Workload Analyzer Archiver:
 1. Disable all data collection policies for the instance of Workload Analyzer Archiver to be uninstalled.
 2. If the Workload Analyzer Archiver agent to be uninstalled is for ControlCenter 5.1.1 SP3 or below, stop the **NobleNet Portmapper for TCP** service on the agent host.
 3. Stop all instances of Workload Analyzer Performance View.
- b. If you plan to uninstall the Integration Gateway, and a Microsoft Operations Manager framework resides on the target host, ensure that the OnePoint service is stopped on the target host before uninstalling the agent. If the OnePoint service is running when you try to uninstall the Integration Gateway, the uninstall will fail.
- c. To uninstall agents, right-click the **Hosts** folder in the tree panel. Select **Agents, Uninstall**.

The Console displays the Host Selection dialog box:

- Hosts that are available for the agent uninstall action are listed with selectable checkboxes, with a status of *Available*.
 - Hosts that are *not* available for the agent uninstall action are listed with grayed-out checkboxes.
- d. Select the host(s) for which you want to uninstall agents.
To select multiple hosts, click the checkboxes next to the desired hosts. If you mistakenly select a host, click the checkbox again to deselect the host.
 - e. Click **Next**.
The wizard displays the Agent Selection dialog box, which lists the agents running on the selected hosts for which the uninstall action is valid.
 - f. Select the agent(s) you wish to uninstall. Then click **Next**.

The wizard displays the Review Uninstall Agent Task dialog box, which shows the agents to be uninstalled (select the **Agents** tab), along with the hosts on which those agents are running (select the **Hosts** tab).

- g. Click **Finish**.

The Execute Now Page dialog box appears.

- h. Click **OK**.

Uninstalling the Master Agent with Sudo

1. Grant the script <MA_INSTALL_DIR>/uninstall_master.sh Sudo permission.
2. Run this script with Sudo.

Step 3 Uninstall ControlCenter Console(s)

Repeat this procedure for each Console to be uninstalled:

- ◆ 3.1 *Ensure the ControlCenter Console is not running* on this page.
- ◆ 3.2 *Remove the ControlCenter Console files* on this page.

Keep in mind that you must have one valid ControlCenter Console to manage ControlCenter agents, including uninstall.

3.1 Ensure the ControlCenter Console is not running

In the ControlCenter Console menu, select **File, Exit**, or click the close box on the ControlCenter Console window.

3.2 Remove the ControlCenter Console files

The method depends on the host operating system.

Windows

Be aware that when you launch the Install Shield Wizard to remove the ControlCenter Console files, Install Shield closes all Internet Explorer windows that are currently open on the desktop.

- a. From the **Start** menu, select **Settings, Control Panel**.
- b. Open **Add/Remove Programs**.
- c. Select **EMC ControlCenter Console**.
- d. Click **Change/Remove** to launch the InstallShield Wizard.

The welcome screen appears.

- e. Click **Next**.

The uninstall screen appears and shows the path to the location from which the ControlCenter Console will be uninstalled.

- f. Click **Next** to begin the ControlCenter Console uninstall.

The Install Shield Wizard runs automatically. Wait for it to complete.

- g. Click **Finish** to exit the wizard.

EMC ControlCenter Console is removed from the **Add/Remove Programs** list.

- h. Optional: If you have no need for the Console log files and configuration data for this Console user, delete these directories:

- %USERPROFILE%\ecc\console\data
- <install_root>\ecc\console
(the default is: %Program Files%\ecc\console\data)
where <install_root> is the ECC infrastructure install directory.

Solaris

Uninstall the application as follows:

- a. Change to the root directory:

```
cd /
```

- b. Type:

```
<ECCRootDirectory>/_uninstall/uninstaller.bin
```

- c. Optional: If you have no need for the ControlCenter Console log files and configuration data for this Console user delete these directories:

- \$HOME/ecc
- <install_root>/ecc/console
(the default is: /opt/ecc/console)
where <install_root> is the ECC Console install directory.

Step 4 Uninstall Integration Packages

Perform this procedure to uninstall the Integration Packages (if you installed them originally).

- ◆ 4.1 *Ensure the Integration Packages is not running* on this page.
- ◆ 4.2 *Remove the Integration Packages files* on this page.

4.1 Ensure the Integration Packages is not running

Refer to *EMC ControlCenter Integration Packages Product Guide* for detailed information about stopping the application.

4.2 Remove the Integration Packages files

Access the Windows installation utility as follows:

- a. From the **Start** menu, select **Settings, Control Panel**.
- b. Open **Add/Remove Programs**.
- c. Select **EMC ControlCenter Open Integration Packages**.
- d. Click **Change/Remove** to launch the InstallShield Wizard.

The welcome screen appears.

- e. Click **Next**.

The uninstall screen appears and shows the path to the location from which the Integration Packages will be uninstalled.

- f. Click **Next** to begin the uninstall.

The InstallShield Wizard now runs automatically; wait for it to complete.

- g. Click **Finish** to exit the wizard.

EMC ControlCenter Integration Packages is removed from the **Add/Remove Programs** list.

Step 5 Uninstall Other Components and Products

Use this procedure to uninstall all components and products, except agents, Integration Packages, and ControlCenter Consoles (which were uninstalled using previous steps in this section). The uninstall program will automatically stop any ControlCenter services that are running when the program is invoked.

In some cases, you might need to use a command line method to uninstall the Master Agent (such as when the Master Agent is installed on a UNIX host). Refer to *Uninstall Only the Master Agent (Using the Command Line)* on page 283.

Follow these steps:

- a. Ensure that any currently opened Windows Explorer or command windows do not have open folders within the installation tree.
- b. Ensure that any currently opened Wordpad or Notepad (or other such editors) do not have files within the installation tree opened.
- c. Stop the Distributed Transaction Coordinator Service.

From the Windows Start menu, select **Settings, Control Panel, Administrative Tools, Services**, and then right-click **Distributed Transaction Coordinator Service** and select **Stop**.

- d. From the **Start** menu, select **Settings, Control Panel, Add/Remove Programs**.

The system displays a list of components, which includes **EMC ControlCenter 5.2 Uninstall**.

- e. Click **Change/Remove** to launch the ControlCenter uninstall wizard.

The program displays the uninstall initial screen.

- f. Click **Next**.

The program displays a warning to disable any antivirus software that is currently running on the machine.

Important: Some antivirus programs might be monitored by Services and therefore restart automatically after being stopped initially. Refer to your antivirus software documentation to determine if additional Services need to be stopped.

- g. Disable any running antivirus software, if necessary. Then click **OK** to continue.

The program displays the component uninstall options in a column titled **Available Components**.

- h. If you want to uninstall *all* ControlCenter components and products from a *single host infrastructure* (all-in-one) configuration, do the following:
 1. Select *all* the components and products in the **Available Components** column.
 2. Click **Add** to move the selected items from the **Available Components** to the **Selected Components** column. Then click **Next**.

The program displays a percent-finished status bar indicating removal progress for each component. When each component's uninstall is complete, the progress bar shows 100 percent.

3. Click **Yes** to return to the (updated) initial screen.

To confirm that a component is removed, click **View** to see the revised component list, which should no longer show the removed component. Then click **Back** to exit the list.

4. Click **Exit** to close the uninstall wizard.
5. Verify that ControlCenter uninstalled successfully. Display the **Add/Remove Programs** list. **EMC ControlCenter 5.2** should no longer appear in the list. All desktop icons should also be removed.
6. Reboot the host machine.
7. Manually remove the `<ECCRootDirectory>`.

- i. If you want to uninstall *individual* (not all) ControlCenter components and products from a *single-host infrastructure* (all-in-one) or *distributed* configuration, do the following:
 1. Select the desired components and products in the **Available Components** column, ensuring that components are uninstalled in the following order (if you want to uninstall more components, you will need to repeat this step later):
 - a. Uninstall the following components first (you may install them in any order, as long as you uninstall *all* of them before you go on to step b):
 - Master Agent
 - StorageScope
 - StorageScope API
 - Store(s)
 - SupportTools
 - WebConsole Server
 - Performance Manager
 - b. Uninstall the ECC Server.
 - c. Uninstall the Repository.
 - d. Uninstall the INSTALLTOOLS component (be sure this is the *last* ControlCenter component to be uninstalled on a given host).

Distributed Configuration

Uninstall the components *on all machines* in ControlCenter in the order specified. For example, you must uninstall all Stores, on all machines, before uninstalling the ECC Server.

2. Click **Add** to move the selected items from the **Available Components** to the **Selected Components** column; then click **Next**. (If you want to uninstall more components, you will need to repeat this step later.)

The program displays a percent-finished status bar indicating removal progress for each component selected for uninstallation. When each component's uninstall is complete, the progress bar shows 100 percent.

3. Click **Yes** to return to the (updated) initial screen. (If you want to uninstall more components, you will need to repeat this step later.)

To confirm that a component is removed, click **View** to see the revised component list, which should no longer show the removed component. Then click **Back** to exit the list.

4. If you want to remove additional components, repeat steps 1 through 3 in this procedure as many times as necessary.
5. Click **Exit** to close the uninstall wizard.

Uninstall Only the Master Agent (Using the Command Line)

Use this procedure to uninstall the Master Agent if it was installed using a method *other than* the installation wizard from the ControlCenter installation CDs.

Windows

- a. Run `<ECCRootDirectory>\uninstall_master.bat`.

Wait until the uninstall is complete. If there are no more products installed to this directory, go on to the next step.

- b. Manually delete the following:
 - `uninstall_master.bat` (the batch file you ran in the previous step)
 - `<ECCRootDirectory>\` (the current directory)

UNIX

- a. Run `<ECCRootDirectory>/uninstall_master.sh`

The uninstall prompts you to ensure that all agents running on the target host are stopped (using the Console).

- b. Ensure that all agents running on the target host are stopped (using the ControlCenter Console).
- c. If there are no other products installed under `<ECCRootDirectory>` you can manually delete:
 - `uninstall_master.sh`
 - `<ECCRootDirectory>/`(base directory)

Step 6 Uninstall ControlCenter Cluster Support

This section describes how to perform a *full* uninstall of ControlCenter from a clustered environment:

- ◆ 6.1 *Uninstall ControlCenter components on all hosts* on this page.
- ◆ 6.2 *Copy the uninstall utility files* on this page.
- ◆ 6.3 *Run the uninstall utility* on this page.
- ◆ 6.4 *Verify the uninstall was successful* on page 285.

6.1 Uninstall ControlCenter components on all hosts

Follow the standard procedures for uninstalling ControlCenter components on nonclustered hosts (refer to *Uninstall ControlCenter* on page 271) for details.

6.2 Copy the uninstall utility files

From one of the hosts in the clustered environment, copy the following files to the shared E: drive using the following commands:

```
copy E:\ECC\tools\utils\regutil.exe E:\
copy E:\ECC\tools\utils\eccfiles.txt E:\
```

6.3 Run the uninstall utility

Run the following commands for each installed product, in the order shown below, on all hosts in the clustered environment:

```
cd E:\
regutil STS clean >> uninstall.log
regutil MTR clean >> uninstall.log
regutil IGT clean >> uninstall.log
regutil IGS clean >> uninstall.log
regutil IGR clean >> uninstall.log
regutil Tools clean >> uninstall.log
```

6.4 Verify the uninstall was successful

Check the `uninstall.log` file for the text `ERROR`. If it is not present, then uninstall was successful—otherwise, contact EMC Customer Support.

The uninstall is complete. It is now safe to remove the uninstall utility:

```
del E:\regutil.exe  
del E:\eccfiles.txt
```


Installing FibreZoneBridge and FibreZone CLI

This appendix describes how to install FibreZoneBridge and FibreZone CLI software on a Connectrix service processor.

Note that FibreZoneBridge and FibreZone command line interface (CLI) are typically installed by EMC Customer Support representatives.

This appendix includes the following topics:

◆ About FibreZoneBridge	288
◆ Install the FibreZoneBridge Software	290
◆ Uninstalling the FibreZoneBridge Software	291
◆ Installing the FibreZone CLI Software	292
◆ Uninstalling the FibreZone CLI Software.....	294
◆ FibreZone CLI Support Matrix	295

About FibreZoneBridge

To communicate with certain switches (refer to *EMC ControlCenter Support Matrix* on Powerlink for supported switch versions), the FibreZoneBridge must be installed on the Connectrix service processor located on the front door of the cabinet, or it must be installed on the host that is running the DSM Connect application.

DSM Connect is an EMC product designed to support stand-alone “M” series switches. Currently, SAN Manager supports the management of these switches using DSM Connect and the FibreZoneBridge. Ensure that DSM Connect has exclusive access to ports 161 and 162, and any other ports that are required for the RPC connection to the bridge, on the host where DSM Connect resides.

FibreZoneBridge must be reinstalled after every installation or upgrade of EMC Connectrix Manager (ECM) on the Connectrix service processor.

Accessing the Service Processor

To access the service processor:

1. Open the front door using a 5/16-inch hex nut driver.

The service processor is a laptop PC located on the inside of the front door.

2. Fold down the service processor and open the laptop cover. The service processor should be ON.

Preparing for Installation

Before you install FibreZoneBridge:

- ◆ Ensure that Connectrix Manager (CM) version 4.0 or higher is installed.
- ◆ Uninstall all previous versions of FibreZoneBridge, EMCFibreZoneBridge, or ZoneBridge software.
- ◆ Be aware that the FibreZoneBridge installation package includes NobleNet Portmapper for TCP. The portmapper utility allows an application (in this case, the FibreZoneBridge application) to secure a port or socket. The portmapper allocates a dedicated socket for use by the FibreZoneBridge until released by the application. If a portmapper is already installed on the service processor, you do not need to install the NobleNet Portmapper.

To check for an existing installation of NobleNet Portmapper for TCP, go to **Start, Settings, Control Panel, Services**. Then look for the **Portmapper for TCP** service.

- ◆ Understand that FibreZoneBridge does not support the use of Dynamic Host Configuration Protocol (DHCP) for dynamic allocation of IP addresses.
- ◆ Be aware that the *Secure Mode* FibreZoneBridge installation is used for authentication purposes only. This username/password pair is used when discovering McDATA switches or fabrics under the control of that Connectrix Manager service processor. To further restrict access to active fabric management operations you should configure ControlCenter users with the appropriate administrative privileges.

Install the FibreZoneBridge Software

To install the FibreZoneBridge software on a Connectrix service processor:

1. Download the latest version of the FibreZoneBridge software from the EMC Powerlink website:
<http://powerlink.emc.com>
on the Connectrix service processor.

FibreZoneBridge will check for the proper version of Connectrix Manager (refer to *EMC ControlCenter Support Matrix* on Powerlink for supported versions).

2. Install the FibreZoneBridge software using the instructions available on Powerlink.

Finish the Installation

Once you restart the service processor, the software installation is complete. Do not shut down the service processor. Complete the following steps to finish the installation.



CAUTION

Leave the Connectrix service processor running!

1. Close the service processor laptop cover and fold it up against the door.
2. Close the Connectrix door and lock it using a 5/16-inch hex nut driver.

Uninstalling the FibreZoneBridge Software

From the **Control Panel**:

1. Stop the FibreZoneBridge service.
 - a. Click **Services**.
 - b. Stop the EMCFibreZoneBridge service.
 - c. Close the Services window.
2. Remove the program files.
 - a. Click **Add/Remove Programs**.
 - b. Select EMCFibreZoneBridge to remove the program files.

Installing the FibreZone CLI Software

To install the FibreZone CLI software:

1. Insert the EMC ControlCenter installation CD #4 in the CD-ROM drive on the Connectrix CLI host.
2. Run one of the following from the CD-ROM.

- On an Windows host:

FibreZoneCLI\fz_nt_install.exe

- On a UNIX host:

FibreZoneCLI/fz_unix_install.sh

The EMC FibreZone Welcome dialog box opens.

3. Click **Next**.

A License Agreement dialog box opens.

4. Click **Next**.

If a previous version of FibreZoneCLI software is detected, you are asked if you want to overwrite it.

If you choose not to overwrite the old version, the installation is cancelled.

5. The Choose Destination Location dialog box appears. Accept the default installation root folder, C:\Program Files\EMC, or browse for another (EMC recommends that you select the default directory), and click **Next**.

When the installation is complete, the Setup Complete dialog box opens.

6. Click **Finish**.
7. Remove the ControlCenter Installation CD #4.
8. Reboot the host. You cannot use the FibreZoneCLI application until you do so.

FibreZone CLI allows you to create, manage, and store Fibre Channel zone configurations in a common database created by FibreZone CLI, on the management host. The FibreZone CLI common database is not integrated with the ControlCenter Repository. The FibreZone CLI will not populate the zoning

information into the ControlCenter Repository. A Fibre Channel Connectivity Agent discovery must be done to populate the zoning information into the ControlCenter Repository.

The default locations for the FibreZone database are:

- Windows: C:\Program Files\EMC\FibreZone
- UNIX:/usr/emc/FibreZone

Uninstalling the FibreZone CLI Software

To uninstall the software:

1. Stop the FibreZoneCLI software.
2. Do one of the following:
 - On a Windows NT or Windows 2000 host, click **Add/Remove Programs**. Then select **EMCFibreZone** to remove the program files.
 - On a UNIX host, run:

```
./FibreZoneCLI/fz_unix_uninstall.sh
```

FibreZone CLI Support Matrix

The *FibreZone CLI Support Matrix* is now maintained in the *EMC ControlCenter Support Matrix*. Refer to *EMC ControlCenter Support Matrix* on Powerlink for supported vendor hardware and firmware.

Port Usage and Firewall Configuration

This appendix describes port usage requirements for running ControlCenter through a firewall. Any agent can be located outside of the firewall.

You must configure firewall openings that correspond to the required listening ports for each ControlCenter component. This appendix describes the listening ports required for ControlCenter components. With the exception of SNMP ports 161 and 162, which use the UDP protocol, all ports use the TCP protocol.

When the term *firewall* is used, it is assumed to be an *IP stateful firewall*.

This appendix includes the following topics.

- ◆ Understanding ControlCenter NAT Firewall Support with Multihome..... 298
- ◆ Configure Communications over a NAT Firewall with Multihome..... 299
- ◆ Fibre Channel Connectivity Agent Port Usage 307
- ◆ Controlling Port 162 Usage for SNMP 310
- ◆ ControlCenter Infrastructure Port Usage 313
- ◆ ControlCenter Console Port Usage 316
- ◆ Agent-to-Infrastructure Communication Ports 318
- ◆ Workload Analyzer Archiver Port Usage..... 323
- ◆ StorageScope Port Usage 324

Understanding ControlCenter NAT Firewall Support with Multihome

ControlCenter Network Address Translation (NAT) support encompasses the following:

- ◆ Only Static NAT address translation is supported.
- ◆ Dynamic NAT is not supported.
- ◆ Port Address Translation (PAT) is not supported.
- ◆ All ControlCenter agents are supported outside the NAT firewall.
- ◆ WLA Archiver component is not supported outside the NAT firewall.
- ◆ ControlCenter Agents that communicate through a NAT firewall to a WLA Archiver agent are not supported. Hence, WLA DCPs of agents deployed outside of NAT firewall should be disabled.
- ◆ ControlCenter infrastructure components such as Repository, Server, Store, Web Console, and Console are not supported outside the NAT firewall.

Terminology

The terminology used in this appendix is based on Cisco standards. For more information refer to: www.cisco.com.

Inside local address - The IP address assigned to a host on the inside network. This is the address configured as a parameter of the computer's operating system or received via dynamic address allocation protocols such as DHCP. The address is likely not a legitimate IP address assigned by the Network Information Center (NIC) or service provider.

Inside global address - A legitimate IP address assigned by the NIC or service provider that represents one or more inside local IP addresses to the outside world.

Outside local address - The IP address of an outside host as it appears to the inside network. Not necessarily a legitimate address, it is allocated from an address space routable on the inside.

Outside global address - The IP address assigned to a host on the outside network by the host's owner. The address is allocated from a globally routable address or network space.

Configure Communications over a NAT Firewall with Multihome

When ControlCenter components reside in a private inside network behind a NAT firewall, and agents are behind another firewall with the Internet between the two NAT firewalls, you must modify ControlCenter component configurations to allow communications to occur between ControlCenter components across the firewall. Figure 13 shows an example of the NAT deployment with the Infrastructure having multihomes and it shows NIC1 of the infrastructure is used in NAT communication with NAT deployed agents. NIC2 of the infrastructure is used as second multihomed NIC and is not used in NAT communication. The subsequent sections of this appendix explain the configuration of NAT with NIC1 and the multihomed support with NIC1 and NIC2.

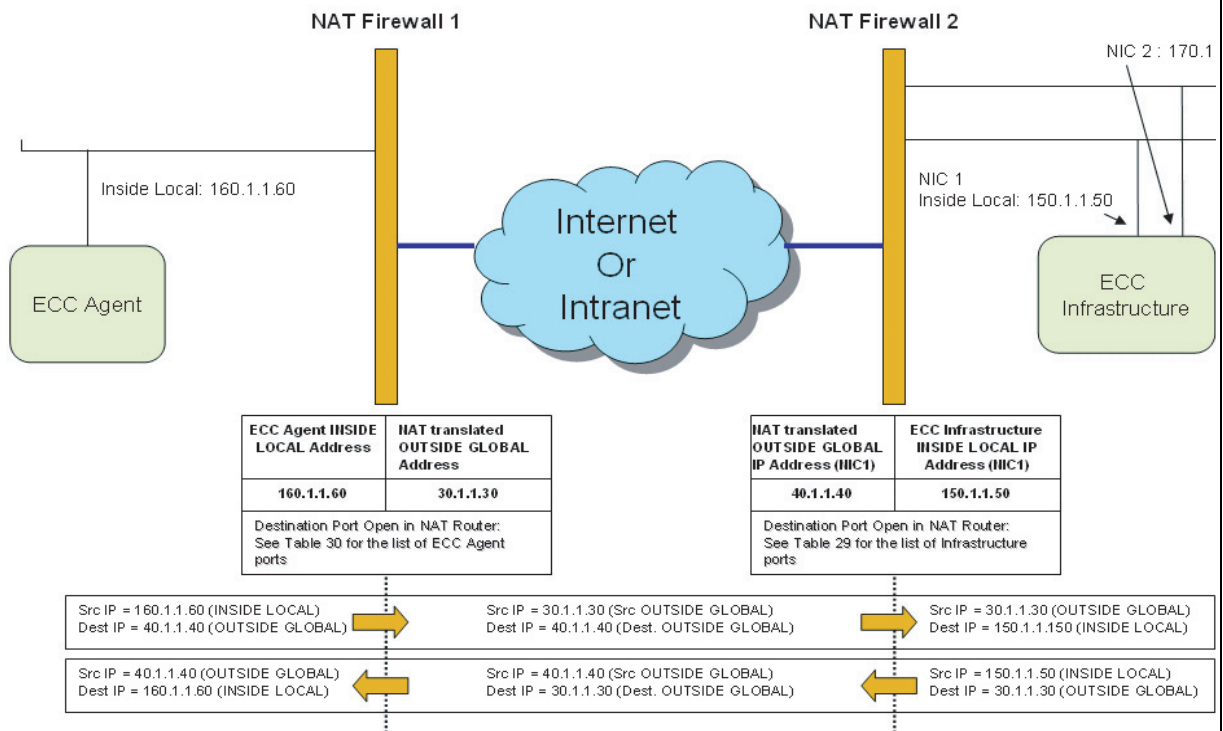


Figure 13 Sample NAT Firewall Configuration

Configuring ControlCenter for NAT Communication

NAT firewalls are set up to conceal the internal network addresses from the outside networks. Figure 13 on page 299 shows a sample NAT table of an inside local physical IP address to an outside global address. Note that the source and destination addresses traversing the Internet only contain the NAT translated outside global addresses as shown in Figure 13 on page 299, all internal inside local addresses are concealed.

- ◆ ControlCenter components (ControlCenter Agents) that reside outside the NAT firewall must communicate with the ECC Server host using the outside global IP address of the ECC Server. As shown in Figure 13 on page 299, NIC1 at the ControlCenter Infrastructure host is used in NAT communication and has the following outside global IP address translation:

Outside Global Address = 40.1.1.40

- ◆ Only ControlCenter Agents are supported outside the NAT firewall. Hence, only the Master Agent's `ctg.ini` file needs modification to support NAT communication. The following example describes the modification required to the Master Agent `ctg.ini` file for NAT communication.

Master Agent

When the Master Agent is installed and communicating to the ControlCenter infrastructure through a NAT firewall, modify the agent `ctg.ini` file to use the ECC Server outside global address as follows:

Important: This example of NAT deployment with multihome is using IP address for ease of illustrating the example of NAT address translation. The fully qualified domain name (FQDN) hostname should be used, and is recommended, in place of the IP address shown.

1. Stop all ControlCenter agents and the Master Agent.
2. Edit the following file, where `<install_root>` is the root ControlCenter install directory:

`<install_root>/exec/ctg.ini`
3. In `ctg.ini`, update the `Server Host` parameter to specify the outside global IP address of the ECC Server (NIC1) that will be used to communicate with the agent host.

In our example, because the NAT translated outside global IP address of the NIC1 is 40.1.1.40, the entry in `ctg.ini` would appear as follows:

```
# IP address of the Server
Server Host = 40.1.1.40
```

For more information on configuring agent communication ports, refer to *Agent-to-Infrastructure Communication Ports* on page 318.

MVS Master Agent

If you are using a MVS Master Agent, refer to the following information.

The MVS Master Agent (MMNSERVER) determines the network location of the ECC server from a dataset determined by the installation's `dataHLQ`, as follows:

```
dataHLQ.SSTINI
```

This exact specification for that dataset will be found in the member `MMNSERVER` in either the `dataHLQ.PROCLIB` or in the host's current JES proclib concatenation, and it should look something like:

```
//ECCINI DD DISP=SHR,DSN=dataHLQ.SSTINI(MMN520)
```

The `MMN520` member must be changed as follows:

- a. Find the line containing the string:

```
Server host = PARM
```

- b. Change the current `PARM` parameter after the `=` sign to reflect the outside global host name or IP address of the ECC server. For example:

```
Server host = ECCHOSTA
or
Server host = 40.1.1.40
```

4. Restart all ControlCenter agents and the Master Agent.

For more information on configuring Console communication ports, refer to *ControlCenter Console Port Usage* on page 316.

The ControlCenter infrastructure is now ready to communicate with ControlCenter agents across the NAT firewall.

Important: In order for communications to occur with specific agents, you must ensure that ports enabling firewall communication are open for those agents. Refer to the remaining sections of this chapter.

Configuring ControlCenter for Multihome Support

Figure 13 on page 299 shows the infrastructure with multihome using NIC1 and NIC2. Note that no change is needed in any of the ControlCenter infrastructure .ini files to support NAT. All .ini files use only the inside local or physical address of the NICs (150.1.1.50 and 170.1.1.70 of NIC1 and NIC2 respectively).

During the initial installation of ControlCenter, the installation menu prompted for selection of multihomes hostname/IP addresses. Deployment of multihome should be planned ahead as documented in *Plan the Infrastructure* on page 7.

The following section is included for completeness when a multihome environment is deployed with NAT. For cases when the planning is not done at the initial installation of ControlCenter or when the environment has been changed for multihome, this section describes the modifications needed to the infrastructure .ini files to support multihome.

Repository

Follow this procedure to enable ControlCenter multihome support:

1. On the ControlCenter Repository host, select **Start, Settings, Control Panel**, and then open **Administrative Tools**. Open **Services** and stop the following Oracle database services:

```
OracleServiceRAMBDB
OracleECCREP_HOMETNSListener
```

2. On the ControlCenter Repository host, edit the following file, where `<install_root>` is the root ControlCenter install directory:

```
<install_root>/Repository/NETWORK/ADMIN/listener.ora
```

3. In `listener.ora`, update the `ECC_Server_IP_Address` field (which follows) with the IP address of NIC1 and NIC2 from which the Repository listens to the DB connection requests.

```
(ADDRESS = (PROTOCOL = TCP) (HOST =
<ECC_Server_IP_Address>) (PORT = 1521)
```

```
(ADDRESS = (PROTOCOL = TCP) (HOST =
<ECC_Server_IP_Address>) (PORT = 1521)
```

In our example, the IP address for one of the two ECC Server listening NIC1 and NIC2 are entered in the described field (shown next).

```
(ADDRESS = (PROTOCOL = TCP) (HOST = 150.1.1.50) (PORT
= 1521)
```

```
(ADDRESS = (PROTOCOL = TCP) (HOST = 170.1.1.70) (PORT
= 1521)
```

Figure 14 shows sample code from the `listener.ora` file.

Important: This example of NAT deployment with multihome uses the IP address for ease of illustrating the NAT example. The FQDN hostname should be used, and is recommended, in place of the IP address shown.

```
LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS_LIST =
        (ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC0))
      )
      (ADDRESS_LIST =
        (ADDRESS = (PROTOCOL = TCP) (HOST = 150.1.1.50) (PORT = 1521)
        (ADDRESS = (PROTOCOL = TCP) (HOST = 170.1.1.70) (PORT = 1521)
        )
      )
    )
  )
)
```

Figure 14 Sample Code from `listener.ora` file

4. Save and exit `listener.ora`.
5. Restart the Oracle services that you stopped earlier in this procedure.

ECC server.ini File Modifications for Multihome

Important: This example of NAT deployment with multihome uses the IP address for ease of illustrating the NAT example. The FQDN hostname should be used, and is recommended, in place of the IP address shown.

6. On the ECC Server host, select **Start, Settings, Control Panel**, and then open **Administrative Tools**. Open **Services** and stop the following service:

```
EMC ControlCenter Server
```

7. On the ECC Server host, edit the following file, where `<install_root>` is the root ControlCenter install directory:
`<install_root>/ecc_inf/<hostname>/data/ecc_server.ini`
8. In `ecc_server.ini`, update the `ECC_Server_IP_Address` field shown below to specify the IP address for an ECC Server listening port:

```
[Voyager]
name server url = //<ECC_Server_IP_Address>:30751
```

In our example, the IP address of the first ECC Server NIC1 is entered in the described field:

```
[Voyager]
name server url = //150.1.1.50:30751
```

9. Specify the additional NIC IP addresses on the `name server aliases` parameter in `ecc_server.ini`. The hostnames or IP addresses specified on `name server aliases` parameter must be different than the one specified on `name server url`.

In our example, the IP address of the second ECC Server NIC2 is entered in the described field:

```
name server aliases = 170.1.1.70
```

By populating `name server aliases`, it will allow Consoles (for instance), on the additional network to communicate with the Server.

10. Specify the IP addresses of the ECC Server NIC1 and NIC2 on the `Database Host Name` parameter in `ecc_server.ini`. For example:

```
Database Host Name = 150.1.1.50, 170.1.1.70
```

11. Save and exit `ecc_server.ini`.

12. Restart the EMC ControlCenter Server service that you stopped earlier in this procedure.

ECC store.ini File Modifications for Multihome

It is important to understand that a multihome Store can use one of two paths, NIC1 or NIC2, to communicate to the ECC Server and Repository. This applies to a Store in the single-host infrastructure or an external Store in a distributed configuration.

In this example, NIC1 is the communication path from the ECC Store. It is important that the Repository is also listening on NIC1 at port 1521 and the Server is listening on NIC1 at port 30751 to complete the communication paths for the Store connection request as shown previously.

Important: This example of NAT deployment with multihome uses the IP address for ease of illustrating the example of NAT address translation. The FQDN hostname should be used, and is recommended, in place of the IP address shown.

13. On the ECC Store host, select **Start, Settings, Control Panel**, and then open **Administrative Tools**. Open **Services** and stop the following service:

EMC ControlCenter Store

14. On the ECC Store host, edit the following file, where `<install_root>` is the root ControlCenter install directory:

`<install_root>/ecc_inf/<hostname>/data/ecc_store.ini`

15. In `ecc_store.ini`, update the `ECC_Server_IP_Address` field shown next to specify the IP address for an ECC Server listening port:

Server host= `<ECC_Server_IP_Address>`

In our example, the IP address of the first ECC Server NIC1 is entered in the described field:

Server host= **150.1.1.50**

16. In `ecc_store.ini`, update the `ECC_Server_IP_Address` field shown next to specify the IP address for an ECC Server listening ports:

[Voyager]

name server url = `//<ECC_Server_IP_Address>:30751`

Login url = `////<ECC_Server_IP_Address>:30721`

In our example, the IP address of the chosen ECC Server NIC1 is entered in the described field:

```
[Voyager]
```

```
name server url = //150.1.1.50:30751
```

```
login url = //150.1.1.50:30721
```

17. Save and exit `ecc_store.ini`.
18. Restart the EMC ControlCenter Store service that you stopped earlier in this procedure.

Fibre Channel Connectivity Agent Port Usage

For communications to occur over a firewall between switches and Fibre Channel Connectivity agent, ensure that the ports listed in Table 60 are open. For switches that are not listed, refer to the documentation for those specific switches.

For all switches in Table 60, the *client initiator port* is dynamic, except for SNMP, which is dynamic by default, but can be configured to a fixed set of port numbers in the SNMP configuration file (see *Fixing FCC Agent Ports for SNMP* on page 308 for details).

Table 60 Switch Ports for FCC Agent Firewall Communication

Vendor	Interface	Protocol	Proxy/Switch Server Listening Port
Brocade	SNMP	UDP	161 ^a
	FAL	TCP	80, 111, 600-1023 (for firmware 2.x, 3.0, 4.0.x)
			80, 111, 897 (firmware 3.1.x, 4.1.x and higher, nonsecure fabric)
			80, 111, 898 (firmware 3.1.x, 4.1.x and higher)
McDATA	SNMP	UDP	161 ^a
	EMC SWAPI	TCP	111, 4023 ^b , 3127 ^b
	McDATA SWAPI via proxy		111, 59521 ^b , 59520 ^b
	McDATA SWAPI direct		2048
CNT	SNMP	UDP	161 ^a
	SWAPI	TCP	4000 ^a , ICMP
	SWAPI	TCP	4001
CISCO	SNMP	UDP	161 ^a
QLogic	SNMP	UDP	161 ^a
	SWAPI		5000

a. Default - might be configurable on switch, service processor, or SAN Manager Console.

b. Default - configurable by authorized personnel.

Fixing FCC Agent Ports for SNMP

The ports that FCC Agent uses to receive SNMP replies are dynamic by default, as shown in Figure 15.

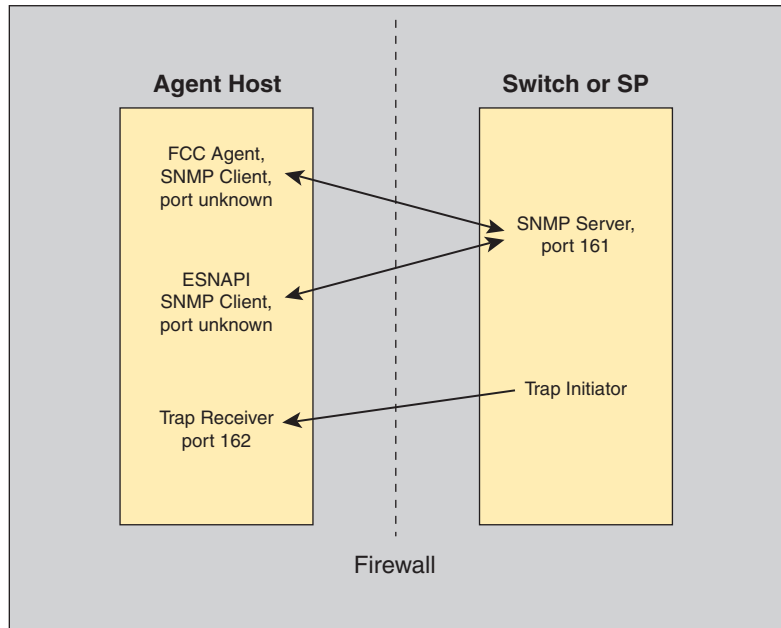


Figure 15 SNMP Communications between FCC Agent and Switch or SP

To provide higher security for switches and service processors, ControlCenter allows you to specify fixed port numbers for SNMP communications with FCC Agent, as follows.

1. Stop FCC Agent, using the ControlCenter Console.
2. Edit the following file, where `fcc_agent_home` is the root directory where Fibre Channel Connectivity Agent is installed.
`<fcc_agent_home>/conf/conf.txt`
3. In `conf.txt`, locate the following strings.
`<SNMPCLIENTPORT>`
`</SNMPCLIENTPORT>`
4. Between `<SNMPCLIENTPORT>` and `</SNMPCLIENTPORT>`, enter port numbers to be tried for SNMP communications, as shown below.

Important: The port numbers must be no lower than 1024 and no higher than 65535. If you are implementing a firewall, EMC recommends that you use ports 3127 and 4023.

The following example indicates that FCC Agent is to select any port from the following list for SNMP communications: 3127, 4023, 9004, 9006, 9007, 9008, 9009, or 9010.

```
<SNMPCLIENTPORT>  
3127 4023  
9004  
9006-9010  
</SNMPCLIENTPORT>
```

Important: If you specify a range of ports, do not include spaces between the hyphen and the port numbers.

Note: If you do not specify any ports between `<SNMPCLIENTPORT>` and `</SNMPCLIENTPORT>`, the ports that FCC Agent uses to receive SNMP replies will continue to be dynamic.

5. Save `conf.txt`.
6. Start FCC Agent, using the ControlCenter Console.

The agent will perform SNMP communications with switches using the ports specified in `conf.txt`.

Controlling Port 162 Usage for SNMP

By default, Storage Agent for NAS and Fibre Channel Connectivity Agent both require exclusive access to port 162 so they can listen for SNMP traps from devices that they manage. If both agents run on the same host, the first agent to obtain access to port 162 blocks the other agent from receiving SNMP traps, so the blocked agent cannot send ControlCenter alerts. Any other process that uses port 162 to listen for block these agents from receiving SNMP traps.

To avoid conflicts on port 162, EMC recommends that you do not install Storage Agent for NAS and Fibre Channel Connectivity Agent on the same host, and do not install either agent on a host that is already running software that requires access to port 162. This allows all software that requires access to port 162 to function normally with no additional configuration updates.

If you must install Storage Agent for NAS and Fibre Channel Connectivity Agent on the same host, or you must install one or both agents on the same host that is already running software that requires access to port 162, do *one* of the following.

- ◆ Change the port where Fibre Channel Connectivity Agent listens for SNMP traps (see *Changing the FCC Agent Listening Port* below).
- ◆ Change the port where Storage Agent for NAS listens for SNMP traps (see *Changing the Storage Agent for NAS Listening Port* on page 311).

Changing the FCC Agent Listening Port

This section describes how to change the port where Fibre Channel Connectivity Agent listens for SNMP traps.

Important: This procedure requires that you reconfigure switches to send SNMP traps to the new port, which is not supported for Brocade switches. If you use Brocade switches, do *not* change the <SNMPTRAPPORT> port setting in the `conf.txt` file. Brocade switches can *only* send SNMP trap information to port 162 (unlike Cisco and McData switches).

Edit the following file, where `fcc_agent_home` is the agent root installation directory on the agent host:

```
<fcc_agent_home>/conf/conf.txt
```

7. In `conf.txt`, find the following lines. Then change 162 (on the second line) to the new port number:

```
<SNMPTRAPPORT>
162
</SNMPTRAPPORT>
```

8. Save `conf.txt` and exit the file.

Fibre Channel Connectivity Agent might use UDP port 161 to exchange information between the agent and the devices managed by the agent. This will vary by device and software level within the device. If a firewall separates the agent host from the device, port 161 and 162 must be open in both directions through the firewall.

Changing the Storage Agent for NAS Listening Port

Change the port where Storage Agent for NAS listens for SNMP traps as follows:

Important: This procedure requires that you configure the Celerra Network Server to send traps to the new listening port. If you are using Storage Agent for NAS to monitor Network Appliance (NetApp) devices, you cannot change the Storage Agent for NAS listening port (NetApp devices do not support that change). In that case, alternatively consider changing the listening port for Fibre Channel Connectivity Agent or other software that requires access to port 162.

1. Ensure that Storage Agent for NAS is stopped.
2. Edit the following file:

```
<path_to_agent_install_dir>/cnn.ini
```

where `<path_to_agent_install_dir>` is the path to the directory where Storage Agent for NAS is installed. For example:

```
C:\ecc\exec\CNN520\cnn.ini
```

3. Add the following entry to the `cnn.ini` file (the position does not matter, as long as it does not disrupt the current contents - for example, you could add it to the end of the file):

```
[snmp]
```

```
port = <port_number>
```

where `<port_number>` is the port where Storage Agent for NAS is to listen for SNMP traps.

4. Configure the Celerra to send traps to the host where Storage Agent for NAS is running. Enter the following line in `/nas/site/trap.cfg` on the Celerra:

```
snmpmanager <ip_address>:<port_number>; communityname public
```

where `<ip_address>` is the IP address of the host running Storage Agent for NAS, and `<port_number>` is the port number where Storage Agent for NAS will listen for SNMP traps.

For example:

```
snmpmanager 127.127.127.127:163; communityname public
```

Integration Gateway

The Integration Gateway sends ControlCenter alerts to third-party management products as SNMP traps. If a firewall exists between the Integration Gateway and a Framework, ensure that the ports described below are open.

- ◆ The agent sends SNMP traps to the Framework's destination SNMP port 162 and listens on port 1273 for incoming `ecc3pi` or MIB browser SNMP requests.
- ◆ The Framework listens on ports 161 and 162, and sends to Integration Gateway Agent's port 1273 if the `ecc3pi` process is running (active integration).

Dynamic IP Address and DHCP Support

EMC does not recommend that you implement dynamic IP addressing or DHCP support in ControlCenter configurations. Hosts in the configuration must know where ControlCenter components and products reside, which requires static IP addresses for the infrastructure. Dynamic IP implementation cannot deliver the manageability and security requirement to meet the complex management software needs.

ControlCenter Infrastructure Port Usage

This section describes port usage for the ECC Server, Repository, and Store infrastructure components.

Repository

When installing the Repository, select the *Enable ECC Repository Access via a Firewall* option to fix the Repository port number at 1521, disallowing later dynamic port assignment by the network and allowing the Repository to be configured for access through a firewall. If you do not select that option, dynamic port assignment by the network might render the Repository inaccessible through a firewall.

Store

Each instance of the Store has a configured port that is derived by adding two to the ECC Server's default configured port. In addition, the Store has a second listening port that is dynamic. The Store's configured port and the second port may be configured separately by adding the following lines to `ecc_store.ini`:

```
use fixed port = true
store port = 5801
client base port = 30730
```

In this example, the Store opens two listening ports: 5801 and 30730. If `use fixed port` is false, the configured port is derived as described above, and a dynamic port is used for the second listening port.

ECC Server Connection Process

The ECC Server requires the following ports (by default) to be accessible to the ControlCenter Console through a firewall:

- ◆ 5799 (ECC Server port)
- ◆ 30721 (Login URL port)
- ◆ 30750 (plain server port)
- ◆ 30751 (name server port)
- ◆ 30753

Ports 30721, 30750, 30751, and 30753 must be open for Console access. Port 30753 is a derived value that is two higher than the greater of the plain server port and the secure server port. The secure server port is defined as 30751 in the following file:

```
<install_root>\ecc_inf\data\<hostname>\data\ecc_server.ini
```

where `<install_root>` is the root ControlCenter install directory.

Port 30722 is also a derived port number opened by the ECC Server and is used by the Store when logging into the ECC Server. The ECC Server and Store are generally not separated by a firewall.

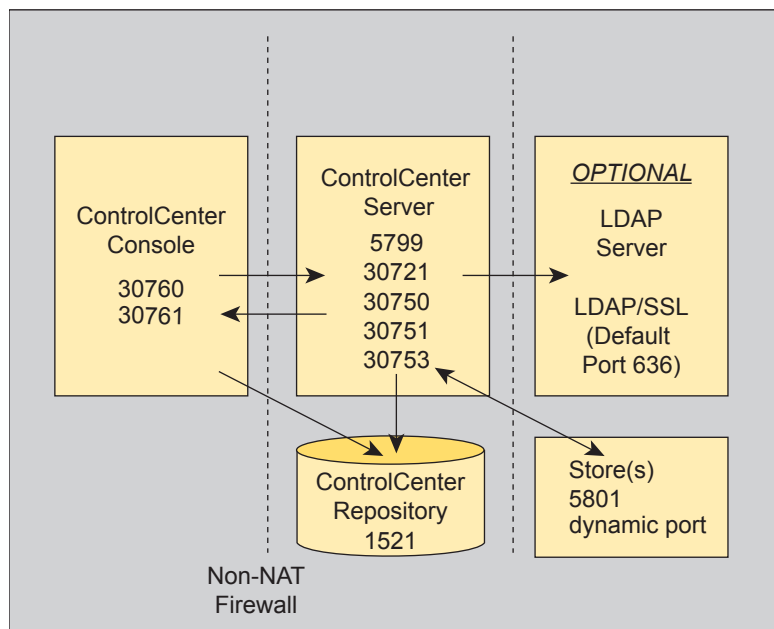
The ECC Server listening ports are configured in the `ecc_server.ini` file, with the exception of the derived port values noted above, and may be changed if necessary to conform to needs of the environment. If you change port numbers, be aware of the derived port numbers and configure your firewalls according to your new ports.

The following table describes the ports required for communication between the ECC Server and other ControlCenter components:

Table 61 **Ports for ECC Server Communications**

Component	Component Ports	ECC Server Ports
ControlCenter Consoles	30760 and 30761 (can be altered in <code>ecc_console.ini</code> refer to <i>ControlCenter Console Port Usage</i> on page 316 for details)	5799, 30721, 30750, 30751, 30753
Stores	5801, dynamic port	5799, 30722
Agents	See Table 62 on page 320	5799

Figure 16 shows the Console and the ECC Server communicating over a firewall.



CC-000233

Figure 16 ControlCenter Console-to-Server Communication

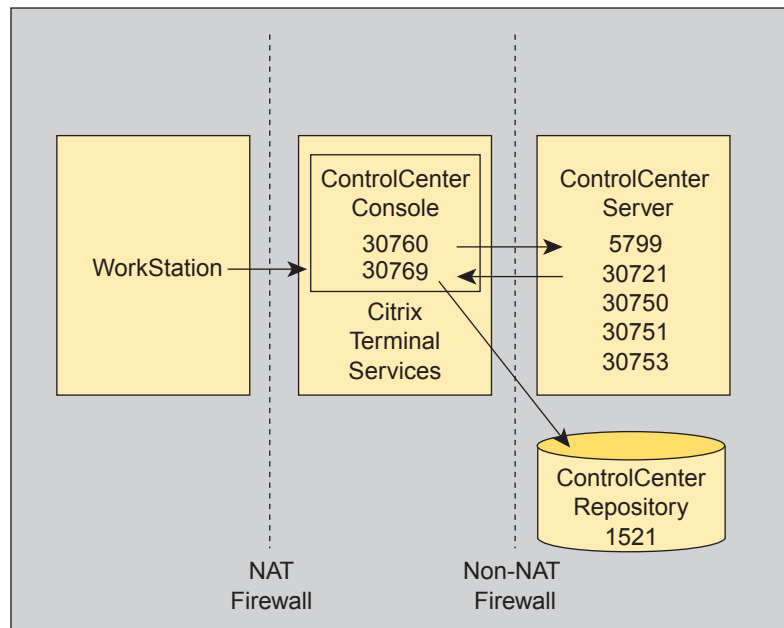
The ECC Server may be configured to perform user authentication against an LDAP directory. It is possible, though unlikely, that a firewall would be placed between the ECC Server and the LDAP server or one of its backup LDAP servers. Should this be the case, the firewall must allow the ECC Server to connect to its primary and backup LDAP servers using the LDAP/SSL port used by the LDAP servers.

ControlCenter Console Port Usage

When installing the Console use port 30000 and use port 7070 if installing the Web Console.

The ControlCenter Console can communicate with the ECC Server through a firewall (NAT or non-NAT):

- ◆ To configure ControlCenter communications with the ECC Server across a NAT firewall, refer to *Understanding ControlCenter NAT Firewall Support with Multihome* on page 298.
- ◆ For both NAT and non-NAT firewalls, ensure that the listening ports shown in Figure 17 are open on the appropriate ControlCenter Console hosts.



CC-000232

Figure 17 Accessing the ControlCenter Console across a Firewall

Specifying Console Listening Ports

The ControlCenter Console uses dynamic listening ports by default. Do the following to tell the Console to use a specific range of ports.

1. Edit the following file.

```
<console_install_root>\data\ecc_console.ini
```

where *<console_install_root>* is the ControlCenter Console install directory.

2. Update the following three parameters in `ecc_console.ini` to appear as follows.

```
use fixed port = true
```

Tells the Console to use the fixed listening ports starting at the value of `client base port` (shown below).

```
max consoles per host = 1
```

The number of ports in the range is two times the value specified by this parameter. In this example, ports 30760 to 30761 would be used by the Console. If multiple instances of the Console to be accessed using Citrix or Terminal Services (refer to *Step 23: Consider Services for Remote Access* on page 105 for details) the maximum number of Console instances that you expect to run on that host must be specified on this parameter.

```
client base port = 30760
```

This is the starting value at which the range of fixed Console listening ports begins. The Consoles will select from available ports in the range from the client base port number through twice the number specified on `max consoles per host` minus 1.

For example, if you set `max consoles per host` to 5, and the client base port is set to 30760, Consoles will attempt to open ports in the range 30760 to 30768, as shown in Figure 17 above.

Agent-to-Infrastructure Communication Ports

Each ControlCenter agent has an `.ini` file in the following directory:

```
<install_root>\exec\<agent_acronym>
```

where `<agent_acronym>` is the three letter acronym corresponding to the agent (refer to Table 62 on page 320 for the acronyms) and `<install_root>` is the ControlCenter root installation directory on the target host.

Each agent `.ini` file contains the following line:

```
ECC Agent Port = xxxxx
```

where `xxxxx` is the specific listening port used by the agent. The Server and Store communicate with the agent via this port.

The Master Agent uses the `MGA.ini` file in the `MGA510` directory. The `ECC agent port` parameter is required in the `MGA.ini` file.

In a multihomed environment (refer to *Step 5: Plan for ControlCenter Multihoming (Optional)* on page 17 for details), you can specify the network interface card (NIC) to be used for ControlCenter communications as follows:

1. Edit *one* of the following:

- `<install_root>\exec\ctg.ini`
where `<install_root>` is the ControlCenter root installation directory
- The agent `.ini` file

EMC recommends that you update `ctg.ini` because the change will apply to *all agents* installed on the host. If you update individual agent `.ini` files, the changes will apply only to the individual agents.

2. Enter the following line in the file:

```
ECC Agent IP = xxxxx
```

where `xxxxx` is the IP address of the NIC that is to listen for ControlCenter communications. For example, this is useful when you want to specify that all agent to ECC Server/Store communications are to occur on the management LAN, rather than the production LAN (specify the IP address of the NIC that is connected to the management LAN).

Table 62 on page 320 shows ControlCenter agent port usage.

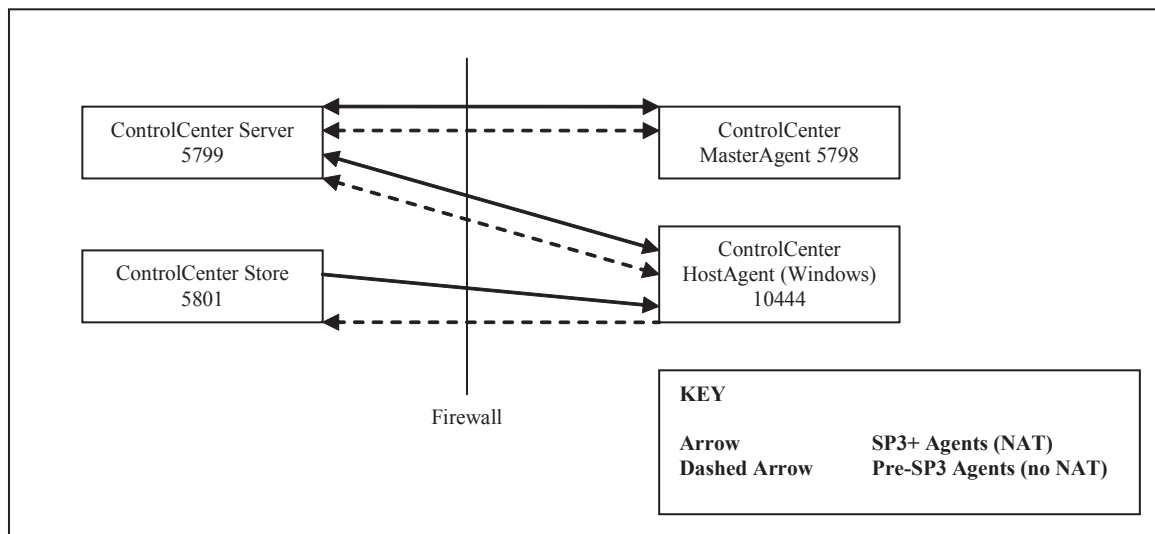


Figure 18 ControlCenter Infrastructure and Agents

- ◆ NAT-ed firewalls are supported only from SP3 (agents) onwards:
 - Infrastructure components should always reside on the same side of a NAT-ed firewall; the agent can reside on both sides.
- ◆ Non-NAT firewalls can be supported with pre-SP3 agents. In this case, the listening port 5801 on the Store needs to be opened.
- ◆ For any firewall
 - Listening ports of Agents (see Table 62) residing on the opposite side of the firewall to the infrastructure must be opened.
 - Listening ports of Infrastructure components need to be opened (depending on deployment).
- ◆ WLA Archiver is not supported in NAT environments, unless both agent collecting WLA data and the WLA Archiver are run on the same side of the firewall as ControlCenter Server.

The following table shows agent acronyms, listening ports, platforms, process names, and filenames.

Table 62 Agent Acronyms, Listening Ports, Processes, Filenames

Agent Name	Acronym	Listening Port	Platforms	Process Name	Filename
Common Agents					
Master Agent	MGA	5798	Windows	mstragent.exe	MGA.ini
			AIX, HP-UX, Solaris, Linux	mstragent	
Integration Gateway	CNG	10666 ^a	Windows	cngagent.exe	CNG.ini
			Solaris	csgagent	CSG.ini
Workload Analyzer Archiver	ENW	11000	Windows	enwagent.exe	ENW.ini
Common Mapping Agent	EGZ	10777	Windows	egzagent.exe	EGZ.ini
			Solaris	egzagent	
Backup Agents					
Backup Agent for Tivoli Storage Manager	MNY	11026	Windows	mnyagent.exe	MNY.ini
	MSY		Solaris	msyagent	MSY.ini
	MHY		HP-UX	mhyagent	MHY.ini
	MAY		AIX	mayagent	MAY.ini
Backup Agent for Legato NetWorker	MNN	11023	Windows	mnnagent.exe	MNN.ini
	MSN		Solaris	msnagent	MSN.ini
	MHN		HP-UX	mhnagent	MHN.ini
	MAN		AIX	managent	MAN.ini
Backup Agent for EDM	EGB	11015	Solaris	egbagent	EGB.ini
Backup Agent for VERITAS NetBackup	MAB	11014	AIX	mabagent	MAB.ini
	MHB		HP	mhbagent	MHB.ini
	MNB		Windows	mnbagent.exe	MNB.ini
	MSB		Solaris	msbagent	MSB.ini
Connectivity Agents					

Table 62 Agent Acronyms, Listening Ports, Processes, Filenames (continued)

Agent Name	Acronym	Listening Port	Platforms	Process Name	Filename
Symmetrix SDM Agent	EGF	11031	Windows	egfagent.exe	EGF.ini
			Solaris, HP-UX, AIX	egfagent	
Fibre Channel Connectivity Agent	EGN	11011	Windows	egnagent.exe	EGN.ini
			Solaris, HP-UX, AIX	egnagent	
Database Agents					
Database Agent for Oracle	EGO	10999	Windows	egoagent.exe	EGO.ini
			Solaris, HP-UX, AIX	egoagent	
Host Agents					
Host Agent for AIX	MAR	11018	AIX	maragent	MAR.ini
Host Agent for HP-UX	MHR	11021	HP-UX	mhragent	MHR.ini
Host Agent for Linux	MLR	10555	Linux	mlragent	MLR.ini
Host Agent for Novell	MVR	11013	Novell	mvragent.exe	MVR.ini
Host Agent for Solaris	MSR	10555	Solaris	msragent	MSR.ini
Host Agent for Windows	MNR	10444	Windows	mnragent	MNR.ini
Storage Agents					
Storage Agent for NAS	CNN	10667	Windows	cnnagent.exe	CNN.ini
Storage Agent for CLARiiON	MGL	11041 ^b	Windows	mglagent.exe	MGL.ini
			Solaris, HP-UX, AIX	mglagent	
Storage Agent for Centera	CGC	11042 ^c	Windows	cgcagent.exe	CGC.ini
Storage Agent for ESS	MGC	11045 ^d	Windows	mgcagent.exe	MGC.ini
Storage Agent for HP StorageWorks	MNQ	11024	Windows	mnqagent.exe	MNQ.ini
Storage Agent for HDS	MGD	11027	Windows	mgdagent.exe	MGD.ini
			Solaris, HP-UX, AIX	mgdagent	

Table 62 Agent Acronyms, Listening Ports, Processes, Filenames (continued)

Agent Name	Acronym	Listening Port	Platforms	Process Name	Filename
Storage Agent for Symmetrix	EGS	10222	Windows	egsagent.exe	EGS.ini
			Solaris, HP-UX, AIX	egsagent	
	N/A		Supported proxy hosts	depends on platform	depends on platforms
EMC Invista Agent	FGX	11051	Windows	fgxagent.exe	fgx.ini

- a. TCP and UDP access on all access node IP addresses for port 1273 (in both directions) is required to access frameworks through a firewall.
- b. If the agent needs to go through a firewall to access the CLARiiON, the agent requires TCP and UDP access on all access node IP addresses, in both directions, for port 6389.
- c. If the agent needs to go through a firewall to access the Centera, the agent requires TCP and UDP access on all access node IP addresses, in both directions, for port 3218.
- d. If the agent needs to go through a firewall to access the IBM ESS array, the agent requires TCP and UDP access on all access node IP addresses, in both directions, for port 443.

Workload Analyzer Archiver Port Usage

Workload Analyzer Archiver communicates through port 30103 by default, and Performance Manager requires that port 30103 is enabled in a firewall setting.

To change the port used by Workload Analyzer Archiver, update the following files on all hosts that run the listed components:

- ◆ Workload Analyzer Archiver:

```
<install_dir>/exec/enw510/ENW.ini
```

The field in ENW.ini is: report server port

- ◆ ECC Server: <install_root>/WLAXML.ini
where <install_root> is the ControlCenter root installation directory.

- ◆ Performance Manager—One of the following:

- Windows NT:

```
C:\WINNT\<username>\Application Data\WLA\WLA.ini
```

- Windows 2000, XP, and 2003:

```
C:\Documents and Settings\<username>\Application  
Data\WLA\WLA.ini
```

Important: All three files (ENW.ini, WLA.ini, and WLAXML.ini) must contain the same port information. If not, communication between the Workload Analyzer Archiver, Performance Manager, and Performance Manager Automated Reports will not function properly.

By default, the Workload Analyzer Web interface for viewing reports of the performance archives also uses port number 30103. To change this port, add the following line after the Alias and UserID lines in WLA.ini:

```
ReportServerPort=<port_number>
```

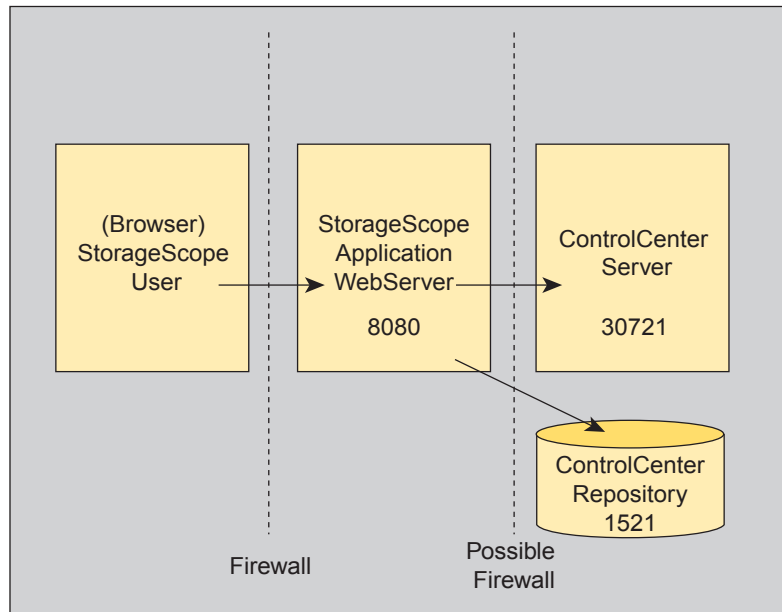
The EMC ControlCenter Performance Manager Automated Reports service uses port 30002 as the default HTTP server port. When communicating through a firewall, the service connects to the Repository using port 1521 and to the ECC Server on port 30721.

StorageScope Port Usage

StorageScope uses the following ports:

- ◆ 8080 - default HTTP server port, which may be changed during installation. When one or more StorageScope sites access StorageScope through a firewall, ensure that port 8080 is left open so StorageScope communications can occur through the firewall.
- ◆ 8005 - service port internal to the application and has no bearing on firewall configurations, but may conflict with other applications.

StorageScope connects to the Repository using port 1521 and to the ECC Server on port 30721, as shown in Figure 19.



CC-000231

Figure 19 StorageScope Port Usage

Refer to *EMC StorageScope Reference Guide* for details about changing StorageScope ports.

Alternate Methods for Installing the Master Agent

This appendix describes alternate methods for distributing the ContolCenter Master Agent.

Important: EMC recommends that you use the methods discussed in this appendix to distribute the Master Agent.

This appendix contains the following topics:

- ◆ Install the Master Agent with the Push Utility 326
- ◆ Install the Master Agent with UNIX Package Tools 330

Install the Master Agent with the Push Utility

The *multihost push utility* “pushes” the Master Agent (transfers a file containing all the Master Agent information entered during an initial Master Agent installation) to any number of remote hosts and starts it on those hosts.

Important: Do not use the Windows graphical interface method (see *Deploy the Master Agent on Windows (GUI)* on page 193 for details) to install the first instance of the Master Agent. The push utility is only supported when the first instance of the Master Agent is installed from the command line.

The utility supports Windows and UNIX platforms, but you can use it for only one platform at a time. For example, you can invoke the utility once to push the Master Agent from one AIX host to any number of AIX hosts, but you must invoke the utility a second time for Windows hosts, a third time for Solaris hosts, and so on.

Use this utility when you have several remote hosts with the same platform that require the Master Agent, but you want to save the time and effort involved with repeating the standard installation procedure for each target host. Perform the following steps:

- ◆ *Ensure that Target Hosts are Ready for Installation* on page 327.
- ◆ *Install the First Master Agent Instance* on page 327.
- ◆ *Use the Multihost Push Utility to Distribute the Master Agent* on page 328.



CAUTION

The *multihost push utility* requires an input file that contains host names, usernames, and cleartext passwords. The cleartext passwords will transfer across the network during Telnet and FTP operations. Be aware of the security concerns this creates before proceeding.

Ensure that Target Hosts are Ready for Installation

To ensure that the installation will complete successful, ensure that the remote hosts:

- ◆ Have active FTP and Telnet servers that accept logins from the root or administrator accounts
- ◆ Support telnet session prompts that end with the following characters:
 - Windows: >
 - UNIX: \$, %, #, or > (each of these characters must be followed by a space)
- ◆ Match the default root directory of the FTP server to the root of the directory where the *multihost push utility* runs, (for example, C:\ or /).

The FTP server allows write access in order to create destination directories and files. Because the *multihost push utility* tries to install the Master Agent onto the same drive where the source file was installed, that drive must be available for writing.

The *multihost push utility* might not be able to parse remote command results if extra information is present on the screen. For example, if `.cshrc` on the remote host echoes information.

Install the First Master Agent Instance

Before you install the first instance of the Master Agent prepare the push utility according to the directions for your operating system.

Windows

1. Enter the following command in a DOS window to create the `EMC_ENABLE_PUSHMA` environment variable:

```
set EMC_ENABLE_PUSHMA=x
```

2. In the same window, change the current directory to the CD-ROM drive (for example, D:).
3. Enter the following command:

```
install_master.bat
```

4. Continue with step d in *Deploy the Master Agent on Windows (Command Line)* on page 195 to complete the Master Agent installation.

**Use the Multihost
Push Utility to
Distribute the Master
Agent**

UNIX

1. Enter the following command in a Korn or Bourne shell window, to create the EMC_ENABLE_PUSHMA environment variable:

```
EMC_ENABLE_PUSHMA=x; export EMC_ENABLE_PUSHMA
```

2. In the same window, enter the following command:

```
install_setup.sh <mount_point>
```

where *<mount_point>* is the mount point for the ControlCenter installation CD-ROM.

3. Continue with step c in *Deploy the Master Agent on UNIX (Command Line)* on page 196 to complete the Master Agent installation.

After installation on the target host, the entire installation directory is automatically zipped into a compressed file.

Ensure that the original installation (from which the zip file was created) starts and connects to the ECC Server correctly.

1. Change the directory to:

- Windows: *<install_root>\exec*
- UNIX: *<install_root>/exec*

where *<install_root>* is the root directory for Master Agent installation.

2. Delete any entries currently in *Hosts.txt*.

3. Enter information for the target host in the following format:

- Each line represents one host and contains these three fields delimited by the pipe character:
hostname|username|password
- The username must be **root** for UNIX and **Administrator** (or equivalent) for Windows.
- Enter each host on a separate line. The host in *Hosts.txt* must run the same operating system as the host where the original Master Agent was installed.

4. Do one of the following:

- If you installed the Master Agent on Windows (and are therefore pushing the Master Agent to Windows hosts), enter the following command:

```
utils\Perl\Win32\5.6.0\bin\MSWin32-x86\perl.exe  
pushMA.pl Hosts.txt
```

The Master Agent is distributed and starts on each remote host.

Secure or remove the `Hosts.txt` file (it contains sensitive information about your hosts).

- If you installed the Master Agent on UNIX (and are therefore pushing the Master Agent to UNIX hosts), enter the following command, substituting `<os_dir>` with the name of the operating system you are using (AIX, HP-UX, or SunOS):

```
./utils/perl/<os_dir>/perl/bin/perl pushMA.pl Hosts.txt
```

The Master Agent is distributed and starts on each remote host.

If you installed the Master Agent on an HP-UX or Solaris host, the program asks if you would like the Master Agent to restart on reboot:

Would you like add "rc.d" entries for Master Agent
on the remote hosts? [y|n] (default n)

Enter **y** for yes or **n** for no. The default is n.

Secure or remove the `Hosts.txt` file (it contains sensitive information about your hosts).

Install the Master Agent with UNIX Package Tools

You can use native UNIX package installation tools, such as `pkgadd` for Solaris, to install the Master Agent on remote hosts.

- ◆ Ensure that the first instance of the Master Agent is installed and that you answered “yes” to the prompt about creating native installable images (refer to *Step 45: Deploy and Start Master Agents* on page 192 for details about installing the first Master Agent instance).
- ◆ Be aware that the native installation tools do not check for the required disk space for installing the Master Agent (as is normally done by the ControlCenter installation wizard and command line interface).
- ◆ Be aware that the native installation tools do not set the Master Agent to automatically start when a system reboot occurs. You must set the autostart function manually, or manually restart the Master Agent each time the system is rebooted.

Run the installation tools on the target host as follows:

AIX Native Installation Tool

Do one of the following to run the installation tools on AIX:

- ◆ AIX GUI:
 - a. Type **smit** at a command prompt. A GUI appears.
 - b. Select **Software Installation and Maintenance, Install and Update Software, Install and Update from LATEST Available Software**. The program prompts for a directory path.
 - c. Enter the full path to the Master Agent native install image.
 - d. Click **OK**. A window appears, which you use to install the latest available software.
 - e. Click **LIST**, to see the software available in the directory you specified in step c.
 - f. Select **ECCALL@@ECC_all_filesets** and click **OK**.
 - g. Click **OK**.
 - h. Click **OK** to confirm. The installation begins.

- ◆ *Command Line:* Enter the following command at the prompt:

```
installp -acFXq -d $package_path/ECCMAGT.bff  
ECC.MAGENT
```

where *\$package_path* is the full path to the Master Agent native install image.

HP-UX Native Installation Tool

Do one of the following to run the installation tools on HP-UX:

- ◆ HP-UX GUI:
 - a. Type **swinstall** at a command prompt. The Specify Source dialog box appears.
 - b. For **Source Depot Path**, enter the full path to the Master Agent native install image.
 - c. Click **OK**.
 - d. In the SD Install - Software Selection dialog box, select **ECC** as the software bundle.
 - e. Select **Actions, Install Analysis**.
 - f. Once the analysis is complete, click **OK** to complete the install.
 - g. Click **Yes** to confirm.

You can also type **sam** at the command line to run the GUI. Then click **Software Management, Install Software to Local Host**.

- ◆ *Command Line* — Enter the following command at the prompt:

```
swinstall $install_flags -s $package_path
```

- *\$install_flags* are the desired flags on the **swinstall** command (see the man pages for more information about the flags). Depending on the hardware and software at your installation, some flags might be required.
- **-s** indicates that the specified *\$package_path* is to be used instead of the default, which is described under *\$package_path* below.
- *\$package_path* is the full path to the Master Agent native install image. Ensure that you specify a leading forward slash (/) to indicate that the path is relative to the root directory. The default value is */var/spool/sw*. The value can also appear in

the form `host:/directory`, where `host` is the network name of the target host, and `directory` is the directory on the target host where the Master Agent native install image resides.

Example: If you specified `/usr/ecc` as the path when creating the native package, the `$package_path` is `/usr/ecc/ECCMAGT`. You can use the following command, which specifies no `$install_flags`, to install the package:

```
swinstall -s /usr/ecc/ECCMAGT
```

LINUX Native Installation Tool

Do the following to install the Linux package using the command line:

- a. Copy the RPM file to the target host.
- b. Enter the following command in the directory where the RPM file resides:

```
rpm -i --nodeps <rpm_file_name>
```

Important: When you create an RPM on one LINUX distribution, you cannot use the RPM on a different LINUX distribution. For example, an RPM created on a machine running Red Hat LINUX will not work on a machine running SUSE LINUX.

Solaris Native Installation Tool

Do the following to install the Solaris package using the command line:

- a. Enter the following at a command prompt:

```
pkgadd -d $package_path
```

where *\$package_path* is the full path to the Master Agent native install image. A list of all native install packages in the *\$package_path* directory appears.

- b. Select the number of the package you want to install.

The default is to install all packages.

- c. Select **MAGENT** and the installation begins automatically.

AccessInfoChange Utility

This *AccessInfoChangeUtility* performs batch updates of access information required by the Common Mapping Agent and the Database Agent for Oracle. The utility can be used for Sybase, Oracle, Informix, DB2, and Microsoft SQL Server 2000 databases.

- ◆ *Running the Utility* on page 336
- ◆ *Update Template File* on page 338
- ◆ *Output File* on page 339

If the username or password information has changed for one or more databases, you can use the utility to update the username and password information used by the agent as a batch process instead of manually changing the password in each location in the ControlCenter Console.

The utility can update the following access information:

- ◆ Username
- ◆ Password
- ◆ System Password (Oracle databases only)

After retrieving the relevant host, type, and instance information for each database monitored by the agent, the *AccessInfoChangeUtility* creates a user-modifiable Update template File. After the user updates the file by inserting new access information for the database instances, the file is then read back into the utility as a source for updates to the database access information used by the agent.

The following files are used with the *AccessInfoChangeUtility*. They are located in the `<ECC_INSTALL_ROOT>\tools\utils\accessinfo` directory on the ControlCenter Server Host.

- ◆ *AccessInfoChangeUtility.bat*
- ◆ *AccessInfoChangeUtility.jar*

Running the Utility

You can type: `AccessInfoChangeUtility.bat -help` on the command line for help information about the `AccessInfoChangeUtility` command.

To run the AccessInfoChange Utility:

1. Stop all Oracle and Common Mapping Agents for which access information will be changed.
2. Stop the ControlCenter Server, Store, API Server, and close all open ControlCenter console instances.
3. Run the utility from a Command Prompt (DOS) window to generate the prerequisite Update Template File. The utility command is:

```
AccessInfoChangeUtility.bat -generate <filename>
```

where *<filename>* is a user-specified filename for the Update Template File that meets Windows file-naming conventions. No specific nomenclature is required for this filename, but if no value is provided, then the file will be called `AccessInfoChangeUtilityInput.txt` by default.

While it is running, the utility will generate status indicators and write them to an output file called `AccessInfoChangeUtilityReport.txt`. They are also displayed on-screen.

For more information about the `AccessInfoChangeUtility`'s output file, refer to *Output File* on page 339.

4. After the Update Template File has been generated, open it using a text editor. Update only those fields being changed.

For more information about the Update Template File, refer to *Update Template File* on page 338.

5. Run the utility again from the Command Prompt window to update database access settings in the ControlCenter Repository with the new information supplied in the Update Template File:

```
AccessInfoChangeUtility.bat -update <filename>
```

where *<filename>* is the name of the Update Template File.

6. Restart the ControlCenter infrastructure components: Server, Store, and API Server.
7. Restart all Oracle and/or Common Mapping Agents that monitor the databases for which access information was changed.
8. Reopen the ControlCenter Console and manually clear any alerts that exist for each database instance that has been updated. Table 63 lists alerts indicating that database access information has been changed. If there are any other underlying problems causing the database to be inaccessible, ControlCenter will regenerate the alert the next time it checks for the alert condition.

The frequency of alert checks is determined by the configuration of individual alerts. For instructions on clearing and configuring ControlCenter alerts, refer to the ControlCenter online help.

Table 63 Database Accessibility Alert Indicators

Database Type	Output
Oracle	Oracle Instance Not Accessible
Sybase	Sybase Instance Down
Informix	Informix Instance Down
DB2	DB2 Instance Down
Microsoft SQL Server 2000	SQL Instance Down

Update Template File

As described earlier, the AccessInfoChange Utility generates an Update Template File based on the existing database access information that it retrieves from the ControlCenter Repository, as described in steps 3 and 4 beginning on page 336.

The Update Template File will include two lines for each database monitored by the Common Mapping Agent or the Database Agent for Oracle. The file is generated using the following format for all database types except for Oracle:

```
[ Host = InformixHost1, DbInstance = prod,
  UserName = informix, DbType = Informix ]
  UserName = , UserPassword =
```

For Oracle databases, the following format is used:

```
[ Host = OracleHost2, DbInstance = dev,
  UserName = oraagent, DbType = Oracle ]
  UserPassword = , SysUserPassword = , UserName =
```

When updating database access information, only enter information in fields that are changing. Leave all other fields as they appear in the file. For example, if you are changing the UserPassword used by the Common Mapping Agent to access Informix database *demo*, but want to leave the UserName as is, leave the nonchanging field empty as shown in the following example:

```
[ Host = InformixHost3, DbInstance = demo, UserName =
  InformixUser, DbType = Informix ]
  UserName = , UserPassword = NewPassword
```

For security reasons, the utility does not write the current database passwords into the generated file.

Restrictions

The following restrictions apply when modifying the Update Template File:

- ◆ The fields within the brackets are mandatory and must not be changed; they are used to identify the databases that will be updated by the utility. The fields following the bracket are the only fields that can be modified.

- ◆ If a single record in the Update Template File identifies multiple records in the database, then all matching records in the database will be updated from the values contained in that record.
- ◆ If there are multiple records in the Update Template File that identify one or more database instances, then all matching database access settings will be updated using the values in the last record of that type that appears in the file.
- ◆ The utility cannot be used to add or delete database access records, only to update access information for existing ones.

To delete database access records use the EMC ControlCenter Console, refer to the *EMC ControlCenter 5.2 SP4 Release Notes* for more information on this topic.

Output File

The AccessInfoChange Utility also generates an output result file named `AccessInfoChangeUtilityReport.txt` containing the results of the execution of the utility. The output file contains the result (including any errors) of each record processed, as shown in the following example:

```
WARNING: No matching record(s) found in the database for key :
[ HostName = host069.company.com, OracleSID = rambdb, AgentUserName = MGR_WRONG,
  DatabaseKind = Oracle]
Successfully updated UserName for record with key :
[ HostName = host069.company.com, OracleSID = rambdb, AgentUserName = MGR_RIGHT,
  DatabaseKind = Oracle]

***** Update Summary *****
Total number of record(s) in the input file : 2
Total number of record(s) modified in the input file : 1
Total number of record(s) updated in the database : 1
Total number of record(s) that did not have matching record(s) in the database : 1
```

Whenever the AccessInfoChange Utility generates a new version of the `AccessInfoChangeUtilityReport.txt` file, it overwrites any existing versions of the file that may already exist.

This appendix describes the EMC ControlCenter support for ConnectEMC.

EMC ControlCenter 5.2 SP4 supports ConnectEMC reporting of alerts coming from switches in your managed environment. This new functionality replaces equivalent functionality that existed in previous versions of ControlCenter that utilized OnAlert™.

ConnectEMC simplifies and standardizes the method EMC products use to transport event files—error, informational, configuration, and others—from a service PC to EMC back-office support systems.

ControlCenter 5.2 SP4 only provides ConnectEMC support for switch alerts.

This appendix provides an overview of the configuration of ConnectEMC support in ControlCenter and how ControlCenter passes alert information to ConnectEMC:

- ◆ *Overview of ConnectEMC Process* on page 342
- ◆ *Installation and Configuration* on page 343

Overview of ConnectEMC Process

When ControlCenter receives switch alerts, it passes the information to a ConnectEMC service installed on the ControlCenter server.

Alert information is passed along for alerts with the following severity levels:

- ◆ Warning
- ◆ Critical
- ◆ Fatal

The alerts are filtered through a configuration file, which forwards to ConnectEMC only alerts for those switches that have been marked for ConnectEMC reporting in the `connectEmc_service.ini` configuration file, which is documented in full in the next section.

After it has determined which alerts should be reported to ConnectEMC, ControlCenter constructs an XML file for each alert, which is then made available for input into ConnectEMC for processing via a shared directory that is accessible to both applications.

ConnectEMC then processes the incoming alert information and sends it to EMC Customer Support via e-mail, dial-up modem, FTP, or SNMP.

For more information about ConnectEMC, refer to the *ConnectEMC for Windows User Guide* (EMC P/N 300-001-829).

Installation and Configuration

The ConnectEMC support is installed as part of ControlCenter. No special installation processes are required. However, activation of the feature requires configuration steps to be carried out by, or under the supervision of, EMC Customer Support personnel.

Construction of the Configuration File

The configuration file for the ControlCenter ConnectEMC service is called `connectEmc_service.ini`. It resides in the ControlCenter `ini` folder and contains the following information:

Table 64 Contents of the `ConnectEmc_service.ini` File

Value	Description
Site Name	The name of the EMC customer site.
Directory	The ConnectEMC service input directory (e.g., <code>C:\ECC\ecc_inf\connectEMCDir</code>). This is the location of the XML input file. If this directory is not specified, is incorrect, or is not reachable, ControlCenter will not generate XML files. Note: The XML file may be placed in any local or networked folder as long as both ControlCenter and ConnectEMC have access to it. When the directory is set to a networked folder, it should be set as a shared drive (e.g., <code>X:\PathName</code>).
MaxFiles	The maximum number of XML files that can reside in the ConnectEMC input directory at any one time. This value is not equivalent to the number of files in the directory but rather the maximum number of files that trigger the Server to delete files.
Delete Files	The number of XML files that are deleted from ConnectEMC input directory when the maximum number has been reached or exceeded. The oldest files are deleted first. For example, <code>MaxFiles = 100</code> and <code>Delete Files = 25</code> , when the Server generates the 100th file it starts a process to control the number of files generated during which anywhere from 1 to 25 files can be deleted.

Table 64 Contents of the ConnectEmc_service.ini File (continued)

Value	Description
IDInfo	A comma-separated listing of the World Wide Names (WWNs) and serial numbers for each switch being reported to ConnectEMC. Every switch appears on a new line in the configuration file. Located in the <code>SwitchIDInfo</code> section of the configuration file. The serial number information entered here will be used to generate a Clarify ID for the alert in ConnectEMC. Note: This information must be entered by onsite EMC Customer Support personnel. If no devices are specified, then no ControlCenter switch alerts will be passed to ConnectEMC.

Changes made to the `connectEmc_service.ini` file will only take effect when the ControlCenter Server has been restarted.

In addition to the information listed here, there are other configuration variables in the `connectEmc_service.ini` file. Those values should not be changed from their default settings without approval from EMC Customer Support.

Construction of the ConnectEMC Input File

ControlCenter produces a separate XML file for each switch alert being reported to ConnectEMC. The file is called `RSC_ClarifyID_Date_Time.XML`, where:

- ◆ `RSC` is the filename prefix, as specified in the configuration file.
- ◆ `ClarifyID` is a Clarify ID generated from the serial number of the switch being reported
- ◆ `Date` and `Time` are the date and time that the alert was generated.

The following information is gathered about switches that are reported to ConnectEMC, and is included in each XML file:

Table 65 Contents of the ConnectEMC Input XML File

Tag Name	Description
ClarifyID	Clarify ID generated for the alert. Identical to the switch's serial number (as entered in the configuration file).
SiteName	Site name (as entered in the configuration file).
SerialNumber	Serial number of the switch.

Table 65 Contents of the ConnectEMC Input XML File (continued)

Tag Name	Description
WWN	WWN of the switch.
IP Address	IP address of the switch.
LastTime	Date and time of the alert.
Description	A description of the alert.

Communication between ControlCenter and ConnectEMC

The ControlCenter ConnectEMC service communicates with ConnectEMC using a shared directory on the ControlCenter Server, to which both applications are pointed with configuration settings. After ControlCenter writes an alert output XML file to this directory, ConnectEMC reads the file and processes the information in accordance with its own configuration settings.

ConnectEMC and ControlCenter can be installed on the same machine, or on physically distinct machines, as long as they both have access to the shared folder in which the output XML file resides.

For instructions on configuring ConnectEMC to point to the ControlCenter output XML file, refer to the ConnectEMC documentation.

A

- agent load balancing 154
- agents
 - deploying use 217
 - finishing setup 223
 - set up 223
 - simplifying deployment 216
- applications
 - licensing 171
- architecture
 - distributed infrastructure 10
 - single-host infrastructure 9
- assisted discovery
 - entering settings 229
 - for SMI-enabled arrays 228
 - reviewing results 235
 - starting managed objects 235
 - stopping object management 236
- Automated Resource Manager 32
- automatic discovery 227

B

- backing up ControlCenter 238
- Backup Agent for EDM
 - planning for 61
- Backup Agent for LEGATO NetWorker
 - planning for 63
- Backup Agent for TSM
 - planning for 64
- Backup Agent for VERITAS NetBackup
 - planning for 65

C

- Celerra
 - configuring SNMP traps 90
- cluster 243
 - considerations 245
 - create names 247
 - install components 252,262
 - troubleshoot 266
 - uninstall 284
- comments xiv
- Common Array Manager 32
- Common Mapping Agent
 - performance and scalability 69
 - planning for 67
- configuring, Console 168
- connectivity device discovery 237
- Console
 - configuring and launching 168
 - logging in to 174
- ControlCenter Console
 - downloading 165
 - installing 164
 - launching 168
 - logging in 170
- Customer Support xiii

D

- Database Agent for Oracle
 - planning for 74
- deploying
 - agents 217
- distributed configuration
 - cluster 245

Do 165
Documentation, related xii

E

EACLI Client
installing 189
ECC Server, starting 160,184
eccadmin user 114
creating 114

F

Fibre Channel Connectivity Agent
performance and scalability 72
planning for 70
FibreZoneBridge 287
install software 290
CLI 292
uninstall software 291
CLI 294
framework applications 57

H

Help xiii
Host Agent for Novell
planning for 77,78
Host Agent for Windows
planning for 78
Host Agents for AIX, HP-UX, Linux, Solaris
planning for 76
hosts, transferring tools to 116

I

infrastructure
installing 129,131
verifying setup 164
installing
FibreZoneBridge 287
from a shared folder 120
infrastructure 129,131
Integration Packages 175
Master Agent
from Windows command line 54,193
on HP-UX 197
MVS components from tape 191

Repository 132
Store 140
integrating, ControlCenter with 30
Integration Gateway
prerequisites 57
Integration Packages 175
download 175
uninstall 278

L

launching, Console 168
license
applications 171
use one Console 171
load balancing (for agents) 154
logging in to the Console 174

M

Master Agent
deploying
from Windows command line 193
deploying using BMC common install 201
deploying using UNIX command line 196
deploying using Windows command line 195
deploying using Windows GUI 193
ensuring required rights (Windows only) 206
install 54,192
on UNIX command line 196
on Windows command line 195
installing
from Windows command line 54
on HP-UX 197
installing on infrastructure host 143
pushing to remote hosts 328
start
UNIX 207
Windows 207
starting 207
uninstall 283
Multihost Push Utility 328

N

native install tools
Solaris 332,333
ndix 297

NetApp filers
 configuring to send traps 89

O

open integration components 30

P

Performance Manager
 connect additional Repositories 179
 enable license 177
 install and run 146,178
 installing 177
 installing on infrastructure host 143
 port usage 297
 firewall access 313
 SNMP 310
 proxy agents
 performance and scalability 96
 planning for 95

R

Repository
 installing 132
 starting 160

S

SAN Manager 33
 service xiii
 service processor, accessing 288
 Solaris native install tools 332,333
 Solutions Enabler
 deploying 213
 making available 138
 planning for 97
 SSL
 configuring 147
 starting
 ECC Server 160,184
 Repository 160
 Storage Agent for Centera
 planning for 81
 Storage Agent for CLARiiON
 planning for 82

Storage Agent for ESS
 planning for 81
 Storage Agent for HDS
 planning for 83
 Storage Agent for HP StorageWorks
 planning for 85
 Storage Agent for NAS
 planning for 86
 Storage Agent for SMI
 planning for 91
 Storage Agent for Symmetrix
 planning for 92
 StorageScope
 installing 182
 installing on infrastructure host 143
 integration with 35
 reports 35
 StorageScope API 36
 install 185
 Store, installing 140
 SupportTools 187,189
 install 187
 Symmetrix array
 enabling access 224
 Symmetrix Manager 35
 Symmetrix Optimizer 37
 Symmetrix SDM Agent
 planning for 73

T

tape, installing MVS components from 191
 technical support xiii
 TimeFinder Manager 34
 tools, transferring 116

U

uninstall
 agents 274
 cluster support 284
 Console 276
 Integration Packages 278
 Master Agent 283
 users, creating eccadmin 114
 utilities, Multihost Push 328

W

Web Console

- configuring SSL 147
- launching 172
- logging in 173

WebConsole Server

- installing 145
- installing on infrastructure host 143
- verifying setup 172

Workload Analyzer 38

Workload Analyzer Archiver

- performance and scalability 59
- planning for 58,59