

Oracle® Enterprise Manager

Cloud Control Advanced Installation and Configuration Guide

12c Release 3 (12.1.0.3)

E24089-24

July 2013

Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide, 12c Release 3 (12.1.0.3)

E24089-24

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Primary Author: Aravind Jayaraaman

Contributing Author: Dennis Lee, Pradeep Gopal, Genevieve D'Souza, Namrata Bhakthavatsalam, Leo Cloutier, Akshaya Govind, Thom Chumley

Contributor: Enterprise Manager Cloud Control Development Teams, Quality Assurance Teams, Customer Support Teams, and Product Management Teams.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	xvii
Intended Audience.....	xvii
Purpose of the Document.....	xvii
Documentation Accessibility	xviii
Related Documents	xviii
Conventions	xix

Part I Getting Started

1 Procuring Software

1.1	Releases Available for Enterprise Manager Cloud Control.....	1-1
1.2	Procuring Enterprise Manager Cloud Control Software	1-3
1.2.1	How Do You Access the Software from DVD?	1-3
1.2.1.1	Accessing Software from DVD.....	1-4
1.2.1.2	Setting Mount Point for DVD	1-4
1.2.2	How Do You Procure the Software from Oracle Technology Network?	1-5
1.2.2.1	Downloading Software	1-6
1.2.2.2	Verifying File Size.....	1-6
1.2.2.3	Extracting Contents	1-6
1.2.2.4	Verifying Software Release Description.....	1-7
1.2.2.5	Verifying Platform Information	1-7
1.3	Procuring Oracle Management Agent Software	1-8

2 Understanding the Basics

2.1	Understanding Installation Basics	2-1
2.1.1	What Different Installation Modes Can You Use?.....	2-2
2.1.2	What Is Enterprise Manager Cloud Control Installation Wizard?	2-2
2.1.3	What Installation Types Are Offered by the Installation Wizard?	2-3
2.1.3.1	Create a New Enterprise Manager System	2-3
2.1.3.2	Upgrade an Existing Enterprise Manager System.....	2-3
2.1.3.3	Install Software Only	2-4
2.1.4	What Is Oracle Configuration Manager?	2-4
2.1.4.1	Manually Collecting and Uploading Configuration Information.....	2-5
2.1.4.2	Enabling Oracle Configuration Manager After Installing Enterprise Manager Cloud Control	2-5

2.1.5	What Are Software Updates?.....	2-5
2.1.5.1	What Is a Software Update?.....	2-6
2.1.5.2	How Does the Software Update Feature Work?.....	2-6
2.1.5.3	What Types of Software Updates Are Downloaded and Applied?.....	2-6
2.1.5.4	How Can I Find Out What Bugs Have Been Fixed by the Software Updates? ...	2-7
2.1.5.5	How Can You Download the Software Updates?	2-7
2.1.5.6	Can I Download and Apply These Patches After Installation or Upgrade?.....	2-9
2.1.5.7	How Can You Identify What Patches Have Been Applied?	2-9
2.1.6	What is a Deployment Size?.....	2-9
2.1.7	What Is Add Host Target Wizard?.....	2-10
2.1.8	What Is Add Management Service Deployment Procedure?	2-11
2.1.9	What Ports Are Used for Installation?	2-12
2.1.9.1	What Default Ports Are Used?	2-12
2.1.9.2	How Can You Customize Ports?	2-13
2.1.9.3	What Precautions You Must Take While Customizing Port Numbers?	2-15
2.1.10	What Data Files Are Created While Configuring Oracle Management Repository?	2-16
2.1.11	How Do You Delete Data Files?	2-16
2.2	Understanding Oracle WebLogic Server Requirement.....	2-17
2.2.1	How Do I Verify Whether Oracle WebLogic Server Is Installed?	2-17
2.2.2	Is Oracle WebLogic Server Cluster Supported?	2-18
2.2.3	If Oracle WebLogic Server Already Exists, Is the Existing Domain Used?.....	2-18
2.2.4	When and Why Do You Need Oracle WebLogic Server Credentials?	2-18
2.2.5	When and Why Do You Need Node Manager Credentials?	2-18
2.2.6	How Do You Find Admin Server Port After Installing Enterprise Manager?	2-19
2.2.7	How Do You Verify Whether Admin Server Is Running?	2-19
2.2.8	How Do You Start Admin Server?	2-19
2.3	Understanding Installation Directories	2-19
2.3.1	What Is Oracle Inventory Directory?	2-20
2.3.2	What Is Oracle Middleware Home?.....	2-20
2.3.3	What Is Oracle Management Service Instance Base Location?	2-21
2.3.4	What Is Oracle Home?	2-21
2.3.5	What Is Agent Base Directory?	2-22
2.3.6	What is Agent Instance Directory?.....	2-22
2.3.7	What Is /TMP C:\Temp Directory Used For?	2-22
2.4	Understanding Configuration Assistants.....	2-23
2.4.1	What Are Configuration Assistants?	2-23
2.4.2	What Configuration Assistants Are Run by the Installation Wizard?.....	2-23
2.4.2.1	Configuration Assistants Run While Installing a New Enterprise Manager....	2-23
2.4.2.2	Configuration Assistants Run While Upgrading an Existing Enterprise Manager....	2-24
2.4.2.3	Configuration Assistants Run While Upgrading an Additional Oracle Management Service	2-25
2.4.3	What Do You Do When Configuration Assistants Fail?	2-26
2.5	Understanding Prerequisite Checks.....	2-26
2.5.1	What Prerequisite Checks Are Run by Default?	2-26
2.5.2	How Can You Run Prerequisite Checks in Standalone Mode?	2-27
2.6	Understanding Limitations of Enterprise Manager Cloud Control	2-27

2.6.1	Can You Access Unlicensed Components?.....	2-27
2.6.2	What Are the Limitations with DHCP-Enabled Machines?.....	2-28
2.7	Understanding Startup Scripts	2-28
2.8	Understanding Other Miscellaneous Concepts.....	2-29
2.8.1	What Is a Host List File?	2-29
2.8.2	What Scripts Are Run During the Installation Process?	2-29

Part II Installing Enterprise Manager System

3 Installing Enterprise Manager System in Silent Mode

3.1	Overview	3-1
3.2	Before You Begin.....	3-2
3.3	Prerequisites	3-5
3.4	Installation Procedure	3-5
3.4.1	Installing Enterprise Manager	3-5
3.4.2	Using Advanced Installer Options.....	3-8
3.4.3	Understanding the Limitations.....	3-8
3.4.4	Editing Response File for Installing Software	3-9
3.5	After You Install	3-17

4 Installing Enterprise Manager Software Now and Configuring Later

4.1	Overview	4-1
4.2	Before You Begin.....	4-3
4.3	Prerequisites	4-7
4.4	Installation Procedure	4-7
4.4.1	Installing in Graphical Mode	4-7
4.4.1.1	Installing Software.....	4-7
4.4.1.1.1	Using Advanced Installer Options	4-14
4.4.1.2	Running Root Script.....	4-15
4.4.1.3	Configure Software	4-16
4.4.1.3.1	Using Advanced Script Options	4-27
4.4.1.4	Performing Post-Configuration Tasks.....	4-28
4.4.2	Installing in Silent Mode.....	4-28
4.4.2.1	Installing Software.....	4-29
4.4.2.1.1	Editing Response File for Installing Software	4-30
4.4.2.2	Running Root Script.....	4-32
4.4.2.3	Configuring Software.....	4-33
4.4.2.3.1	Editing Response File for Configuring Software	4-35
4.4.2.4	Performing Post-Configuration Tasks.....	4-39

Part III Installing Additional Oracle Management Service

5 Installing Additional Oracle Management Service in Silent Mode

Part IV Installing Oracle Management Agent

6 Installing Oracle Management Agent in Silent Mode

6.1	Overview	6-1
6.2	Before You Begin.....	6-2
6.3	Prerequisites	6-3
6.4	Installation Procedure	6-7
6.4.1	Installing a Management Agent Using the AgentPull Script.....	6-8
6.4.1.1	Acquire the Management Agent Software	6-8
6.4.1.2	Install the Management Agent Using the AgentPull Script.....	6-9
6.4.2	Installing a Management Agent Using the agentDeploy Script	6-10
6.4.2.1	Using EM CLI from the Remote Destination Host.....	6-10
6.4.2.1.1	Acquire the Management Agent Software and Download it onto the Destination Host Using EM CLI	6-10
6.4.2.1.2	Install the Management Agent Using the agentDeploy Script.....	6-12
6.4.2.2	Using EM CLI from the OMS Host.....	6-14
6.4.2.2.1	Acquire the Management Agent Software and Download it onto the OMS Host Using EM CLI	6-14
6.4.2.2.2	Transfer the Management Agent Software to the Destination Host	6-16
6.4.2.2.3	Install the Management Agent Using the agentDeploy Script.....	6-16
6.4.3	Installing a Management Agent Using the RPM File	6-16
6.4.3.1	Acquire the Management Agent Software and Download the RPM File onto the OMS Host	6-16
6.4.3.2	Transfer the RPM File to the Destination Host	6-18
6.4.3.3	Install the Management Agent Using the RPM File	6-18
6.4.4	Creating a Response File for Installing Using AgentPull Script.....	6-18
6.4.5	Using a Response File for Installing Using agentDeploy Script.....	6-19
6.4.6	Creating a Response File for Installing Using an RPM File.....	6-22
6.4.7	Understanding the Options Supported by the AgentPull Script.....	6-23
6.4.8	Understanding the Options Supported by the agentDeploy Script.....	6-23
6.4.9	Understanding the Contents of the Downloaded Management Agent Software...	6-24
6.4.10	Understanding the Contents of the Management Agent RPM File	6-25
6.5	After You Install	6-25

7 Cloning Oracle Management Agent

7.1	Overview	7-1
7.2	Before You Begin.....	7-2
7.3	Prerequisites	7-5
7.4	Cloning Procedure	7-13
7.4.1	Cloning in Graphical Mode.....	7-13
7.4.1.1	Supported Additional Parameters	7-18
7.4.1.2	Format of Host List File	7-19
7.4.2	Cloning in Silent Mode	7-20
7.4.2.1	Setting Environment Variables for Cloning Agent Using ZIP File	7-21
7.5	After You Clone.....	7-22

8 Installing Shared Agent

8.1	Overview	8-1
8.2	Before You Begin.....	8-2

8.3	Prerequisites	8-4
8.4	Installation Procedure	8-12
8.4.1	Installing in Graphical Mode	8-12
8.4.1.1	Supported Additional Parameters	8-16
8.4.2	Installing in Silent Mode.....	8-17
8.4.2.1	Creating a Response File	8-18
8.5	After You Install.....	8-20

9 Installing Oracle Management Agent Software Now and Configuring Later

9.1	Overview	9-1
9.2	Before You Begin.....	9-2
9.3	Prerequisites	9-2
9.4	Installation Procedure	9-2
9.5	Configuration Procedure	9-2
9.6	After You Install	9-3

Part V Advanced Installation and Configuration

10 Performing Additional Configuration Tasks

10.1	Understanding Default and Custom Data Collections.....	10-1
10.1.1	How Enterprise Manager Stores Default Collection Information	10-1
10.2	Enabling Multi-Inventory Support for Configuration Management	10-2
10.2.1	AGENT_HOME Versus AGENT_STATE Directories.....	10-3
10.3	Manually Configuring a Database Target for Complete Monitoring	10-4
10.4	Modifying the Default Login Timeout Value	10-6
10.5	Configuring Clusters and Cluster Databases in Cloud Control	10-7
10.5.1	Configuring Cluster Databases.....	10-7
10.5.2	Discovering Instances Added to the Cluster Database	10-8
10.5.2.1	Troubleshooting.....	10-8
10.6	Collecting Client Configurations	10-9
10.6.1	Configuring the Client System Analyzer	10-10
10.6.1.1	Client System Analyzer in Oracle Cloud Control.....	10-10
10.6.1.2	Deploying Client System Analyzer Independently	10-10
10.6.2	Configuration Parameters	10-11
10.6.2.1	Associating the Parameters with an Application	10-14
10.6.3	Rules	10-15
10.6.4	Customization	10-17
10.6.5	CSA Deployment Examples.....	10-17
10.6.5.1	Using Multiple Collection Tags.....	10-17
10.6.5.2	Privilege Model for Viewing Client Configurations	10-18
10.6.5.3	Using the Customization API Example	10-19
10.6.5.4	Using the CSA Servlet Filter Example.....	10-20
10.6.5.5	Sample Deployments	10-21
10.6.5.5.1	Example 1: Helpdesk	10-21
10.6.5.5.2	Example 2: Inventory	10-22
10.6.5.5.3	Example 3: Problem Detection	10-23

10.7	Configuring Privilege Delegation Providers	10-23
10.7.1	Creating a Privilege Delegation Setting	10-24
10.7.1.1	Creating a Sudo Setting Using EM CLI.....	10-25
10.7.1.2	Creating a PowerBroker Setting Using EM CLI.....	10-25
10.7.2	Applying Privilege Delegation Settings	10-26
10.7.2.1	Applying Settings to Host Targets Using EM CLI	10-26
10.7.2.2	Applying Settings to a Composite Target.....	10-26
10.7.3	Disabling Host Privilege Delegation Provider Settings Using EM CLI.....	10-27
10.7.4	Sudo Configuration: Sudoers File	10-27
10.7.5	Configuring Privilege Delegation Providers Using Cloud Control Console.....	10-27
10.7.5.1	Configuring Sudo Settings For a Host Using Enterprise Manager Cloud Control Console 10-28	
10.7.5.2	Configuring PowerBroker Settings For a Host Using the Cloud Control Console 10-28	
10.7.5.3	Applying Settings to Multiple Host Targets Using the Cloud Control Console..... 10-28	
10.7.5.4	Disabling Host Privilege Delegation Provider Settings For One or More Hosts Using Cloud Control Console 10-29	

11 Configuring Enterprise Manager for Firewalls

11.1	Firewall Configuration Considerations	11-1
11.1.1	Enabling ICMP Echo Requests on Firewalls.....	11-2
11.2	Overview of Enterprise Manager Components and Ports.....	11-2
11.2.1	Viewing a Summary of the Ports Assigned During Installation	11-2
11.2.2	Default Port Assignments for Enterprise Manager Components.....	11-2
11.3	Firewall Configurations for Enterprise Management Components.....	11-3
11.3.1	Firewalls Between Your Browser and the Enterprise Manager Console	11-5
11.3.2	Configuring the Management Agent on a Host Protected by a Firewall.....	11-5
11.3.2.1	Configuring the Management Agent to Use a Proxy Server	11-6
11.3.2.2	Configuring the Firewall to Allow Incoming Communication From the Management Service 11-7	
11.3.3	Configuring the OMS on a Host Protected by a Firewall	11-7
11.3.3.1	Configuring the OMS to Use a Proxy Server to Communicate with Management Agents 11-8	
11.3.3.2	Configuring the Firewall to Allow Incoming Management Data From the Management Agents 11-9	
11.3.3.3	Enabling OMS to Access My Oracle Support.....	11-9
11.3.3.4	About the dontProxyfor Property	11-10
11.3.4	Firewalls Between the OMS and the Management Repository	11-10
11.3.5	Firewalls Between Enterprise Manager and a Managed Database Target.....	11-10
11.3.6	Firewalls Used with Multiple OMS Instances	11-11
11.3.7	Configuring Firewalls to Allow ICMP and UDP Traffic for Beacons	11-11

12 Sizing Your Enterprise Manager Deployment

12.1	Overview of Oracle Enterprise Manager Cloud Control Architecture	12-1
12.2	Enterprise Manager Cloud Control Sizing.....	12-2
12.2.1	Overview of Sizing Guidelines	12-2
12.2.1.1	Hardware Information.....	12-2

12.2.1.2	Sizing Specifications	12-3
12.2.1.3	Sizing for Upgraded Installs	12-3
12.2.1.4	Minimum Hardware Requirements	12-3
12.2.1.5	Network Topology Considerations	12-3
12.2.2	Software Configurations	12-4
12.2.2.1	Small Configuration	12-4
12.2.2.2	Medium Configuration	12-4
12.2.2.3	Large Configuration	12-5
12.2.2.4	Repository Tablespace Sizing	12-5
12.2.3	Additional Configurations	12-6
12.2.3.1	Large Concurrent UI Load	12-6
12.2.3.2	BI Publisher Configuration	12-8
12.3	Enterprise Manager Cloud Control Performance Methodology	12-8
12.3.1	Step 1: Choosing a Starting Platform Cloud Control Deployment	12-8
12.3.2	Step 2: Periodically Evaluating the Vital Signs of Your Site	12-9
12.3.3	Step 3: Using DBA and Enterprise Manager Tasks To Eliminate Bottlenecks	12-11
12.3.3.1	Offline Monthly Tasks	12-11
12.3.4	Step 4: Eliminating Bottlenecks Through Tuning	12-11
12.3.4.1	High CPU Utilization	12-11
12.3.4.2	Loader Vital Signs	12-12
12.3.4.3	Rollup Vital Signs	12-13
12.3.4.4	Rollup Process	12-13
12.3.4.5	Job, Notification, and Alert Vital Signs	12-15
12.3.4.6	I/O Vital Signs	12-15
12.3.4.7	About the Oracle Enterprise Manager Performance Page	12-16
12.3.4.8	Determining the Optimum Number of Middle Tier OMS Servers	12-17
12.3.5	Step 5: Extrapolating Linearly Into the Future for Sizing Requirements	12-17
12.3.6	Using Returning Query Safeguards to Improve Performance	12-18
12.4	Overview of Repository and Sizing Requirements for Fusion Middleware Monitoring	12-18
12.4.1	ADP Monitoring	12-19
12.4.2	JVMD Monitoring	12-19

13 Installing ADP with Advanced Installation Options

13.1	Application Dependency and Performance Architecture	13-1
13.2	Before you Begin	13-2
13.3	Prerequisites	13-2
13.4	Installation Procedure	13-3
13.4.1	Deploying ADP Engines	13-3
13.4.1.1	Deploying ADP Engine on a Remote Host	13-3
13.4.1.1.1	Meet the Prerequisites	13-3
13.4.1.1.2	Deploy ADP Engine on the Remote Host	13-6
13.4.1.2	Deploying ADP Engine Manually Using ApmEngineSetup.pl	13-7
13.4.2	Deploying ADP Agents Manually Using deploy_adpagent.pl	13-7
13.5	After You Install	13-8
13.5.1	Verifying ADP Engine and ADP Agent Installation	13-8
13.5.2	Configuring Oracle SOA Suite for Secure Connectivity	13-8

13.5.3	Configuring Oracle WebLogic Server or Oracle WebLogic Portal (WLP) for Secure Connectivity	13-8
13.5.4	Importing a Certificate into ADP Engine's Keystore.....	13-9
13.5.5	Configuring ADP Agent When WebLogic Is Installed As a Windows Service	13-10

14 Installing JVMMD with Advanced Install Options

14.1	JVMMD Architecture	14-1
14.2	Before you Begin	14-3
14.3	Prerequisites	14-3
14.4	Installation Procedure	14-3
14.4.1	Deploying JVMMD Engine	14-3
14.4.1.1	Deploying JVMMD Engine on a Remote Host	14-3
14.4.1.1.1	Meet the Prerequisites	14-3
14.4.1.1.2	Deploy JVMMD Engine on the Remote Host	14-6
14.4.1.2	Deploying JVMMD Engine Manually	14-7
14.4.1.2.1	Download jvmd.zip	14-7
14.4.1.2.2	Deploy JVMMD Engine	14-8
14.4.1.3	Deploying JVMMD Engine Manually Using ApmEngineSetup.pl	14-9
14.4.2	Deploying JVMMD Agents.....	14-10
14.4.2.1	Deploying JVMMD Agents Manually.....	14-10
14.4.2.1.1	Download javadiagnosticagent.ear or jamagent.war	14-10
14.4.2.1.2	Deploy JVMMD Agent.....	14-12
14.4.2.2	Deploying JVMMD Agents Manually Using deploy_jvmdagent.pl	14-15
14.4.2.3	Deploying JVMMD Agents for High Availability.....	14-15
14.4.2.3.1	Deploying JVMMD Agents for High Availability Using the Application Performance Management Page	14-15
14.4.2.3.2	Deploying JVMMD Agents for High Availability Manually	14-16
14.4.2.4	Deploying JVMMD Database Agent	14-16
14.4.2.5	Connecting JVMMD Agent to the JVMMD Engine Secure Port.....	14-17
14.5	After You Install	14-18

15 Integrating BI Publisher with Enterprise Manager

15.1	Overview	15-2
15.1.1	Limitations.....	15-2
15.1.2	Downloading Oracle BI Publisher.....	15-2
15.2	BI Publisher Installation and Integration with Enterprise Manager 12c	15-3
15.2.1	Enterprise Manager and BI Publisher Inventory	15-3
15.2.2	Installing Enterprise Manager and Required Infrastructure	15-3
15.2.2.1	Installing BI EE Using Software-only Install	15-4
15.2.2.2	Integrating BI Publisher with Enterprise Manager using the configureBIP Script.....	15-5
15.2.2.2.1	Integrating BI Publisher with Enterprise Manager using the <i>configureBIP</i> Script in Normal Mode	15-6
15.2.2.2.2	Integrating BI Publisher with Enterprise Manager Using the <i>configureBIP</i> Script in Upgrade Mode	15-7
15.3	Verifying Integration of BI Publisher with Enterprise Manager	15-9
15.4	Allowing Access to BI Publisher for Enterprise Manager Administrators	15-10

15.4.1	Enterprise Manager Authentication Security Model.....	15-10
15.4.2	BI Publisher security model	15-11
15.4.3	BI Publisher Permissions	15-11
15.4.4	BI Publisher OPSS Application Roles	15-11
15.4.5	Authenticating and limiting access BI Publisher features	15-12
15.5	Limiting access to BI Publisher features	15-13
15.5.1	Granting BI Publisher OPSS Application Roles to Enterprise Manager Administrators in Repository-Based Authentication Mode Using wlst 15-13	
15.5.2	Propagation Time for Changes to OPSS.....	15-15
15.6	Allowing Access to BI Publisher for Enterprise Manager Administrators in an underlying LDAP Authentication security model environment 15-15	
15.6.1	Mapping LDAP Groups to BI Publisher OPSS Application Roles	15-16
15.7	Securing BI Publisher with a Secure Socket Layer (SSL) Certificate	15-17
15.8	BI Publisher Administration	15-19
15.9	Post-Upgrade Steps to take after upgrading to BI Publisher to 11.1.1.6.0	15-20
15.10	EMBIP* Roles: Granting Access to Folders and Catalog Objects.....	15-21
15.11	Access to Enterprise Manager Repository.....	15-22
15.12	Troubleshooting	15-22
15.12.1	Rerunning configureBIP	15-22
15.12.2	BI Publisher Log File Locations	15-22
15.12.2.1	configureBIP Log Files	15-22
15.12.2.2	Enterprise Manager BI Publisher Tree and EM CLI Log File Output	15-22
15.12.2.3	BI Publisher Runtime	15-22
15.12.3	Additional Troubleshooting.....	15-23
15.12.4	Redeploying All Enterprise Manager-Supplied BI Publisher Reports	15-23
15.13	Managing Enterprise Manager - BI Publisher Connection Credentials.....	15-23
15.14	Managing the BI Publisher Server	15-25
15.15	Configuring BI Publisher behind a Load-Balancer	15-26

16 Running OMS in Console-Only Mode

Part VI Deinstallation

17 Deinstalling Enterprise Manager (Single and Multi-OMS Environments)

17.1	Deinstalling Enterprise Manager.....	17-1
17.1.1	Prerequisites for Deinstalling Only the OMS and Retaining the Management Repository 17-1	
17.1.2	Prerequisites for Deinstalling the Entire Enterprise Manager System	17-3
17.1.3	Deinstallation Procedure	17-5
17.1.3.1	Deinstalling in Graphical Mode	17-5
17.1.3.2	Deinstalling in Silent Mode.....	17-7
17.1.4	After You Deinstall	17-10
17.2	Deinstalling or Undeploying Only Plug-ins from the OMS.....	17-10
17.3	Deleting OMS Entries from the Management Repository	17-10

18 Deinstalling Oracle Management Agent

18.1	Deinstalling Oracle Management Agents	18-1
18.1.1	Prerequisites	18-1
18.1.2	Deinstallation Procedure	18-2
18.1.2.1	Deinstalling Oracle Management Agent in Graphical Mode	18-2
18.1.2.2	Deinstalling Oracle Management Agent in Silent Mode	18-3
18.1.2.2.1	Deinstalling in Silent Mode Using the Installer	18-3
18.1.2.2.2	Deinstalling in Silent Mode Using AgentDeinstall.pl Script	18-5
18.1.2.3	Deinstalling Shared Agent	18-5
18.1.2.4	Deinstalling Oracle Management Agent Installed Using an RPM File	18-6
18.1.3	After You Deinstall	18-6
18.2	Deinstalling or Undeploying Only Plug-ins from the Oracle Management Agent	18-7

19 Deinstalling ADP and JVMDB

19.1	Deinstallation Procedure for ADP	19-1
19.1.1	Removing ADP Engine	19-1
19.1.1.1	Removing ADP Engine Using Application Performance Management Page..	19-1
19.1.1.2	Removing ADP Engine Manually	19-2
19.1.1.3	Removing ADP Engine Manually Using ApmEngineSetup.pl	19-2
19.1.2	Removing ADP Agents	19-3
19.1.2.1	Removing ADP Agents Using Application Performance Management Page..	19-3
19.1.2.2	Removing ADP Agents Deployed to Targets Manually	19-4
19.2	Deinstallation Procedure for JVMDB	19-5
19.2.1	Removing JVMDB Engine	19-5
19.2.1.1	Removing JVMDB Engine Using Application Performance Management Page	19-5
19.2.1.2	Removing JVMDB Engine Manually	19-6
19.2.1.3	Removing JVMDB Engine Manually Using ApmEngineSetup.pl	19-6
19.2.2	Removing JVMDB Agents	19-7
19.2.2.1	Removing JVMDB Agents Using Application Performance Management Page	19-7
19.2.2.2	Removing JVMDB Agents Deployed to Targets Manually	19-8

20 Removing Standby Oracle Management Services

20.1	Removing Additional Standby OMS Instances	20-1
20.2	Removing the First Standby OMS	20-3

Part VII Appendixes

A Understanding the Enterprise Manager Directory Structure

A.1	Understanding the Enterprise Manager Directories Installed with Oracle Enterprise Manager Cloud Control 12c A-1	
A.1.1	About the Oracle Management Service Home Directory	A-2
A.1.2	About the Oracle Management Agent Home (AGENT_HOME) Directory	A-2
A.1.3	About Business Intelligence Publisher Home Directory	A-2
A.1.4	Summary of the Important Directories in the Oracle Management Service Home..	A-2
A.2	Understanding the Enterprise Manager Directories Installed with Management Service	A-3

A.3	Understanding the Enterprise Manager Directories Installed with Management Agent.....	A-3
A.3.1	Summary of the Important Directories in the Oracle Management Agent Home....	A-4
A.3.2	Understanding the Oracle Management Agent Directory Structure in Windows ...	A-6
A.4	Identifying the Agent Instance Home When Using the emctl Command	A-6
B	Installation and Configuration Log Files	
B.1	Enterprise Manager Cloud Control Installation Logs	B-1
B.1.1	Installation Logs.....	B-1
B.1.2	Configuration Logs.....	B-1
B.1.2.1	General Configuration Logs.....	B-2
B.1.2.2	Repository Configuration Logs	B-2
B.1.2.2.1	SYSMAN Schema Operation Logs.....	B-2
B.1.2.2.2	EMPrereqKit Logs	B-4
B.1.2.2.3	MDS Schema Operation Logs.....	B-4
B.1.2.3	Secure Logs.....	B-5
B.1.2.4	Oracle Management Service Logs.....	B-5
B.2	Add Host Log Files.....	B-5
B.2.1	Initialization Logs	B-5
B.2.2	Application Prerequisite Logs	B-6
B.2.3	System Prerequisite Logs.....	B-6
B.2.4	Agent Installation Logs.....	B-6
B.2.5	Other Add Host Logs.....	B-7
B.3	Manual Management Agent Installation Logs.....	B-7
B.4	Additional OMS Installation Logs.....	B-8
C	Redirecting Oracle Management Agent to Another Oracle Management Service	
C.1	Prerequisites	C-1
C.2	Procedure	C-2
D	Applying One-Off Patches to Oracle Management Agents	
D.1	Saving Management Agent Patches to an OMS Host	D-1
D.2	Verifying Patch Application After Management Agent Deployment or Upgrade.....	D-3
E	Using RepManager Utility	
E.1	Overview	E-1
E.2	Supported Actions and Commands.....	E-1
F	Collecting OCM Data Using Oracle Harvester	
F.1	Oracle Harvester	F-1
F.1.1	Supported Targets in Oracle Harvester.....	F-4
F.1.2	Configuration Data Not Available in My Oracle Support.....	F-5
F.2	Oracle Configuration Manager	F-5
F.3	Additional Information.....	F-6

F.4	Troubleshooting Configuration Data Collection Tools	F-6
F.4.1	Oracle Harvester Collection Fails If the state/upload/external Directory Is Missing.....	F-6
F.4.2	Oracle Configuration Manager Is Not Running.....	F-7
F.4.3	Configuration Data Not Available in My Oracle Support.....	F-7
F.4.4	Only a Subset of the Targets Is Collected by the Oracle Harvester.....	F-7

G Enabling Enterprise Manager Accessibility Features

G.1	Enabling Enterprise Manager Accessibility Mode.....	G-1
G.2	Setting uix-config.xml Flag.....	G-2
G.3	Configuring web.xml File	G-2
G.4	Verifying That Screen Reader Support Is Enabled	G-3

H Configuring Targets for Failover in Active/Passive Environments

H.1	Target Relocation in Active/Passive Environments.....	H-1
H.2	Installation and Configuration.....	H-2
H.2.1	Prerequisites	H-2
H.2.2	Configuration Steps.....	H-2
H.2.2.1	Discovering Targets.....	H-2
H.2.2.2	Deploying Plug-ins.....	H-2
H.3	Failover Procedure.....	H-3
H.4	Failback Procedure	H-4
H.5	EM CLI relocate_targets Parameters.....	H-4
H.6	Relocation Script	H-5
H.6.1	Relocation Script Example.....	H-5

I Troubleshooting

I.1	Troubleshooting Configuration Assistant Failures.....	I-1
I.1.1	Plugins Prerequisite Check Configuration Assistant	I-1
I.1.2	Repository Configuration Assistant.....	I-2
I.1.3	Repository Out Of Box Configuration Assistant.....	I-3
I.1.4	MDS Schema Configuration Assistant	I-4
I.1.5	OMS Configuration Assistant	I-4
I.1.6	Plugins Deployment and Configuration Configuration Assistant.....	I-5
I.1.7	Start Oracle Management Service Configuration Assistant.....	I-6
I.1.8	Plugins Inventory Migration Configuration Assistant	I-6
I.1.9	Oracle Configuration Manager Repeater Configuration Assistant.....	I-7
I.1.10	OCM Configuration for OMS Configuration Assistant	I-7
I.1.11	Agent Configuration Assistant	I-8
I.1.12	Agent Upgrade Configuration Assistant	I-9
I.1.13	Repository Upgrade Configuration Assistant	I-9
I.1.14	Stopping APM Engines Configuration Assistant	I-10
I.1.15	Stop Admin Server Configuration Assistant	I-10
I.2	Troubleshooting ADP and JVMMD Failures	I-11
I.2.1	ADP Engine Name Conflict	I-11
I.2.2	Failure to Deploy ADP Agent On a Target.....	I-11

1.2.3	Failure to Deploy JVMD Agent On a Target	I-12
1.2.4	SSL Handshake Failure Agent Deployment Errors	I-13
1.2.5	Copying ADP Agent Zip or Javadiagnosticagent.ear Failure.....	I-13
1.3	Troubleshooting Package-Related Issues	I-14
1.4	Troubleshooting Deinstallation Failures	I-14
1.5	Troubleshooting Management Agent Installation Failures.....	I-16

Index

Preface

Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide is an extension to *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

While the *Oracle Enterprise Manager Cloud Control Basic Installation Guide* covers basic installation procedures that help you get started with Enterprise Manager Cloud Control, the *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide* covers advanced installation procedures that help you install and configure the Enterprise Manager Cloud Control components in more complex environments.

This preface contains the following topics:

- [Intended Audience](#)
- [Purpose of the Document](#)
- [Documentation Accessibility](#)
- [Related Documents](#)
- [Conventions](#)

Intended Audience

Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide is meant for system administrators who want to install Enterprise Manager Cloud Control components in complex environments.

Purpose of the Document

Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide covers the following:

- Installing the following in graphical mode:
 - Enterprise Manager Cloud Control software only so that you can configure it later
 - Oracle Management Agent using a shared Oracle home
 - Application Dependency and Performance (ADP) with advanced installation options
 - JVM Diagnostics (JVMD) with advanced installation options
- Installing the following in silent mode:
 - Enterprise Manager Cloud Control

- Enterprise Manager Cloud Control software only so that you can configure it later
- Additional Oracle Management Service
- Oracle Management Agent
- Oracle Management Agent software only so that you can configure it later
- Oracle Management Agent using a shared Oracle home
- Cloning Oracle Management Agent in graphical and silent mode
- Configuring advanced installation tasks such as configuring firewalls, sizing the Enterprise Manager deployment, and integrating BI publisher.
- Deinstalling Enterprise Manager Cloud Control and Oracle Management Agent in graphical and silent mode

Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide does NOT cover the following procedures. These procedures are documented in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

- Installing Enterprise Manager Cloud Control in graphical mode
- Installing an additional Oracle Management Service in graphical mode
- Installing Oracle Management Agent in graphical mode
- Installing JVM Diagnostics and Application Dependency and Performance with default installation options

Also, *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide* does NOT cover the procedure for upgrading your existing Enterprise Manager system. The upgrade procedure is documented in the *Oracle Enterprise Manager Cloud Control Upgrade Guide*.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Related Documents

For more information, see the following books in the Enterprise Manager Cloud Control documentation library:

- *Oracle Enterprise Manager Cloud Control Basic Installation Guide*
- *Oracle Enterprise Manager Cloud Control Upgrade Guide*
- *Oracle Enterprise Manager Cloud Control Administrator's Guide*

For the latest releases of these and other Oracle documentation, check the Oracle Technology Network at the following URL:

<http://www.oracle.com/technetwork/indexes/documentation/index.html>

Enterprise Manager also provides extensive online Help. Click **Help** at the top-right corner of any Cloud Control page to display the online help window.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Part I

Getting Started

This part describes how you can procure the Enterprise Manager Cloud Control software and the Oracle Management Agent software, and explains some key concepts you must know before you start using Enterprise Manager Cloud Control. In particular, this part contains the following chapters:

- [Chapter 1, "Procuring Software"](#)
- [Chapter 2, "Understanding the Basics"](#)

Procuring Software

This chapter describes how you can procure the Enterprise Manager Cloud Control software and the Oracle Management Agent software. In particular, this chapter covers the following:

- [Releases Available for Enterprise Manager Cloud Control](#)
- [Procuring Enterprise Manager Cloud Control Software](#)
- [Procuring Oracle Management Agent Software](#)

1.1 Releases Available for Enterprise Manager Cloud Control

[Table 1–1](#) describes the releases Enterprise Manager Cloud Control has had so far.

Table 1–1 Enterprise Manager Cloud Control Releases

Release Numbers	Release Type	Release Date	Implementation Method	Description
(Recommended) Oracle Enterprise Manager Cloud Control 12c Release 3 (12.1.0.3)	Patch Set 2 [PS2]	June 2013	<ul style="list-style-type: none"> ■ New installation of 12c Release 3 (12.1.0.3) ■ Upgrade from 12c Release 2 (12.1.0.2) ■ Upgrade from 12c Release 1 (12.1.0.1), only with BP1 ■ Upgrade from 10g Release 5 (10.2.0.5), 11g Release 1 (11.1.0.1) 	Patch set containing several bug fixes, enhancements, and new features.
Oracle Enterprise Manager Cloud Control 12c Release 2 Plug-in Update 1 (12.1.0.2)	Plug-In Update 1 <i>(Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2) software with plug-ins released in February 2013)</i>	February 2013	<ul style="list-style-type: none"> ■ New installation of 12c Release 2 (12.1.0.2) ■ Upgrade from 12c Release 1 (12.1.0.1), with or without BP1 ■ Upgrade from 10g Release 5 (10.2.0.5), 11g Release 1 (11.1.0.1) 	<p>Contains the 12c Release 2 (12.1.0.2) software binaries updated with new plug-ins and updated plug-in versions.</p> <p>However, the 12c Release 2 (12.1.0.2) software binaries have not been changed; they have only been integrated with new plug-ins and updated plug-in versions. Even the Management Agent software binaries have not been changed. This is essentially a release, and not a patch set or a patch.</p> <p>To view a list of plug-ins integrated with this release, see the <i>List of Plug-ins Integrated with this Release</i> section in the <i>Getting Started</i> chapter of the <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide 12c Release 2 (12.1.0.2)</i>. The guide is available in the Enterprise Manager documentation library at the following URL:</p> <p>http://www.oracle.com/technetwork/indexes/documentation/index.html</p>

Table 1–1 (Cont.) Enterprise Manager Cloud Control Releases

Release Numbers	Release Type	Release Date	Implementation Method	Description
Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2)	Patch Set 1 [PS1]	August 2012	<ul style="list-style-type: none"> ▪ New installation of 12c Release 2 (12.1.0.2) ▪ Upgrade from 12c Release 1 (12.1.0.1), with or without BP1 ▪ Upgrade from 10g Release 5 (10.2.0.5), 11g Release 1 (11.1.0.1) 	Patch set containing several bug fixes, enhancements, and new features.
Enterprise Manager Cloud Control 12c Release 1 (12.1.0.1)	Bundle Patch 1 [BP1]	January 2012	<ul style="list-style-type: none"> ▪ New installation of 12c Release 1 (12.1.0.1) containing BP1. ▪ Patching of the base release, that is, 12c Release 1 (12.1.0.1) ▪ Upgrade from 10g Release 5 (10.2.0.5), 11g Release 1 (11.1.0.1) 	Bundle patch containing several bug fixes and support for ported platforms.
Enterprise Manager Cloud Control 12c Release 1 (12.1.0.1)	Base Release	October 2011	<ul style="list-style-type: none"> ▪ New installation of 12c Release 1 (12.1.0.1) ▪ Upgrade from 10g Release 5 (10.2.0.5), 11g Release 1 (11.1.0.1) 	First ever 12c release.

Note: For more information on these releases and the platforms they support, access the Enterprise Manager Cloud Control Certification Matrix. For instructions to access this matrix, refer to the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

1.2 Procuring Enterprise Manager Cloud Control Software

You can procure the Enterprise Manager Cloud Control software from either the product DVD or the Oracle Technology Network (OTN) Web site. This section describes these sources and covers the following:

- [How Do You Access the Software from DVD?](#)
- [How Do You Procure the Software from Oracle Technology Network?](#)

1.2.1 How Do You Access the Software from DVD?

You can obtain the Enterprise Manager Cloud Control software from the product DVD that is available through Oracle Service Delivery Managers or Oracle Sales Representatives. The software may be available either on a single DVD or on DVDs depending on the operating system.

This section covers the following:

- [Accessing Software from DVD](#)
- [Setting Mount Point for DVD](#)

1.2.1.1 Accessing Software from DVD

If the software is available on a single DVD, then insert the DVD into the DVD drive, and manually run the Enterprise Manager Cloud Control Installation Wizard.

If the software is available on DVDs, then copy the archived software from each of the DVDs to a location on your local disk. Extract the contents of each of the archived files to the same location. Then, invoke the Enterprise Manager Cloud Control Installation Wizard.

For example, Oracle delivers three DVDs for Linux x86 and x86_64, mainly these:

DVD1, containing a ZIP file with the name `em12103_linux_disk1of3.zip`

DVD2, containing a ZIP file with the name `em12103_linux_disk2of3.zip`

DVD3, containing a ZIP file with the name `em12103_linux_disk3of3.zip`

In this case, copy the three ZIP files to a location on your disk, for example, `/temp`, and then extract their contents in the same location.

WARNING: Extracting the contents to different locations will cause the installation to fail.

```
$ cp -r em12103_linux_disk1of3.zip /temp
$ cp -r em12103_linux_disk2of3.zip /temp
$ cp -r em12103_linux_disk3of3.zip /temp
$ cd /temp
$ unzip em12103_linux_disk1of3.zip
$ unzip em12103_linux_disk2of3.zip
$ unzip em12103_linux_disk3of3.zip
```

Once the contents are extracted, you can invoke the Enterprise Manager Cloud Control Installation Wizard. To do so, on UNIX platforms, invoke `runInstaller`, and on Microsoft Windows platforms, invoke `setup.exe`.

Note: For information about the Enterprise Manager Cloud Control Installation Wizard, see [Section 2.1.2](#).

1.2.1.2 Setting Mount Point for DVD

If you want to access the DVD from a shared DVD drive, then set a mount point for the DVD drive.

On most Linux operating systems, the disk mounts automatically when you insert the DVD into the DVD drive. However, for some Linux operating systems, you might have to manually mount the disk. To verify whether the disk mounts automatically

and to manually mount the disk if it does not mount itself automatically, follow these steps:

1. Insert the DVD into the disk drive.
2. To verify if the disk is automatically mounted, run the following command:
 - On Red Hat Enterprise Linux:


```
# ls /mnt/cdrom
```
 - On SUSE Linux Enterprise Server:


```
# ls /media/cdrom
```
3. If the command in Step (2) fails to display the contents of the disk, then run the following command:
 - On Red Hat Enterprise Linux:


```
# mount -t nfs <host name>:/mnt/<full path to the dvdrom>
```
 - On SUSE Linux Enterprise Server:


```
# mount -t nfs <host name>:/media/<full path to the dvdrom>
```

On most AIX operating systems, the disk mounts automatically when you insert the DVD into the DVD drive. However, for some AIX operating systems, you might have to manually mount the disk. To manually mount the disk if it does not mount itself automatically, follow these steps:

1. Switch the user to *root* user by running the following command:


```
$ su -root
```
2. Insert the disk into the drive.

Note: If required, enter the following command to eject the currently mounted disk and to remove it from the drive:

```
# /usr/sbin/umount /<SD_DVD>
```

3. Enter the following command:

```
# /usr/sbin/mount -rv cdrfs /dev/cd0 /SD_DVD
```

In this example command, */SD_DVD* is the disk mount point directory and */dev/cd0* is the device name for the disk device.

4. If you are prompted to specify the disk location, then specify the disk mount point directory path. For example, */SD_DVD*

1.2.2 How Do You Procure the Software from Oracle Technology Network?

You can procure the Enterprise Manager Cloud Control software from OTN. The software available on OTN is archived using Info-ZIP's highly portable ZIP utility. The software is available in ZIP files. After downloading the software, you will need the UNZIP utility to extract the files.

This section covers the following:

- [Downloading Software](#)
- [Verifying File Size](#)

- [Extracting Contents](#)
- [Verifying Software Release Description](#)
- [Verifying Platform Information](#)

1.2.2.1 Downloading Software

To download the Enterprise Manager Cloud Control software from OTN, access the following URL:

<http://www.oracle.com/technetwork/oem/enterprise-manager/downloads/index.html>

The software is available in ZIP files. Download the ZIP files to a common location on your local disk.

1.2.2.2 Verifying File Size

After downloading the ZIP files, do the following:

1. Run the `cksum` command against the ZIP files and check if the file checksum of the downloaded software is the same as the file checksum displayed on OTN.

The following is the format of the ZIP files:

`em12103_<platform>_diskNofM.zip (<value> bytes) (cksum - <value>)`

Here, `<platform>` refers to the operating system, `N` refers to the ZIP file number, and `M` refers to the total number of ZIP files available for download. For example, `em12103_linux_disk1of3.zip`, `em12103_linux_disk2of3.zip`, `em12103_linux_disk3of3.zip`.

The value `(cksum - <value>)` is the file checksum that you need to check. To check the file checksum of the first ZIP file, run the following command:

```
$ cksum em12_<platform>_diskNofM.zip
```

For example,

```
$ cksum em12_linux_disk1of3.zip
```

2. Extract the contents of the ZIP files to a single directory. Navigate to the directory and verify if you see the following files:

```
[a@adcxxxxxx Disk1]$ ls
install  libskgxn  plugins          response        stage  WT.zip
jdk      oms       runInstaller     wls
```

1.2.2.3 Extracting Contents

You must unzip the archive on the platform for which it was intended. For example, if you download the software for the Linux x86 operating system, then you must unzip the file on a Linux x86 operating system only. If you unzip the file on a Microsoft Windows computer and then move the stage area to a Linux computer, then the staged area files will get corrupted. This is because Microsoft Windows does not preserve the case sensitivity or the permission bits of Linux file names.

If you have downloaded a single ZIP file, then extract the contents of it and manually run the Enterprise Manager Cloud Control Installation Wizard.

Note: For information about the Enterprise Manager Cloud Control Installation Wizard, see [Section 2.1.2](#).

If you have downloaded multiple ZIP files to a common location, then extract the contents of all the ZIP files in the same location, and then manually run the Enterprise Manager Cloud Control Installation Wizard.

WARNING: Extracting the contents to different locations will cause the installation to fail.

Tip: If you plan to store the files on a DVD, then first extract the contents of the ZIP files, and then copy those extracted files to the DVD. Do NOT copy the ZIP files; you need the unzipped contents of the ZIP files to install the product.

1.2.2.4 Verifying Software Release Description

Verify the software release details to ensure that you have downloaded the latest version.

1. After extracting the contents of the software ZIP files, navigate to the following location and access the properties file that contains the software release description:

```
Disk1/install/em/release.properties
```

2. Make sure you see the following description that confirms that it is the latest software:

Release:Oracle Enterprise Manager Cloud Control 12c Release 3 (12.1.0.3)

1.2.2.5 Verifying Platform Information

After extracting the contents of the ZIP file, access the following file to verify the platform information. Here, <Software_Location> can be either the DVD mount point or the location on your local disk where you have extracted the contents of the ZIP files.

```
<Software_Location>/stage/shiphomeproperties.xml
```

Note that a 32-bit Enterprise Manager Cloud Control software (both Enterprise Manager Cloud Control and Oracle Management Agent) can be installed only on a 32-bit operating system that is running on a 32-bit hardware. Similarly, a 64-bit Enterprise Manager software can be installed only on a 64-bit operating system that is running on a 64-bit hardware.

Do NOT try to install a 32-bit software on a 64-bit platform or vice versa; the installation may proceed, but will fail eventually. Therefore, ensure that you use the right software download for the right platform.

The shiphomeproperties.xml file provides the platform information as shown here:

```
<?xml version="1.0" standalone="yes" ?>
<ORACLEHOME_INFO>
<ARU_PLATFORM_INFO>
<ARU_ID>46</ARU_ID>
<ARU_ID_DESCRIPTION>Linux x86</ARU_ID_DESCRIPTION>
</ARU_PLATFORM_INFO>
```

</ORACLEHOME_INFO>

You can see the platform information in the <ARU_ID_DESCRIPTION> syntax. [Table 1–2](#) lists the platform names that may be enclosed in this syntax, and describes whether the names represent a 32-bit or 64-bit software.

Table 1–2 Verifying Platform Information

Platform Name	Platform Specified in ARU_ID_DESCRIPTION	32-bit / 64-bit
Linux x86	Linux x86	32-bit
Microsoft Windows (32-bit)	Win 32	32-bit
Microsoft Windows (64-bit AMD64)	win 64	64-bit
Microsoft Windows (64-bit IA)	Windows Itanium	64-bit
Solaris Operating System (SPARC 64-bit)	Solaris	64-bit
HPUX PA-RISC(64-bit)	HPUNIX	64-Bit
AIX	AIX	64-bit
HP_IA64	HPI	64-bit
Linux x86-64	Linux AMD	64-bit
linux_ia64	Linux Itanium	64-bit
IBM Power Based Linux	Linux PPC	64-bit
linux_zseries64	zLinux	64-bit
HP Tru64 UNIX	Decunix	64-bit
Solaris Operating System (x86-64)	Solaris AMD64	64-bit
Solaris Operating System (x86)	Solaris AMD32	32-bit

1.3 Procuring Oracle Management Agent Software

Oracle Management Agent (Management Agent) is one of the core components of Enterprise Manager Cloud Control, and therefore, its software is part of the Enterprise Manager Cloud Control software. When you install Enterprise Manager Cloud Control, the installation wizard automatically installs a Management Agent.

You can install additional Management Agents using the Add Host Targets Wizard built into the Enterprise Manager Cloud Control console (Cloud Control console). The wizard uses the Management Agent software that is already present in the OMS home.

However, note that the Management Agent software present in the OMS home is always for the version and platform on which that OMS is running. For example, if the OMS is Oracle Management Service 12c and it is running on Linux platform, then the Management Agent software available there is also for Linux platform.

If you want to install a Management Agent for a platform that is different from the one on which the OMS is running, then ensure that you download that software using the Self Update Console, which is built into the Cloud Control console.

For information on Self Update, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*. For instructions to download the software, see the chapter on updating Cloud Control in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

Note: The Management Agent software for 12c Release X (12.1.0.X) is not available on OTN, so the only way you can download the software is using the Self Update Console.

Understanding the Basics

This chapter introduces you to some key concepts of Enterprise Manager Cloud Control, and describes some important aspects of installation that you must know before you proceed any further.

In particular, this chapter covers the following:

- [Understanding Installation Basics](#)
- [Understanding Oracle WebLogic Server Requirement](#)
- [Understanding Installation Directories](#)
- [Understanding Configuration Assistants](#)
- [Understanding Prerequisite Checks](#)
- [Understanding Limitations of Enterprise Manager Cloud Control](#)
- [Understanding Startup Scripts](#)
- [Understanding Other Miscellaneous Concepts](#)

2.1 Understanding Installation Basics

This section describes the fundamental aspects of the installation process. In particular, this section covers the following:

- [What Different Installation Modes Can You Use?](#)
- [What Is Enterprise Manager Cloud Control Installation Wizard?](#)
- [What Installation Types Are Offered by the Installation Wizard?](#)
- [What Is Oracle Configuration Manager?](#)
- [What Are Software Updates?](#)
- [What is a Deployment Size?](#)
- [What Is Add Host Target Wizard?](#)
- [What Is Add Management Service Deployment Procedure?](#)
- [What Ports Are Used for Installation?](#)
- [What Data Files Are Created While Configuring Oracle Management Repository?](#)
- [How Do You Delete Data Files?](#)

2.1.1 What Different Installation Modes Can You Use?

You can install Enterprise Manager Cloud Control or any of its core components either in an interactive, graphical mode or in a silent mode.

Graphical Mode	Graphical mode is the Graphical User Interface (GUI) method that involves usage of a Java-based installation wizard or a browser-based application that is built into and accessed from the Enterprise Manager Cloud Control console. This method is best suited for first-time installations because you are guided through the entire installation process and your installation details are captured using the interview screens.
Silent Mode	Silent method involves usage of Oracle-supplied response files or scripts that capture all the information required for installation. This method is simpler and faster, but requires you to have some knowledge on the installation process so that you can provide your installation details in the response files without having to see the interview screens of the installation wizard.

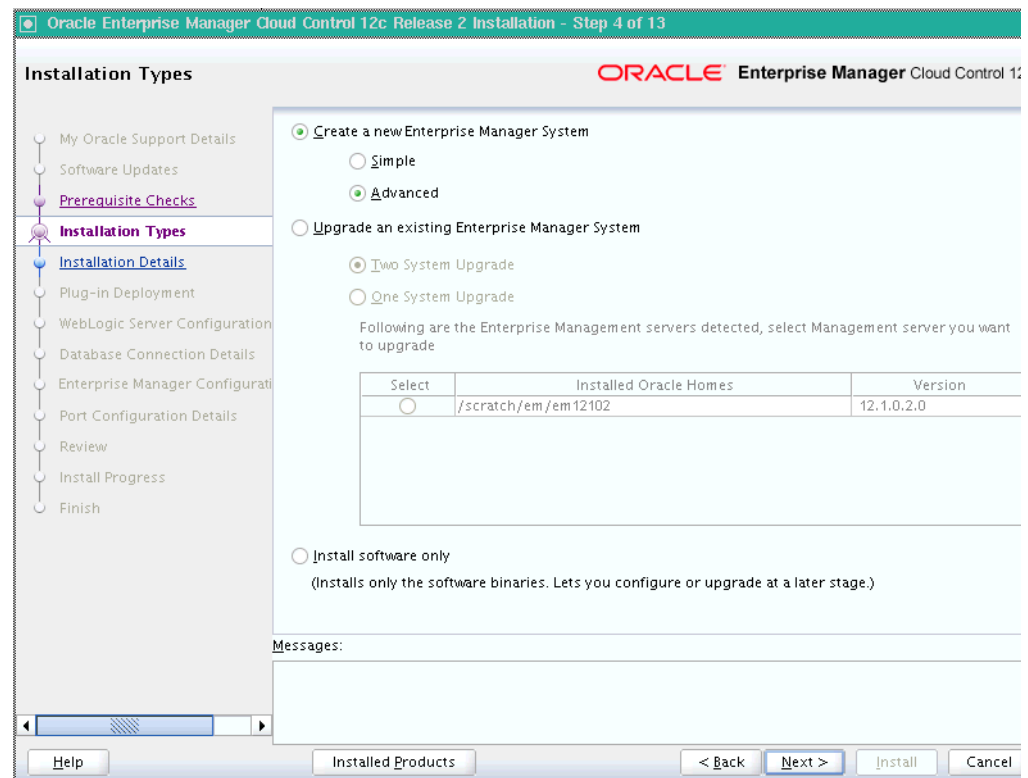
In both these modes, you can perform a *software-only* installation. A *Software-Only* installation is an approach that enables you to install only the software binaries of Enterprise Manager Cloud Control or a Management Agent, that is, without any configuration to the installation. This is best suited when you want to install the software at one point and configure it later.

2.1.2 What Is Enterprise Manager Cloud Control Installation Wizard?

Enterprise Manager Cloud Control Installation Wizard is a Java-based wizard that helps you install or upgrade to Enterprise Manager Cloud Control in graphical mode. If you are installing Enterprise Manager Cloud Control or any of its core components for the first time, then Oracle strongly recommends you to use this installation wizard.

Note: To invoke the installation wizard on UNIX platforms, run `runInstaller`. To invoke on Microsoft Windows platforms, run `setup.exe`.

[Figure 2–1](#) describes the key elements of the installation wizard.

Figure 2–1 Enterprise Manager Cloud Control Installation Wizard

2.1.3 What Installation Types Are Offered by the Installation Wizard?

The Enterprise Manager Cloud Control Installation Wizard offers the following installation types:

- [Create a New Enterprise Manager System](#)
- [Upgrade an Existing Enterprise Manager System](#)
- [Install Software Only](#)

2.1.3.1 Create a New Enterprise Manager System

This installation type enables you to install a new Enterprise Manager Cloud Control system with either simple or advanced configuration settings. For information about simple and advanced installation types, refer to *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

For information about what is installed for both simple and advanced installation types, refer to *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

2.1.3.2 Upgrade an Existing Enterprise Manager System

This installation type enables you to upgrade the following to Enterprise Manager Cloud Control 12c Release 3 (12.1.0.3):

- Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2) [(12.1.0.2) or (12.1.0.2) Plug-in Update 1]
- Enterprise Manager Cloud Control 12c Release 1 (12.1.0.1) [with Bundle Patch 1]
- Enterprise Manager 11g Grid Control Release 1 (11.1.0.1)

- Enterprise Manager 10g Grid Control Release 5 (10.2.0.5)

For upgrading Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) and Enterprise Manager 11g Grid Control Release 1 (11.1.0.1), you can select one of the following approaches. However, for upgrading Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2) or 12c Release 1 (12.1.0.1) with Bundle Patch 1, you can select only *One System Upgrade* approach.

- **One System Upgrade**, enables you to upgrade to Enterprise Manager Cloud Control on the same host where your earlier release of Enterprise Manager is running. This approach also upgrades the Management Repository in the existing Oracle Database itself. Since the upgrade happens on the same host, there is a reasonable downtime involved.
- **Two System Upgrade**, enables you to install Enterprise Manager Cloud Control on a host that is different from the host where your existing Enterprise Manager system is running. This approach does not upgrade the Management Repository in the existing Oracle Database, but upgrades the one in the backed up database, thus offering the scope for two Enterprise Manager systems to exist. Since a new Enterprise Manager system coexists with the old one, there is *no or near zero* downtime involved.

Note: For more information on these upgrade options, see the *Oracle Enterprise Manager Cloud Control Upgrade Guide*.

2.1.3.3 Install Software Only

This installation type enables you to install only the software binaries of Enterprise Manager Cloud Control at one point, and configure it at a later point.

This approach helps you divide the installation process into two phases, mainly the installation phase and the configuration phase. Understandably, the installation phase takes less time compared to the configuration phase because the installation phase involves only copying of binaries.

For information about what is installed during the installation phase and what is configured during the configuration phase, refer to [Section 4.1](#).

2.1.4 What Is Oracle Configuration Manager?

With Enterprise Manager Cloud Control, you can choose to enable Oracle Configuration Manager. Alternatively, you can enable it after installing Enterprise Manager Cloud Control.

Oracle Configuration Manager automatically collects configuration information from your environment at regular intervals and uploads it to Oracle repository. This helps Oracle maintain up-to-date information about your environment, identify security vulnerabilities, quickly diagnose support issues, and offer better solutions consistently.

However, no business or personal information is collected and uploaded, except for local contact name in the event of transmission problems. Oracle guarantees that all the information collected will be kept strictly confidential and under no circumstances will this information be shared with any other party.

Oracle recommends that the host from where you are running the installation wizard have a connection to the Internet so that the configuration information can be automatically collected and uploaded to My Oracle Support.

If the host from where you are running the installation wizard has a connection to the Internet, then on the Oracle Configuration Manager screen of the installation wizard, enter the My Oracle Support user name (or e-mail address) and password.

Otherwise, enter only the e-mail address and leave the other fields blank. After you complete the installation, manually collect the configuration information and upload it to My Oracle Support. To understand how the configuration information can be manually collected and uploaded, see the steps outlined in [Section 2.1.4.1](#).

If you want to enable it after installing Enterprise Manager Cloud Control, then see [Section 2.1.4.2](#).

2.1.4.1 Manually Collecting and Uploading Configuration Information

To manually collect the configuration information, follow these steps:

1. Navigate to the OMS home and run the following command:

```
$<OMS_HOME>/ccr/bin/emCCR collect
```

For Oracle Configuration Manager 10.2.7 and higher, the collected configuration information is stored in the `/ccr/hosts/state/upload/ocmconfig.jar` file. For lower versions of Oracle Configuration Manager, the collected configuration information is stored in the `/ccr/state/upload/ocmconfig.jar` file. When you run the same command next time, the `ocmconfig.jar` file gets overwritten with fresh data. Therefore, at any point, you will see only one `ocmconfig.jar` file.

2. Upload the `ocmconfig.jar` file to a Service Request on My Oracle Support.
3. Repeat Step (1) and Step (2) from the Management Agent home.

2.1.4.2 Enabling Oracle Configuration Manager After Installing Enterprise Manager Cloud Control

To enable Oracle Configuration Manager at a later point, do the following:

1. Set the environment variable `ORACLE_CONFIG_HOME` to the Oracle Management Service instance base directory. Oracle Management Service instance base is the directory where the configuration files of the OMS are created.
 - In bash terminal, run the following command:


```
export ORACLE_CONFIG_HOME=<absolute_path_to_gc_inst>
```
 - In other terminals, run the following command:


```
setenv ORACLE_CONFIG_HOME <absolute_path_to_gc_inst>
```

Note: For information about Oracle Management Service instance base directory, refer to [Section 2.3.3](#).

2. From the OMS home, run the following command:

```
$<OMS_HOME>/ccr/bin/setupCCR
```

2.1.5 What Are Software Updates?

This section describes the following:

- [What Is a Software Update?](#)
- [How Does the Software Update Feature Work?](#)

- [What Types of Software Updates Are Downloaded and Applied?](#)
- [How Can I Find Out What Bugs Have Been Fixed by the Software Updates?](#)
- [How Can You Download the Software Updates?](#)
- [Can I Download and Apply These Patches After Installation or Upgrade?](#)
- [How Can You Identify What Patches Have Been Applied?](#)

2.1.5.1 What Is a Software Update?

Software Update is a feature built in to the Enterprise Manager Cloud Control Installation Wizard. The feature appears as the Software Updates screen in the installer, and enables you to automatically download and deploy the latest recommended patches while installing or upgrading Enterprise Manager Cloud Control.

This way, you do not have to keep a manual check on the patches released by Oracle. All patches required by the installer for successful installation and upgrade are automatically detected and downloaded from My Oracle Support, and applied during the installation or upgrade, thus reducing the known issues and potential failures.

Note: The patches available via the Software Updates screen must be downloaded only via the Software Updates screen, and not from My Oracle Support.

2.1.5.2 How Does the Software Update Feature Work?

The Software Update feature connects to My Oracle Support and first downloads patch 16729224. Patch 16729224 essentially consists of a file called `patch.xml` that the installer parses and creates a directory titled `updates` to download all the required updates. The `updates` directory has the following subdirectories:

- `updates/agent`
Contains patches related only to the central agent (Management Agent installed with the OMS).
- `updates/oms`
Contains patches related to the OMS.
- `updates/metadata`
Contains a subdirectory `patch 16729224`, inside which you will find the `patch.xml` that determines what all updates must be downloaded and on which Oracle home they must be applied.

Note: All software updates must be downloaded and applied only via the Software Updates screen in the Installer, and not from My Oracle Support.

2.1.5.3 What Types of Software Updates Are Downloaded and Applied?

The following are the different types of updates that can be applied using this feature:

- OUI/Opatch Updates

Includes the latest OUI/Opatch versions or their updates. If a new version of the installer is downloaded, then OUI is restarted and launched from the location where the latest version is downloaded.

- **Prerequisite Updates**

Includes new prerequisite check-related updates released in response to issues reported after a release of Enterprise Manager Cloud Control. This enables OUI to always run the latests set of prerequisite checks, thus resulting in a smoother installation or upgrade experience.

- **EM installer Updates**

Includes updates that fix OUI issues—essentially, Java code changes that most likely results in automatic restart of OUI after their application.

- **Interim Patch Updates**

Includes patches such as DST patches, performance-related patches, and so on. They are automatically detected, downloaded, and applied.

- **Patch Set Updates**

Includes multiple patch updates that fix bugs, enhance existing features, and also sometimes introduce new features.

2.1.5.4 How Can I Find Out What Bugs Have Been Fixed by the Software Updates?

To know what bugs or issues have been fixed by the software updates downloaded via the Software Updates screen, refer to My Oracle Support note 1099123.1.

2.1.5.5 How Can You Download the Software Updates?

You can download the software updates in one of the following ways:

- **Download by User (Offline Mode):** Use this option when you do not have Internet connectivity on the host where you are installing Enterprise Manager, to connect to My Oracle Support.
- **Automatic Download by Installation Wizard (Online Mode):** Use this option when you have Internet connectivity to connect to My Oracle Support automatically using the Enterprise Manager Cloud Control Installation Wizard.

The following sections describe how you can download the software updates in offline and online modes.

Download by User (Offline Mode)

To download the software updates, follow these steps:

Caution: Make sure you download and apply the software updates only using the installer. DO NOT directly download them from My Oracle Support.

1. On a host that has Internet connectivity, invoke the Enterprise Manager Cloud Control Installation Wizard with the `-downloadUpdates` argument in the following way. This argument ensures that the installation wizard is invoked only for downloading the software updates.

```
./runInstaller -downloadUpdates
```

Note:

- On Microsoft Windows, run `setup.exe -downloadUpdates`.
 - Make sure you download these updates on another host (with Internet connectivity) that runs on the same operating system as the host on which you want to invoke the installer and install the product. For example, if you want to install on Linux, then make sure the host with Internet connectivity on which you are downloading these updates also runs on Linux. Similarly, if you want to install on Microsoft Windows, make sure you download the patches on another host that runs on Microsoft Windows.
-

Enterprise Manager Cloud Control Installation Wizard appears with only two screens, the titles of which appear on the left menu.

2. On the Software Updates screen, enter the *My Oracle Support* account user name and password, and click **Search for Updates**. The installation wizard displays the *Downloading Updates* dialog, and downloads the software updates to `/tmp/OraInstall<timestamp>/updates`. Click **Next**.

The installation wizard restarts itself, and this time, displays all the screens, the titles of which appear on the left menu. Exit the installation wizard because you have invoked it on this host only to download the software updates, and not install the OMS.

3. Copy the entire updates directory to the host where you want to install the OMS.

Note: Make sure the host from where you are copying the directory and the host on which you are copying the directory run on the same operating system. For example, if you downloaded the updates to the directory on Linux host, then make sure you copy it to another Linux host where want to install the product. Copying the directory across operating systems is not recommended for the installation.

4. On the host where you want to install the OMS, invoke the installation wizard.
 - **In Graphical Mode:** On the Software Updates screen of the installation wizard, select **Search for Updates**, and then, select **Local Directory**. Enter the location where you copied the updates, and click **Search for Updates**. To search the computer and select the location, click **Browse**.

For example, if you copied the entire updates directory to `/u01/home/em/`, then select or enter `/u01/home/em/updates`.

Once the search results appear with patch numbers and their details, click the patch number to view the ReadMe associated with that patch. Otherwise, click **Next**. The installer automatically applies all the patches while installing or upgrading the Enterprise Manager system.

- **In Silent Mode:** Invoke the installer passing the response file with the `INSTALL_UPDATES_SELECTION` parameter set to `"staged"`, and the `STAGE_LOCATION` parameter set to the absolute path of the location where the updates are available.

Note: If you have a proxy server set up, then invoke the installation wizard passing the `-showProxy` argument. For example, if you are invoking in graphical mode, then invoke in the following way:

```
<Software_Location>/runInstaller -showProxy
```

Automatic Download by Installation Wizard (Online Mode)

On a host that has Internet connectivity, invoke the Enterprise Manager Cloud Control Installation Wizard.

- **In Graphical Mode:** On the Software Updates screen of the installation wizard, select **Search for Updates**, then select **My Oracle Support**. Enter the *My Oracle Support* account user name and password, and click **Search for Updates**.

Once the search results appear with patch numbers and their details, click the patch number to view the ReadMe associated with that patch. Otherwise, click **Next**. The installer automatically applies all the patches while installing or upgrading the Enterprise Manager system.

- **In Silent Mode:** Invoke the installer passing the response file with the `INSTALL_UPDATES_SELECTION` parameter set to "download", and the `MYORACLESUPPORT_USERNAME_FOR_SOFTWAREUPDATES` and the `MYORACLESUPPORT_PASSWORD_FOR_SOFTWAREUPDATES` parameters set to your *My Oracle Support* credentials.

2.1.5.6 Can I Download and Apply These Patches After Installation or Upgrade?

No, you must download and apply the software updates only at the time of installing or upgrading the Enterprise Manager system. The software updates fix issues with the installation or upgrade process, and therefore, they are necessary at the time of installing or upgrading the Enterprise Manager system.

2.1.5.7 How Can You Identify What Patches Have Been Applied?

To identify what patches have been applied, run the following command from the OMS home or the Management Agent home. The output of this command lists all the applied patches.

```
<ORACLE_HOME>/OPatch/opatch lsinventory
```

2.1.6 What is a Deployment Size?

When you install Enterprise Manager Cloud Control with advanced configuration settings (*Advanced* installation type), you have an option of selecting the deployment size of your choice. This option is available in both graphical mode (Enterprise Manager Cloud Control Installation Wizard) and silent mode (response file).

The deployment size essentially indicates the number of targets you plan to monitor, the number of Management Agents you plan to have, and the number of concurrent user sessions you plan to have.

Table 2–1 describes each deployment size.

Table 2–1 Deployment Size

Deployment Size	Targets Count	Management Agents Count	Concurrent User Session Count
Small	Up to 999	Up to 99	Up to 10

Table 2–1 (Cont.) Deployment Size

Deployment Size	Targets Count	Management Agents Count	Concurrent User Session Count
Medium	Between 1000 and 9999	Between 100 and 999	Between 10 and 24
Large	10,000 or more	1000 or more	Between 25 and 50

Note: If the database you are connecting to is a database instance created with a preconfigured Management Repository using the database templates offered by Oracle, then make sure the deployment size you select on this screen matches with the deployment size for which you ran the SQL script as described in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. Otherwise, you will see errors.

If you want to select a deployment size different from the deployment size for which you ran the SQL script earlier, then do one of the following:

- Minimize the installer, run the SQL script intended for the deployment size you want to select, then return to this screen and select the desired deployment size. To understand the SQL script to be run for each deployment size, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
 - Select the deployment size of your choice on this screen, and click **Next**. When you see errors, manually fix the parameters in the database, then return to this screen to continue with the installation.
-

The prerequisite checks are run regardless of the selection you make, but the values to be set for the various parameters checked depend on the selection you make. For more information about these deployment sizes, and the database parameters set for each of them, refer to [Chapter 12](#).

After installing Enterprise Manager Cloud Control with a particular deployment size, you can choose to increase or decrease the count of targets, Management Agents, or concurrent user sessions. However, if you do increase the count to a level that is not appropriate for the selected deployment size, then the performance might suffer. Under such circumstances, Oracle recommends you to modify the database parameters according to the desired deployment size, as described in [Chapter 12](#).

2.1.7 What Is Add Host Target Wizard?

The Add Host Targets Wizard ([Figure 2–2](#)) is a GUI-rich application accessible from within the Cloud Control console, and used for installing Management Agents on unmanaged hosts and converting them to managed hosts in the Enterprise Manager system.

Using the Add Host Targets Wizard, you can do the following:

- Install a fresh Management Agent
- Clone an existing well-tested, pre-patched, and running Management Agent
- Install a Management Agent from an existing, centrally shared Management Agent

Figure 2–2 Add Host Target Wizard

ORACLE Enterprise Manager Cloud Control 12c Help

Add Target

Host and Platform Installation Details Review

Add Host Targets : Host and Platform Back Step 1 of 3 Next Cancel

This wizard enables you to install Management Agents on unmanaged hosts, thereby converting them to managed hosts. Enter a session name, and validate (or add) the hosts and their platforms on which you want to install the Management Agent.

* Session Name ADD_HOST_SYSMAN_Jul_6_2011_11:30:37_PM_PDT

+ Add - Remove Load from File Add Discovered Hosts Platform Different for Each Host

Host	Platform
host.example.com	Linux x86

TIP The target host's platform is defaulted based on a combination of factors, including hints received from automated discovery and the platform of the OMS host. default is a suggestion, however, we recommend you to check the platform details before processing to the next step.

TIP If the platform name is appended with "Agent Software Unavailable", then download the software for that platform using 'Self Update'

Although the Add Host Targets Wizard can be used for remotely installing one Management Agent, the wizard is best suited for mass-deployment of Management Agents, particularly while mass-deploying Management Agents of different releases on hosts of different platforms. The wizard gives you the flexibility to select hosts on which you want to install a Management Agent. This helps you when you want to install the Management Agent on several hosts, in one attempt.

2.1.8 What Is Add Management Service Deployment Procedure?

A deployment procedure is a procedure that contains a hierarchical sequence of provisioning or patching steps, where each step may contain a sequence of other steps. In other words, the workflow of all tasks that need to be performed for a particular life cycle management activity is encapsulated in a deployment procedure.

Enterprise Manager Cloud Control offers deployment procedures, and all of these can be accessed from within the Cloud Control console. One of the deployment procedures that falls within the context of Enterprise Manager Cloud Control installation is the Add Management Service deployment procedure.

The Add Management Service deployment procedure (Figure 2–3) helps you meet high-availability requirements by enabling you to install an additional OMS using an existing OMS that is running on an AdminServer host.

Figure 2–3 Add Management Service Deployment Procedure

Oracle Enterprise Manager Cloud Control 12c

Getting Started **Select Destination** Options Post Creation Steps Review

Add Oracle Management Service : Select Destination [Back] Step 2 of 5 [Next] [Cancel]

Middleware Home: /ade/pjaganat_admen/oracle/work/middlewai

Source Management Service: example .com

* Destination Host: [Search Icon]

Specify the host where the Management Service has to be added.

Destination Instance Base Location: /ade/pjaganat_admen/oracle/work

Specify a location where the configuration files for the Management Service will be created. The location must have approximately 100 MB of free disk space.

Source Credentials

Specify operating system credentials of the user that owns the Management Service software installation on the source host.

Credential: ☒ Preferred ☐ Named ☐ New

Preferred Credential Name: Normal Host Credentials

Credential Details: Default credentials are not set

Destination Credentials

Specify operating system credentials of the user that will own the Management Service software installation on the destination host. It is required that the user name be the same on all Management Service hosts.

Credential: ☒ Preferred ☐ Named ☐ New

Preferred Credential Name: Normal Host Credentials

Credential Details: Credentials will be determined at runtime.

In simple words, the Add Management Service deployment procedure enables you to install additional OMS instances in your environment. The deployment procedure clones an existing OMS and replicates its configuration to the destination host.

The earlier releases of Enterprise Manager offered this installation type from the Enterprise Manager Installation Wizard. However, for the Enterprise Manager Cloud Control release, this installation type is offered as a deployment procedure.

For more information about the deployment procedure, see the chapter on adding additional management service in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

2.1.9 What Ports Are Used for Installation?

This section describes the default ports that are honored while installing Enterprise Manager Cloud Control. In particular, this section covers the following:

- [What Default Ports Are Used?](#)
- [How Can You Customize Ports?](#)
- [What Precautions You Must Take While Customizing Port Numbers?](#)

2.1.9.1 What Default Ports Are Used?

The following are the default ports used for installation:

- **Enterprise Manager Cloud Control**

Upload Port

Console Port

HTTP Port	4889 If 4889 is not available, then the first available free port from the range 4889 to 4898 is selected.	The first available free port from the range 7788 - 7798 is selected.
HTTPS Port	1159 If 1159 is not available, then the first available free port from the range 4899 to 4908 is selected.	The first available free port from the range 7799 - 7809 is selected.

- **Oracle Management Agent**

The default upload port for Management Agent is 3872. The same port is used for both HTTP and HTTPS. If 3872 is not available, then the first available free port from the range 1830 to 1849 is selected.

- **Admin Server**

The default HTTPS port for Admin Server is 7101. If 7101 is not available, then the first available free port from the range 7101 to 7200 is selected.

- **Node Manager**

The default HTTPS port for Node Manager is 7401. If 7401 is not available, then the first available free port from the range 7401 to 7500 is selected.

- **Managed Server**

The default HTTP port for Managed Server is 7201. If 7201 is not available, then the first available free port from the range 7201 to 7300 is selected.

The default HTTPS port for Managed Server is 7301. If 7301 is not available, then the first available free port from the range 7301 to 7400 is selected.

2.1.9.2 How Can You Customize Ports?

Enterprise Manager Cloud Control offers you the flexibility to use custom ports instead of default ports.

Customizing Ports While Installing Enterprise Manager Cloud Control

WARNING: Do NOT set any port to a value lower than or equal to 1024. Ports up to 1024 are typically reserved for root users (super users). Therefore, make sure the port you customize is always set to a value greater than 1024.

- If you are installing Enterprise Manager Cloud Control (advanced installation) in graphical mode, that is, using the Enterprise Manager Cloud Control Installation Wizard, then you can use the Port Configuration Details screen to enter custom ports. You can also import a `staticports.ini` file that already captures the custom ports.
- If you are installing Enterprise Manager Cloud Control in silent mode, that is, using the installation procedures described in [Part II](#), then update the `staticports.ini` file with suitable custom ports.

The `staticports.ini` file is available at the following location of the software kit (DVD, downloaded software, and so on):

```
<software_kit>/response/staticports.ini
```

Customizing HTTP/HTTPS Console and Upload Ports After Installing Enterprise Manager Cloud Control

WARNING: Do NOT set any port to a value lower than or equal to 1024. Ports up to 1024 are typically reserved for root users (super users). Therefore, make sure the port you customize is always set to a value greater than 1024.

If you want to change the HTTP/HTTPS console ports and upload ports after installing Enterprise Manager Cloud Control, then follow these steps:

1. Stop the OMS:

```
$<OMS_HOME>/bin/emctl stop oms -all
```

2. Update the emoms properties with HTTP and HTTPS ports as described in [Table 2-2](#). Specify the values for parameters `<http_upload_new>`, `<https_upload_new>`, `<http_console_new>`, and `<https_console_new>`:

Table 2-2 Updating EMOMS Properties with HTTP and HTTPS Ports

Port/Property Type	Command to Run
HTTP Upload Port	<code><OMS_Home>/bin/emctl set property -name oracle.sysman.emSDK.svlt.ConsoleServerPort -value <http_upload_new></code>
HTTPS Upload Port	<code><OMS_Home>/bin/emctl set property -name oracle.sysman.emSDK.svlt.ConsoleServerHTTPSPort -value <https_upload_new></code>
HTTP Console Port	<code><OMS_Home>/bin/emctl set property -name oracle.sysman.emSDK.svlt.EMConsoleServerPort -value <http_console_new></code>
HTTPS Console Port	<code><OMS_Home>/bin/emctl set property -name oracle.sysman.emSDK.svlt.EMConsoleServerHTTPSPort -value <https_console_new></code>

3. Back up the following file:

```
$<OMS_INSTANCE_HOME>/emgc.properties
```

After backing up the file, open the original `emgc.properties` file, and specify the new port numbers for the following parameters:

```
EM_UPLOAD_HTTP_PORT=<http_upload_new>
EM_UPLOAD_HTTPS_PORT=<https_upload_new>
EM_CONSOLE_HTTP_PORT=<http_console_new>
EM_CONSOLE_HTTPS_PORT=<https_console_new>
```

4. Back up the files `httpd.conf`, `ssl.conf`, and `httpd_em.conf` from the following location:

```
$<WEBTIER_INSTANCE_HOME>/config/OHS/ohs#
```

After backing up the files, open the original files, and specify the new port numbers:

- In `httpd.conf` file, in the **Listen** directive section, replace `<http_console_orig>` with `<http_console_new>`.

- In `ssl.conf` file, in the **Listen** and **Virtual Host** directive sections, replace `<https_console_orig>` with `<https_console_new>`.
 - In `httpd_em.conf` file, in the **Listen** and **VirtualHost** directive section, replace `<http_upload_orig>` with `<http_upload_new>`, and `<https_upload_orig>` with `<https_upload_new>`, respectively.
5. Start the OMS, and verify its status:


```
$<OMS_HOME>/bin/emctl start oms
$<OMS_HOME>/bin/emctl status oms -details
```
 6. If the OMS is configured with any Server Load Balance (SLB), then update the ports in the SLB pools, monitors, and so on.
 7. If the OMS is configured for SSO or OAM, then re-run the SSO or OAM configuration.
 8. Back up the following file:


```
$<AGENT_INSTANCE_HOME>/sysman/config/emd.properties
```

Note: Back up the `emd.properties` file from all Management Agents that are communicating with the OMS.

After backing up the file, open the original `emd.properties` file, and verify the URL mentioned in `REPOSITORY_URL`. If the URL is an HTTPS URL, then change the port number to `<https_upload_new>`. If the URL is an HTTP URL, then change the port number to `<http_upload_new>`.

9. If there are any EM CLI instances set up on the ports you have changed, then set up those instances again. To do so, from each EM CLI instance, run the command `emcli setup` or `emcli status`, and note the EM URL that appears.

If you have changed that port number, run the following command:

```
emcli setup -url=http(s)://<host>:<new_port#>/em -dir=<dir>....
```

2.1.9.3 What Precautions You Must Take While Customizing Port Numbers?

While updating the `staticports.ini` file, you must be extremely careful because an error in the file can cause the installation wizard to use default ports without displaying any warning. Therefore, before updating the `staticports.ini` file, check for these points:

- Do NOT set any port to a value lower than or equal to 1024. Ports up to 1024 are typically reserved for root users (super users). Therefore, make sure the port you customize is always set to a value greater than 1024.
- If a port is already being used by a component or any other application, do not enter that port (used port) in the `staticports.ini` file. If you do, then the related configuration assistant also fails.
- If you have entered the same port for more than one component, then the installation displays an error after the prerequisite checks phase. You must rectify this error before proceeding with the installation.
- If you have syntax errors in the `staticports.ini` file (for example, if you omitted the equal (=) character for a line), then the installation wizard ignores the line. For the components specified on such lines, the installation wizard assigns the default

ports. The installation wizard does not display a warning for lines with syntax errors.

- If you misspell a component name, then the installation wizard assigns the default port for the component. Names of components in the file are case-sensitive. The installation wizard does not display a warning for lines with unrecognized names.
- If you enter a nonnumeric value for the port number, then the installation wizard ignores the line and assigns the default port number for the component. It does this without displaying any warning.
- If you misspell the parameter on the command line, then the installation wizard does not display a warning. It continues and assigns default ports to all components.
- If you enter a relative path to the `staticports.ini` file (for example, `./staticports.ini`) in the command line, then the installation wizard does not find the file. It continues without displaying a warning and it assigns default ports to all components. You must enter a full path to the `staticports.ini` file.

2.1.10 What Data Files Are Created While Configuring Oracle Management Repository?

The following are the data files created while configuring Oracle Management Repository:

<code>mgmt.dbf</code>	Stores information about the monitored targets, their metrics, and so on.
<code>mgmt_ecm_depot1.dbf</code>	Stores configuration information collected from the monitored targets.
<code>mgmt_deepdive.dbf</code>	Stores monitoring data related to JVM Diagnostics and Application Dependency Performance (ADP).

2.1.11 How Do You Delete Data Files?

To delete the data files, you must drop the SYSMAN/MDS schema. To do so, run the following command from the OMS home.

```
$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager <repository_database_host>
<repository_database_port> <repository_database_sid> -action dropall
-dbUser <repository_database_user> -dbPassword <repository_database_
password> -dbRole <repository_database_user_role> -mwHome <middleware_
home> -mwOraHome <oms_home> -oracleHome <oms_home>
```

Note:

- For Microsoft Windows, invoke `RepManager.bat`.
 - If you are dropping the schemas that belong to a 10g Release 2 (10.2.x.x) Management Repository, then run the command without these arguments:

```
-mwHome <middleware_home> -mwOraHome <middleware_ora_
home> -oracleHome <OMS_HOME>
```
-

After dropping the schema, manually delete the database files `mgmt.dbf` and `mgmt_ecm_depot1.dbf`.

You can find these files by running the following command as SYS:


```
SELECT FILE_NAME FROM DBA_DATA_FILES WHERE UPPER (TABLESPACE_NAME) LIKE
'MGMT%';
```

[Table 2–3](#) describes the `-action` options that are supported by the different versions of RepManager.

Table 2–3 RepManager Support for `-action dropall` Command

RepManager Version	Command Supported
RepManager 12.1	<ul style="list-style-type: none"> ▪ <code>-action dropall</code> ▪ <code>-action drop</code> <p>The commands drop SYSMAN, SYSMAN_MDS, SYSMAN_APM, SYSMAN_OPSS, and SYSMAN_RO.</p>
RepManager 11.1	<ul style="list-style-type: none"> ▪ <code>-action dropall</code> <p>The command drops only SYSMAN and SYSMAN_MDS.</p> <ul style="list-style-type: none"> ▪ <code>-action drop</code> <p>The command drops only SYSMAN.</p>
RepManager 10.2.0.5	<p><code>-action drop</code></p> <p>The command drops only SYSMAN.</p>

2.2 Understanding Oracle WebLogic Server Requirement

Enterprise Manager Cloud Control requires Oracle WebLogic Server 11g Release 1 (10.3.6) and Java Development Kit 1.6.0.43.0.

If Oracle WebLogic Server 11g Release 1 (10.3.6) and Java Development Kit 1.6.0.43.0 are NOT already installed in your environment, then the installation wizard automatically installs them for you while installing a new Enterprise Manager Cloud Control.

This section describes some important aspects related to Oracle WebLogic Server that you must know before you install Enterprise Manager Cloud Control.

In particular, this section covers the following:

- [How Do I Verify Whether Oracle WebLogic Server Is Installed?](#)
- [Is Oracle WebLogic Server Cluster Supported?](#)
- [If Oracle WebLogic Server Already Exists, Is the Existing Domain Used?](#)
- [When and Why Do You Need Oracle WebLogic Server Credentials?](#)
- [When and Why Do You Need Node Manager Credentials?](#)
- [How Do You Find Admin Server Port After Installing Enterprise Manager?](#)
- [How Do You Verify Whether Admin Server Is Running?](#)
- [How Do You Start Admin Server?](#)

2.2.1 How Do I Verify Whether Oracle WebLogic Server Is Installed?

To verify whether Oracle WebLogic Server is installed, check the following file in the Oracle Middleware home:

```
$<MW_HOME>/logs/log.txt
```

The following is the sample output of the `log.txt` file:

```
release 10.3.6.0 [Added]
|____Common Infrastructure Engineering 7.1.0.0 [Added]
|   |____Uninstall [Added]
|   |____Patch Client [Added]
|   |____Patch Attachment Facility [Added]
|   |____Clone Facility [Added]
|____WebLogic Server 10.3.6.0 [Added]
|   |____Core Application Server [Added]
|   |____Administration Console [Added]
|   |____Configuration Wizard and Upgrade Framework [Added]
|   |____Web 2.0 HTTP Pub-Sub Server [Added]
|   |____WebLogic SCA [Added]
|   |____WebLogic JDBC Drivers [Added]
|   |____Third Party JDBC Drivers [Added]
|   |____WebLogic Server Clients [Added]
|   |____WebLogic Web Server Plugins [Added]
|   |____UDDI and Xquery Support [Added]
|   |____Server Examples [Added]
|   |____Evaluation Database [Added]
|   |____Workshop Code Completion Support [Added]
|____Oracle Configuration Manager 10.3.3.1 [Added]
|   |____Data Collector [Added]
|____Oracle Coherence 3.6.0.3 [Not Installed]
|   |____Coherence Product Files [Not Installed]
|   |____Coherence Examples [Not Installed]
```

2.2.2 Is Oracle WebLogic Server Cluster Supported?

Oracle WebLogic Server cluster consists of Oracle WebLogic Servers running simultaneously and working together to provide increased scalability and reliability. A cluster appears to be a single Oracle WebLogic Server instance. The server instances that constitute a cluster can run on the same host, or be located on different hosts.

You can install Enterprise Manager Cloud Control on an Oracle WebLogic Server Cluster, however, you cannot take advantage of the cluster configurations.

2.2.3 If Oracle WebLogic Server Already Exists, Is the Existing Domain Used?

If Oracle WebLogic Server already exists, then the existing domain is NOT used. Instead, the Enterprise Manager Cloud Control Installation Wizard creates a new domain and deploys the Enterprise Manager Cloud Control software to it.

2.2.4 When and Why Do You Need Oracle WebLogic Server Credentials?

While installing or upgrading to Enterprise Manager Cloud Control, you are prompted to enter the Oracle WebLogic Server credentials (user name and password). The credentials are used for creating the WebLogic domain and other associated components such as the Admin Server, the managed server, and the node manager.

The WebLogic user name is the default user name that will be used as the administrative user for the WebLogic Domain. By default, the user name is `weblogic`. And the WebLogic password is the password for this default administrative user account.

2.2.5 When and Why Do You Need Node Manager Credentials?

While installing or upgrading to Enterprise Manager Cloud Control, you are prompted to enter the Node Manager password for the default Node Manager user

account, which is `nodemanager`. The password is used for configuring the Node Manager. A Node Manager enables you to start, shut down, or restart an Oracle WebLogic Server instance remotely, and is recommended for applications with high availability requirements.

2.2.6 How Do You Find Admin Server Port After Installing Enterprise Manager?

To find the Admin Server port, view the value set for the `AS_HTTPS_PORT` parameter in the `emgc.properties` file. This file is available in the Oracle Management Service Instance Base location.

For example,

```
/DATA/oracle/gc_inst/em/EMGC_OMS1/emgc.properties
```

2.2.7 How Do You Verify Whether Admin Server Is Running?

To install an additional OMS, the Admin Server that is used by the first OMS must be up and running. To verify whether the Admin Server is running, access the Admin Server console using the following URL:

```
https://host:port/console
```

Here, `host` and `port` are values specified in the `EM_INSTANCE_HOST` and `AS_HTTPS_PORT` parameters, respectively, in the `emgc.properties` file. This properties file is available in the Oracle Management Service Instance Base location of the first OMS.

For example,

```
/DATA/oracle/gc_inst/em/EMGC_OMS1/emgc.properties
```

2.2.8 How Do You Start Admin Server?

You can start the Admin Server by running the following command. Although the command is used essentially to start the OMS, the command in turn starts the Admin Server on which that OMS is running. So run this command even if you know that the OMS is already running.

```
emctl start oms
```

2.3 Understanding Installation Directories

This section describes the installation directories that need to be entered while installing Enterprise Manager Cloud Control or any of its core components. In particular, this section covers the following:

- [What Is Oracle Inventory Directory?](#)
- [What Is Oracle Middleware Home?](#)
- [What Is Oracle Management Service Instance Base Location?](#)
- [What Is Oracle Home?](#)
- [What Is Agent Base Directory?](#)
- [What is Agent Instance Directory?](#)
- [What Is /TMP C:\Temp Directory Used For?](#)

2.3.1 What Is Oracle Inventory Directory?

If Enterprise Manager Cloud Control is the first Oracle product that you are installing, then the Enterprise Manager Cloud Control Installation Wizard prompts you to enter an inventory directory (also called the *oraInventory* directory).

This inventory directory is used by the installation wizard to place all the installer files and directories on the host. The installation wizard automatically sets up subdirectories for each Oracle product to contain the inventory data.

You can enter the *oraInventory* directory in two ways:

- While installing Enterprise Manager Cloud Control using the installation wizard, you can enter the *oraInventory* directory in the Oracle Inventory screen. When you enter it in this screen, you must also select the appropriate operating system group name that will own the *oraInventory* directories. The group you select must have write permission on the *oraInventory* directories.
- While installing Enterprise Manager Cloud Control in silent mode, that is, without using the installation wizard, you can enter the *oraInventory* directory using the `-invPtrLoc` parameter. This parameter considers the path to a location where the inventory pointer file (`oraInst.loc`) is available. However, this parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.

For example

```
./runInstaller -invPtrLoc /scratch/OracleHomes/oraInst.loc
```

Note: Ensure that the *oraInventory* directory is not in a shared location. If it is, change it to a non-shared location.

If you already have an Oracle product installed on the host, then the installation wizard uses the existing *oraInventory* directory that was created while installing that Oracle product. Ensure that you have *write* permission on that directory. To do so, run the installer as the same operating system user as the one who installed the other Oracle product.

Note: The *oraInventory* directory is different from *Installation Directory*. For information about *Installation Directory*, see [Section 2.3.2](#).

2.3.2 What Is Oracle Middleware Home?

While installing or upgrading to Enterprise Manager Cloud Control, you are required to enter the Oracle Middleware home.

Oracle Middleware home (Middleware home) is the parent directory that has the Oracle WebLogic Server home, the Java Development Kit, the Web tier instance files, one or more Oracle homes, the OMS instance base directory, and other relevant files. This is where the OMS and the plug-ins are deployed.

For example,

```
/u01/app/Oracle/Middleware
```

If you are installing or upgrading to Enterprise Manager Cloud Control, then:

- If Oracle WebLogic Server 11g Release 1 (10.3.6) and Java Development Kit 1.6.0.43.0 are already installed in your environment, then the installation wizard

automatically detects them and displays the absolute path to the Middleware home where they are installed.

In this case, validate the Middleware home that is detected and displayed by default. If the location is incorrect, then enter the path to the correct location. Ensure that the Middleware home you select or enter is a Middleware home that does not have any Oracle homes.

- If Oracle WebLogic Server 11g Release 1 (10.3.6) and Java Development Kit 1.6.0.43.0 are NOT already installed in your environment, then the installation wizard automatically installs them for you while installing Enterprise Manager Cloud Control.

In this case, enter the absolute path to a directory where you want to have them installed. Ensure that the directory you enter does not contain any files or subdirectories.

For example,

```
/u01/app/Oracle/Middleware/
```

Note: *Oracle Middleware home* is different from *Oracle Home* of OMS or Management Agent. For information about *Oracle Home*, see [Section 2.3.4, "What Is Oracle Home?"](#).

2.3.3 What Is Oracle Management Service Instance Base Location?

While installing Enterprise Manager Cloud Control, you are required to enter the Oracle Management Service Instance Base Location.

Oracle Management Service Instance Base Location is a directory (*gc_inst*) outside the Middleware home where the configuration files of the OMS are stored.

The installation wizard uses its built-in algorithm to identify this location, and displays it for you to validate. If the Middleware home is

`/u01/app/Oracle/Middleware/`, then by default, the following is the Oracle Management Service Instance Base Location:

```
/u01/app/Oracle/gc_inst
```

You can either accept the default location or specify another location that has *write* permission.

Note: For information about *Oracle Middleware home*, see [Section 2.3.2](#).

2.3.4 What Is Oracle Home?

Oracle Home or *Oracle home* is the directory where the OMS, the Management Agent, and the plug-ins are installed. [Table 2–4](#) lists the default *Oracle homes* are created.

Table 2–4 Oracle Homes of OMS, Management Management Plug-Ins

Component	Default Oracle Home	Sample Location
Oracle Management Service	<code>\$<MIDDLEWARE_HOME>/oms</code>	<code>/u01/app/Oracle/Middleware/oms</code>
Oracle Management Agent	<code>\$<AGENT_BASE_DIR>/core/12.1.0.3.0</code>	<code>/u01/app/Oracle/agent/core/12.1.0.3.0</code>

Table 2–4 (Cont.) Oracle Homes of OMS, Management Management Plug-Ins

Component	Default Oracle Home	Sample Location
Plug-In (OMS-specific plug-ins)	<code>\$<MIDDLEWARE_HOME>/plugins/<pluginID_Version></code>	<code>/u01/app/Oracle/software/plugins/oracle.sysman.db.agent.plugin_12.1.0.3.0</code>
Plug-In (agent-specific plug-ins)	<code>\$<AGENT_BASE_DIR>/plugins</code>	<code>/u01/app/Oracle/agent/plugins</code>

Note: *Oracle Home* is different from *OraInventory*. For information about *OraInventory* directory, see [Section 2.3.1](#).

2.3.5 What Is Agent Base Directory?

While installing Enterprise Manager Cloud Control and a standalone Management Agent using the Add Host Targets Wizard, you are required to enter an installation base directory, which is essentially the agent base directory.

Agent Base Directory is a directory outside the Oracle Mddleware Home, where the Management Agent home is created.

For example, if the agent base directory is `/u01/app/Oracle/agent`, then the Management Agent home is created as `/u01/app/Oracle/agent/core/12.1.0.3.0`.

2.3.6 What is Agent Instance Directory?

Agent Instance Directory is a directory (`agent_inst`) created for storing all Management Agent-related configuration files.

Agent Instance Directory is created inside the agent base directory.

For example, if the agent base directory is `/u01/app/Oracle/agent`, then by default, the following is the agent instance directory:

`/u01/app/Oracle/agent/agent_inst`

2.3.7 What Is /TMP C:\Temp Directory Used For?

When you invoke the Enterprise Manager Cloud Control Installation Wizard, it automatically copies some executable files and link files to a temporary directory on the host.

For example, the default `/tmp` directory on UNIX hosts, and `C:\Temp` on Microsoft Windows hosts.

If the host is set to run `cron` jobs along with many other processes that may be running periodically, then these jobs attempt to clean up the default temporary directory, thereby deleting some files and causing the installation wizard to fail.

If there are any `cron` jobs or processes that are automatically run on the hosts to clean up the temporary directories, then ensure that you set the `TMP` or `TEMP` environment variable to a location that is different from the default location. Ensure that the non-default location you set is secure on the hard drive, that is, the non-default location is a location where cleanup jobs are not run. Also ensure that you have *write* permissions on this alternative directory.

This must be done before you run the installer to invoke the Enterprise Manager Cloud Control Installation Wizard. (For UNIX operating systems, you invoke `runInstaller`, and for Microsoft Windows, you invoke `setup.exe`).

Note: Specifying an alternative temporary directory location is not mandatory, and is required only if any cron jobs are set on the computers to clean up the `/tmp` directory.

2.4 Understanding Configuration Assistants

This section describes the postinstallation activities that are performed by the installation wizard. In particular, this section covers the following:

- [What Are Configuration Assistants?](#)
- [What Configuration Assistants Are Run by the Installation Wizard?](#)
- [What Do You Do When Configuration Assistants Fail?](#)

2.4.1 What Are Configuration Assistants?

While installing or upgrading to Enterprise Manager Cloud Control in either GUI mode (using the installation wizard) or silent mode (using a response file), a set of configuration assistants are run at the end of the installation process to configure the installed or upgraded components. Your installation or upgrade process is complete only after all the components are configured using these configuration assistants.

Note: Even when you perform a software-only installation of Enterprise Manager, when you run the `ConfigureGC.sh` script to configure the installation, the configuration assistants are internally run. (On Microsoft Windows, run the `ConfigureGC.bat` script.)

2.4.2 What Configuration Assistants Are Run by the Installation Wizard?

This section lists the configuration assistants run by the installation wizard for the different installation types.

- [Configuration Assistants Run While Installing a New Enterprise Manager](#)
- [Configuration Assistants Run While Upgrading an Existing Enterprise Manager](#)
- [Configuration Assistants Run While Upgrading an Additional Oracle Management Service](#)

2.4.2.1 Configuration Assistants Run While Installing a New Enterprise Manager

The following are the configuration assistants that are run while installing a new Enterprise Manager, that is, when you select *Create a new Enterprise Manager System* in the installation wizard.

- Plugins Prerequisites Check
- Repository Configuration

Note: If you use a database instance that was created with a preconfigured Management Repository using the database templates offered by Oracle, then *Repository Out-of-Box Configuration* is run instead of *Repository Configuration*.

- MDS Schema Configuration

Note: If you use a database instance that was created with a preconfigured Management Repository using the database templates offered by Oracle, then *MDA Schema Configuration* is not run.

- OMS Configuration
- Plugins Deployment and Configuration
- Start Oracle Management Service
- Oracle Configuration Manager Repeater Configuration
- Agent Configuration Assistant

2.4.2.2 Configuration Assistants Run While Upgrading an Existing Enterprise Manager

The following are the configuration assistants that are run while upgrading an existing Enterprise Manager, that is, when you select *Upgrade an existing Enterprise Manager System* in the installation wizard.

1-System Upgrade Approach

- Plugins Prerequisite Check
- Repository Upgrade
- MDS Schema Configuration
- OMS Configuration
- Plugins Deployment and Configuration
- Start Oracle Management Service
- Oracle Configuration Manager Repeater Configuration
- Plugins Inventory Migration (*does not run if you are upgrading from 12c Release X (12.1.0.X) to 12c Release X (12.1.0.X)*).

In addition, while upgrading 12c Release 1 (12.1.0.1) with Bundle Patch1 or 12c Release 2 (12.1.0.2) to 12c Release 3 (12.1.0.3), the following are run:

- Stopping APM Engines
- Stop Admin Server (*does not run if you are upgrading from 10g Release 5 (10.2.0.5) to 12c Release X (12.1.0.X)*)

Note: Agent Configuration Assistant is not run because the Management Agent is not upgraded as it is either predeployed by the *Preupgrade Console* (for 10.2.0.5 or 11.1 Management Agents) or upgraded using the *Agent Upgrade Console* (for 12.1.0.1 [with Bundle Patch 1] and 12.1.0.2 Management Agents).

2-System Upgrade Approach

- Plugins Prerequisite Check
- Repository Upgrade
- MDS Schema Configuration
- OMS Configuration
- Plugins Deployment and Configuration
- Start Oracle Management Service
- Oracle Configuration Manager Repeater Configuration
- Agent Configuration Assistant

1-System Upgrade Approach on a Different Host

- Plugins Prerequisite Check
- Repository Upgrade
- MDS Schema Configuration
- OMS Configuration
- Plugins Deployment and Configuration
- Plugins Inventory Migration
- Start Oracle Management Service
- Oracle Configuration Manager Repeater Configuration
- Agent Configuration Assistant

2.4.2.3 Configuration Assistants Run While Upgrading an Additional Oracle Management Service

Additional OMS instances are upgraded only using the 1-system upgrade approach. The following are the configuration assistants that are run while upgrading an additional OMS, that is, when you select *Upgrade an existing Enterprise Manager System*, then select an additional OMS in the installation wizard.

- Plugins Prerequisite Check
- OMS Configuration
- Plugins Deployment and Configuration
- Start Oracle Management Service
- Oracle Configuration Manager Repeater Configuration

In addition, while upgrading 12c Release 1 (12.1.0.1) with Bundle Patch 1 or 12c Release 2 (12.1.0.2) to 12c Release 3 (12.1.0.3), the following are run:

- Stopping APM Engines

- Stop Admin Server (does not run if you are upgrading from 10g Release 5 (10.2.0.5) to 12c Release X (12.1.0.X))

Note: The Agent Configuration Assistant is not run because the Management Agent is not upgraded as it is either predeployed by the *Preupgrade Console* (for 10.2.0.5 or 11.1 Management Agents) or upgraded using the *Agent Upgrade Console* (for 12.1.0.1 [with Bundle Patch 1] and 12.1.0.2 Management Agents).

2.4.3 What Do You Do When Configuration Assistants Fail?

If an optional configuration assistant fails, then the installation wizard ignores the failure and runs to the next configuration assistant automatically. However, if a mandatory configuration assistant fails, then the installation wizard stops the installation process. In this case, you are expected to resolve the issue and rerun the configuration assistant.

For information about the log files to review when a configuration assistant fails, and the actions to be taken to resolve the issue, see [Appendix I](#).

2.5 Understanding Prerequisite Checks

Every time you install Enterprise Manager Cloud Control using the installation wizard, a set of prerequisite checks are run to verify if the environment meets the minimum requirements for a successful installation. The installation wizard checks for a variety of things including required operating system patches, operating system packages, kernel parameters, and so on.

The following sections describe these prerequisite checks. In particular, this section covers the following:

- [What Prerequisite Checks Are Run by Default?](#)
- [How Can You Run Prerequisite Checks in Standalone Mode?](#)

2.5.1 What Prerequisite Checks Are Run by Default?

The following are the default prerequisite checks that are run for different installation types—*Creating a New Enterprise Manager System* and *Upgrading an Existing Enterprise Manager System*:

- Prerequisite check for verifying whether the installation is being done on a certified operating system.
- Prerequisite check for verifying whether all the certified packages and libraries have been installed.
- Prerequisite check for verifying whether the glibc package has been installed. (*Not applicable for Management Agent installation*)
- Prerequisite check for verifying whether there is sufficient disk space in the temp directory. (*Not applicable for Management Agent installation*)
- Prerequisite check for verifying whether there is sufficient disk space in the inventory directory.
- Prerequisite check for verifying whether there is *write* permission in the inventory directory. (*Not applicable for OMS installation*)

- Prerequisite check for verifying whether the software is compatible with the current operating system.
- Prerequisite check for verifying whether there is sufficient physical memory.
- Prerequisite check for verifying the required `ulimit` value. (*Not applicable for Management Agent installation*)
- Prerequisite check for verifying the host name.
- Prerequisite check for verifying whether the `LD_ASSUME_KERNEL` environment variable is set. (*Not applicable for Management Agent installation*)
- Prerequisite check for verifying whether proper timezone is set.
- Prerequisite check for verifying whether there is 4 GB of swap space. (*Not applicable for Management Agent installation*)
- Prerequisite check for verifying whether the `http_proxy` environment variable is set. Ideally, it must not be set.

2.5.2 How Can You Run Prerequisite Checks in Standalone Mode?

You can run the prerequisite checks in standalone mode before invoking the installation wizard. This helps you identify and resolve issues that might otherwise cause the installation to fail.

Table 2–5 shows the commands you need to run to run the prerequisite checks in standalone mode:

Table 2–5 Running Prerequisite Checks in Standalone Mode

Installation Type	Command
<ul style="list-style-type: none"> ■ Create a New Enterprise Manager System ■ Upgrade an Existing Enterprise Manager System ■ Install Software Only 	<pre><Software_Location>/install/runInstaller -prereqchecker PREREQ_CONFIG_ LOCATION=<Software_Location>/stage/prereq -entryPoint "oracle.sysman.top.oms_Core" -prereqLogLoc <absolute_path_to_log_ location> -silent -waitForCompletion</pre>

Note: On Microsoft Windows, replace `/runInstaller` with `setup.exe`. Also, `<Software_Location>` mentioned in the commands in Table 2–5 refer to the location where the Enterprise Manager software is available. For example, DVD. If you have downloaded the software from Oracle Technology Network (OTN), then enter the absolute path to that downloaded location.

2.6 Understanding Limitations of Enterprise Manager Cloud Control

This section describes the limitations you might face while using Enterprise Manager Cloud Control. In particular, this section covers the following:

- [Can You Access Unlicensed Components?](#)
- [What Are the Limitations with DHCP-Enabled Machines?](#)

2.6.1 Can You Access Unlicensed Components?

Although the installation media in your media pack contain many Oracle components, you are permitted to use only those components for which you have purchased

licenses. Oracle Support Service does not provide support for components for which licenses have not been purchased.

For more information, access the Enterprise Manager documentation library at the following URL and view the *Oracle Enterprise Manager Licensing Information Guide*:

<http://www.oracle.com/technetwork/indexes/documentation/index.html>

2.6.2 What Are the Limitations with DHCP-Enabled Machines?

Do NOT run the OMS on a computer that is DHCP enabled. Oracle strongly suggests that you use a static host name or IP address assigned on the network for Enterprise Manager Cloud Control components to function properly.

For more information, refer to *My Oracle Support* Note 428665.1 at:

<https://support.oracle.com/>

2.7 Understanding Startup Scripts

By default, Enterprise Manager Cloud Control offers a startup script called `gcstartup` with every installation of OMS and Management Agent. The startup script ensures that the OMS and the Management Agent are started automatically every time their hosts are rebooted, thereby relieving you of the manual effort.

Where Is the Startup Script Stored?

The startup script is present in the following location of the OMS host and the Management Agent host:

```
/etc/init.d/gcstartup
```

What Does the Startup Script Invoke?

On the OMS host, the startup script invokes the following file to start up the OMS when its host is rebooted:

```
$<OMS_HOME>/install/unix/scripts/omsstup
```

Similarly, on the Management Agent host, the startup script invokes the following file to start up the Management Agent when its host is rebooted:

```
$<AGENT_HOME>/install/unix/scripts/agentstup
```

How Do I Stop the Startup Script from Starting the OMS or the Management Agent?

If you do not want the startup script to start the OMS and the Management Agent when their hosts are rebooted, then remove the `omsstup` file and the `agentstup` file from the respective hosts.

Alternatively, you can rename the file `/etc/oragchomelist` to `/etc/oragchomelist_bak`.

Can the Startup Script Start an OMS or a Management Agent on a Remote Host?

The startup script is specific to the host on which an OMS or a Management Agent is installed. Therefore, the startup script cannot start an OMS or a Management Agent on a remote host.

Is the Startup Script Available for All Operating Systems?

While the startup script exists on UNIX operating systems, there is no such script for Microsoft Windows operating systems. However, on Microsoft Windows, the startup functionality is offered by the inherent Windows Service that is available within the Microsoft Windows framework.

2.8 Understanding Other Miscellaneous Concepts

This section covers miscellaneous concepts related to the installation of Enterprise Manager Cloud Control. In particular, this section covers the following:

- [What Is a Host List File?](#)
- [What Scripts Are Run During the Installation Process?](#)

2.8.1 What Is a Host List File?

While using the Add Host Targets Wizard, you can enter the hosts on which you want to install Oracle Management Agent, in two ways — you can either enter the host name or the IP address, or select an external file that contains a list of hosts mentioned.

If you choose to select an external file, then ensure that the file contains only the host name ([Example 2–1](#)), or the host name followed by the platform name ([Example 2–2](#)).

Example 2–1 External File with Only the Host Names

```
host1.example.com
host2.example.com
```

Example 2–2 External File with the Host Names and Platform Names

```
host1.example.com linux
host2.example.com aix
```

2.8.2 What Scripts Are Run During the Installation Process?

At least once during or after the installation of Enterprise Manager Cloud Control or Management Agent, you are prompted to log in as a *root* user and run `oraInstRoot.sh`, `allroot.sh`, or `root.sh`. You must log in as a *root* user because the scripts edit files in the `/etc` directory and create files in the local bin directory (`/usr/local/bin`, by default).

After every installation, a check is performed to identify the Central Inventory (`oraInventory`) directory. The Central Inventory directory is a directory that is automatically created by the installation wizard when an Oracle product is installed on a host for the very first time.

Note: Ensure that the central inventory location you specify must NOT be on a shared file system. If it is already on a shared file system, then switch over to a non-shared file system.

- If you have NOT installed an Oracle product before on the host, then run the `oraInstRoot.sh` script from the Central Inventory:

```
$Home/oraInventory/oraInstRoot.sh
```

The `oraInstRoot.sh` script is run to create the `oraInst.loc` file. The `oraInst.loc` file contains the Central Inventory location.

- However, if you already have an Oracle product on the host, then run `allroot.sh` script from the OMS home:
`<OMS_HOME>/allroot.sh`

Part II

Installing Enterprise Manager System

This part describes the different ways of installing Enterprise Manager Cloud Control. In particular, this part contains the following chapters:

- [Chapter 3, "Installing Enterprise Manager System in Silent Mode"](#)
- [Chapter 4, "Installing Enterprise Manager Software Now and Configuring Later"](#)

Installing Enterprise Manager System in Silent Mode

This chapter describes how you can install Enterprise Manager Cloud Control while utilizing an existing, certified Oracle Database, in silent mode. In particular, this section covers the following:

- [Overview](#)
- [Before You Begin](#)
- [Prerequisites](#)
- [Installation Procedure](#)
- [After You Install](#)

Note: All general purpose file systems, including OCFS2 and ACFS, are acceptable for storing Enterprise Manager Cloud Control 12c software binaries and OMS instance home files (configuration files in `gc_inst`). However, OCFS is not considered a general purpose file system, and therefore is not considered acceptable for this use.

3.1 Overview

If you are familiar with the way Enterprise Manager is installed, and if you want to install it without facing any interview screens of the installation wizard, then the best option is to install it in silent mode.

In silent mode, you use a response file that captures all the information you need to successfully complete an installation. This saves time and effort in one way because the installation details are captured just once, and in a single file that can be circulated and reused for installation on other hosts.

However, whether you install Enterprise Manager in graphical mode or silent mode, the installation process, the installed components, and the configuration process remain the same. Therefore, silent mode of installing Enterprise Manager is only an option offered to you.

To understand what components are installed, what configuration assistants are run, and how the directory structure will look after installation, see the chapter on installing Enterprise Manager system in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

3.2 Before You Begin

Before you begin, keep these points in mind:

- You must ensure that you have the latest Enterprise Manager Cloud Control software.

To download the latest software, access the following URL:

<http://www.oracle.com/technetwork/oem/enterprise-manager/downloads/index.html>

For information about downloading the latest software, refer to [Section 1.2.2](#).

- Ensure that there are no white spaces in the name of the directory where you download and run the Enterprise Manager Cloud Control software from. For example, do not download and run the software from a directory titled `EM Software` because there is a white space between the two words of the directory name.
- You can install Enterprise Manager Cloud Control only on a single host—locally on the server where you invoke the installation wizard with a response file. You cannot install on remote hosts.
- To invoke the installation wizard on UNIX platforms, run `runInstaller`. To invoke on Microsoft Windows platforms, run `setup.exe`.
- Oracle Management Service 12c can communicate only with the following versions of Oracle Management Agent 12c:

Table 3–1 OMS and Management Agent Compatibility for 12c Release

	Oracle Management Agent 12c Release 3 (12.1.0.3)	Oracle Management Agent 12c Release 2 (12.1.0.2)	Oracle Management Agent 12c Release 1 (12.1.0.1) + Bundle Patch 1 <i>(Refers to agents and their plug-ins patched or upgraded to, or installed with Bundle Patch 1)</i>
Oracle Management Service 12c Release 3 (12.1.0.3)	Yes	Yes	Yes
Oracle Management Service 12c Release 2 (12.1.0.2)	No	Yes	Yes
Oracle Management Service 12c Release 1 (12.1.0.1) + Bundle Patch 1	No	No	Yes

- You must not set the `ORACLE_HOME` and `ORACLE_SID` environment variables. You must ensure that the Oracle directories do NOT appear in the `PATH`.
- The Enterprise Manager Cloud Control Installation Wizard installs Java Development Kit (JDK) 1.6.0.43.0 and Oracle WebLogic Server 11g Release 1 (10.3.6), but only if you do not specify the use of existing installations. Oracle

strongly recommends using the 12c installation process to install the JDK and Oracle WebLogic Server for use with Enterprise Manager 12c.

- If Oracle WebLogic Server 11g Release 1 (10.3.6) does not exist and if you choose to manually install it, then ensure that you install it using JDK 1.6.0.43.0 (64-bit version for 64-bit platforms and 32-bit version for 32-bit platforms).

- Download JDK 1.6.0.43.0 for your platform from the platform vendor's Web site.

For example, download SUN JDK 1.6.0.43.0 for Linux platforms from the following Oracle Web site URL:

<http://www.oracle.com/technetwork/java/javase/downloads/index.html>

- If you already have JDK, then verify its version by navigating to the <JDK_Location>/bin directory and running the following command:

```
"./java -fullversion"
```

To verify whether it is a 32-bit or a 64-bit JDK, run the following command:

```
"file *"
```

- JROCKIT is not supported.
- If you want to manually install Oracle WebLogic Server 11g Release 1 (10.3.6) on Linux 64-bit platforms, first install the 64-bit JDK for your platform, and then download and use the `wls1036_generic.jar` file to install Oracle WebLogic Server.

For example,

```
<JDK home>/bin/java -d64 -jar <absolute_path_to_wls1036_generic.jar>
```

- If you want to manually install Oracle WebLogic Server 11g Release 1 (10.3.6) on Linux 32-bit platforms, then download and use either the `wls1036_linux32.bin` file or the `wls1036_generic.jar` file.

For example,

```
<JDK home>/bin/java -jar <absolute_path_to_wls1036_generic.jar>
```

- You must follow the instructions outlined in the *Oracle® Fusion Middleware Installation Guide for Oracle WebLogic Server* to install Oracle WebLogic Server. The guide is available in the Fusion Middleware documentation library available at:

<http://www.oracle.com/technetwork/middleware/weblogic/documentation/index.html>

- You must ensure that the Oracle WebLogic Server installation is a typical installation, and even if you choose to perform a custom installation, ensure that components chosen for custom installation are the same as the ones associated with a typical installation.
- You must ensure that the user installing the WebLogic Server is the same as the one installing Enterprise Manager Cloud Control.
- After installing Oracle WebLogic Server, make sure you apply patch 14482558 and patch 13349651 on it. For instructions, see the following URL:

http://docs.oracle.com/cd/E14759_01/doc.32/e14143/intro.htm#CHDCAJFC

For more information on Oracle WebLogic Server downloads and demos, access the following URL:

<http://www.oracle.com/technology/products/weblogic/index.html>

- You must ensure that the Oracle WebLogic Server 11g Release 1 (10.3.6) installed by the Enterprise Manager Cloud Control Installation Wizard or by you is dedicated for Enterprise Manager Cloud Control. You must not have any other Oracle Fusion Middleware product installed in that Middleware home.

Enterprise Manager Cloud Control cannot coexist with any Oracle Fusion Middleware product in the same Middleware home because the `ORACLE_COMMON` property is used by both the products.

- Do not install on a symlink. Installing in such a location may impact life cycle operations such as patching and scaling out.
- You can optionally use the database templates offered by Oracle to create a database instance with a preconfigured Management Repository. To do so, refer to *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. You can use such a database instance for simple as well as advanced installation.

However, note that the database templates are essentially designed for simple installation, although they can be used for advanced installation. Therefore, while performing an advanced installation (possibly with small, medium, or large deployment size selection), when you provide the details of such a database, you will be prompted that the database parameters need to be modified to suit the deployment size you selected. You can confirm the message to proceed further. The installation wizard will automatically set the database parameters to the required values.

- If you are creating the OMS instance base directory (`gc_inst`) on an NFS-mounted drive, then after you install, move the lock files from the NFS-mounted drive to a local file system location. Modify the lock file location in the `httpd.conf` file to map to a location on a local file system. For instructions, refer to [Section 3.5](#).
- Enterprise Manager is not affected when you enable or disable features such as XML DB on the Oracle Database in which you plan to configure the Management Repository. Therefore, you can enable or disable any feature in the database because Enterprise Manager does not rely on them
- If you want to optionally follow the configuration guidelines for deploying the Management Repository so that your management data is secure, reliable, and always available, refer to the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.
- By default, the software updates cannot be applied during installation because the `INSTALL_UPDATES_SELECTION` variable in the response file is set to "skip". However, if you want to apply them during installation, then you can modify this variable as described in [Table 3-3](#).
- Oracle offers bug fixes for a product based on the *Oracle Lifetime Support Policy*. When the license period expires for a particular product, the support for bug fixes offered by Oracle also ends. For more information, see the *Oracle Lifetime Support Policy* available at:

<http://www.oracle.com/support/library/brochure/lifetime-support-technology.pdf>

When determining supportability and certification combinations for an Enterprise Manager Cloud Control installation, you must consider Enterprise Manager Cloud

Control's framework components as well as the targets monitored by Enterprise Manager Cloud Control. Oracle recommends keeping your Cloud Control components and targets updated to the latest certified versions in order to receive code fixes without having to purchase an Extended Support license.

- You can find the OMS and Management Agent entries in the `/etc/oragchomelist` file for all UNIX platforms except HPUNIX, HPia64, Solaris Sparc.

On HPUNIX, HPia64, Solaris Sparc platforms, the entries are present in `/var/opt/oracle/oragchomelist`.

- As a prerequisite, you must have an existing Oracle Database to configure the Management Repository. This database can also have the Automatic Memory Management (AMM) feature enabled.
- The locale-specific data is stored in the `<OMS_Oracle_Home>/nls/data` directory. Oracle strongly recommends that you either set the environment variable `ORA_NLS10` to `<OMS_Oracle_Home>/nls/data` or do not set at all.
- If you install the OMS and the Oracle Database, which houses the Management Repository, on the same host, then when you reboot the host, the OMS and the Management Agent installed with it will not automatically start up. You will have to manually start them.
- Enforcing option is supported for Security-Enhanced Linux (SELinux).

3.3 Prerequisites

Meet the prerequisites described in the chapter on installing Enterprise Manager system that is available in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

3.4 Installation Procedure

This section covers the following:

- [Installing Enterprise Manager](#)
- [Using Advanced Installer Options](#)
- [Understanding the Limitations](#)
- [Editing Response File for Installing Software](#)

3.4.1 Installing Enterprise Manager

To install a complete Enterprise Manager system in silent mode, follow these steps:

Note: Oracle recommends you to run the EM Prerequisite Kit before invoking the installer to ensure that you meet all the repository requirements beforehand. Even if you do not run it manually, the installer anyway runs it in the background while installing the product. However, running it manually beforehand sets up your Management Repository even before you can start the installation or upgrade process. For information on the kit, to understand how to run it, and to know about the prerequisite checks it runs, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

1. Copy the following response file to an accessible location on your local host:

```
<Software_Location>/response/new_install.rsp
```

In this command, <Software_Location> is either the DVD location or the location where you have downloaded the software kit.

2. Edit the response file and enter appropriate values for the variables described in [Table 3–3](#).
3. Invoke the installer. (On Unix, make sure you invoke the installer as a user who belongs to the oinstall group you created. For information about creating operating system groups and users, see the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.)
 - If this is the first Oracle product you are installing on the host, then run the following command:

```
./runInstaller -silent -responseFile <absolute_path>/new_install.rsp [-invPtrLoc <absolute_path_to_orainst.loc>]
```
 - Otherwise, run the following command:

```
./runInstaller -silent -responseFile <absolute_path>/new_install.rsp
```

Note:

- To invoke the installation wizard on UNIX platforms, run `runInstaller`. To invoke on Microsoft Windows platforms, run `setup.exe`.
- Ensure that there are no white spaces in the name of the directory where you download and run the Enterprise Manager Cloud Control software from. For example, do not download and run the software from a directory titled `EM Software` because there is a white space between the two words of the directory name.
- When you invoke `runInstaller` or `setup.exe`, if the Enterprise Manager Cloud Control Installation Wizard does not appear, then it is possible that you do not have read and write access to `/stage`, which is a subdirectory in the `Disk1` directory of the Enterprise Manager software.

There is a classpath variable that the installation wizard computes for OPatch as `../stage/Components/`, and when the `TEMP` variable is set to `/tmp`, the installation wizard tries to look for the `opatch` JAR file in the `/tmp/ ../stage` directory, which is equivalent to `/stage`. However, if you do not have read and write permission on `/stage`, then the installation wizard can hang. Under such circumstances, verify if you have read and write access to the `/stage` directory. If you do not have, then set the `TEMP` variable to a location where the install user has access to, and then relaunch the installation wizard.

- If you connect to a database instance that was created using the database template offered by Oracle, then you will be prompted that the database parameters need to be modified to suit the deployment size you selected. This is because the templates are essentially designed for simple installation, and the database parameters are set as required for simple installation. Since it is used for advanced installation, the parameters must be set to different values. You can confirm the message to proceed further. The installation wizard will automatically set the parameters to the required values.
 - For information about the additional, advanced options you can pass while invoking the installer, refer to [Section 3.4.2](#).
-

Note:

- If a prerequisite check fails reporting a missing package, then make sure you install the required package, and retry the installation. The installer validates the package name as well as the version, so make sure you install the packages of the minimum versions mentioned in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. To understand the logic the installer uses to verify these packages, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
 - If any repository-related prerequisite check fails, then run the check manually. For instructions, see the appendix on EM Prerequisite Kit in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
 - If a configuration assistant fails, the installer stops and none of the subsequent configuration assistants are run. Resolve the issue and retry the configuration assistant. For more information, see [Appendix I](#).
-

3.4.2 Using Advanced Installer Options

The following are some additional, advanced options you can pass while invoking the installer:

- By default, a Provisioning Advisor Framework (PAF) staging directory is created for copying the Software Library entities related to the deployment procedures. By default, this location is the scratch path location (/tmp). The location is used only for provisioning activities—entities are copied for a deployment procedure, and then, deleted once the deployment procedure ends.

If you want to override this location with a custom location, then invoke the installer with the EM_STAGE_DIR option, and enter a unique custom location.

For example,

```
./runInstaller EM_STAGE_DIR=/home/john/software/oracle/pafdir -silent  
-responseFile <absolute_path>/new_install.rsp
```

- After the installation ends successfully, the OMS and the Management Agent start automatically. If you do not want them to start automatically, then invoke the installer with START_OMS and b_startAgent options, and set them to true or false depending on what you want to control.

For example, if you do not want the Management Agent to start automatically, then run the following command:

```
./runInstaller START_OMS=true b_startAgent=false -silent -responseFile  
<absolute_path>/new_install.rsp
```

To understand the limitations involved with this advanced option, see [Section 3.4.3](#).

3.4.3 Understanding the Limitations

When you use START_OMS and b_startAgent as advanced options to control the way the OMS and the Management Agent start up automatically, sometimes the Management Agent and the host on which it was installed do not appear as targets in the Cloud Control console.

Table 3–2 lists the different combinations of these advanced options, and describes the workaround to be followed for each combination:

Table 3–2 Advanced Options and Workarounds

Advanced Option	Workaround
START_OMS=false b_startAgent=false	<ol style="list-style-type: none"> 1. Start the OMS: \$<OMS_HOME>/bin/emctl start oms 2. Secure the Management Agent: \$<AGENT_HOME>/bin/emctl secure agent 3. Start the Management Agent: \$<AGENT_HOME>/bin/emctl start agent 4. Add the targets: \$<AGENT_HOME>/bin/emctl config agent addinternaltargets 5. Upload the targets: \$<AGENT_HOME>/bin/emctl upload agent
START_OMS=true b_startAgent=false	Start the Management Agent: \$<AGENT_HOME>/bin/emctl start agent
START_OMS=false b_startAgent=true	<ol style="list-style-type: none"> 1. Start the OMS: \$<OMS_HOME>/bin/emctl start oms 2. Secure the Management Agent: \$<AGENT_HOME>/bin/emctl secure agent 3. Add the targets: \$<AGENT_HOME>/bin/emctl config agent addinternaltargets 4. Upload the targets: \$<AGENT_HOME>/bin/emctl upload agent

3.4.4 Editing Response File for Installing Software

Table 3–3 describes what variables you must edit and how you must edit them in the new_install.rsp response file for installing Enterprise Manager Cloud Control in silent mode.

Table 3–3 Editing Response File for Installing Enterprise Manager System

Parameter	Description
UNIX_GROUP_NAME	<i>(Required only when central inventory does not exist)</i> Enter the name of the UNIX group you belong to. For example, "dba" Note: This parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
INVENTORY_LOCATION	<i>(Required only when central inventory does not exist)</i> Enter the absolute path to the Central Inventory. For example, /scratch/oracle/oraInventory Note: This parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.

Table 3–3 (Cont.) Editing Response File for Installing Enterprise Manager System

Parameter	Description
SECURITY_UPDATES_VIA_MYORACLESUPPORT	<ul style="list-style-type: none"> Enter TRUE if you want to download and install security updates. Then, enter the credentials for the following variables: MYORACLESUPPORT_USERNAME MYORACLESUPPORT_PASSWORD Enter FALSE if you do not want to download and install security updates:
DECLINE_SECURITY_UPDATES	<ul style="list-style-type: none"> Enter TRUE if you want to decline the security updates. In this case, you should have entered False for SECURITY_UPDATES_VIA_MYORACLESUPPORT. Enter FALSE if you do not want to decline the security updates. In this case, you should have entered TRUE for SECURITY_UPDATES_VIA_MYORACLESUPPORT.
INSTALL_UPDATES_SELECTION	<p>By default, this variable is set to "skip" indicating that the software updates will not be installed during installation.</p> <ul style="list-style-type: none"> If you want to install the software updates from My Oracle Support, then set this variable to "download". Then, enter the credentials for the following parameters: MYORACLESUPPORT_USERNAME_FOR_SOFTWAREUPDATES MYORACLESUPPORT_PASSWORD_FOR_SOFTWAREUPDATES If you want to install the software updates from a staged location, then set this variable to "staged". Then, for the STAGE_LOCATION parameter, enter the absolute path, which leads to the Updates directory, where the software updates are available.
PROXY_USER	<p>Enter the user name that can be used to access the proxy server.</p> <p>Note: Applies only if you have set the SECURITY_UPDATES_VIA_MYORACLESUPPORT variable to TRUE and/or the INSTALL_UPDATES_SELECTION variable to "download", and only if your connection to the Internet requires you to connect through a proxy.</p>
PROXY_PWD	<p>Enter the password that can be used to access the proxy server.</p> <p>Note: Applies only if you have set the SECURITY_UPDATES_VIA_MYORACLESUPPORT variable to TRUE and/or the INSTALL_UPDATES_SELECTION parameter to "download", and only if your connection to the Internet requires you to connect through a proxy.</p>
PROXY_HOST	<p>Enter the name of the proxy host.</p> <p>Note: Applies only if you have set the SECURITY_UPDATES_VIA_MYORACLESUPPORT variable to TRUE and/or the INSTALL_UPDATES_SELECTION parameter to "download", and only if your connection to the Internet requires you to connect through a proxy.</p>
PROXY_PORT	<p>Enter the port used by the proxy server.</p> <p>Note: Applies only if you have set the SECURITY_UPDATES_VIA_MYORACLESUPPORT variable to TRUE and/or the INSTALL_UPDATES_SELECTION parameter to "download", and only if your connection to the Internet requires you to connect through a proxy.</p>

Table 3–3 (Cont.) Editing Response File for Installing Enterprise Manager System

Parameter	Description
ORACLE_MIDDLEWARE_HOME_LOCATION	<p>Enter the location where you want the installer to install Oracle WebLogic Server 11g Release 1 (10.3.6) and Java Development Kit 1.6.0.43.0.</p> <p>For example, /u01/app/Oracle/Middleware.</p> <p>Ensure that the middleware location has <i>write</i> permission.</p> <p>If you have already installed them manually, then enter the location where you have installed them. Also, make sure you have applied patch 14482558 and patch 13349651 on the Oracle WebLogic Server. For instruction, see the following URL:</p> <p>http://docs.oracle.com/cd/E14759_01/doc.32/e14143/intro.htm#CHDCAJFC</p> <p>For more information about Oracle Middleware home, see Section 2.3.2.</p> <p>Note: Ensure that the number of characters in the middleware home path does not exceed 70 characters for Unix platforms and 25 characters for Microsoft Windows platforms.</p> <p>For example, the middleware home path C:\Oracle\MW\EM containing only 15 characters is acceptable. However, C:\OracleSoftware\OracleMiddleware\OracleEnterpriseManager\OMS\newrelease\oms containing more than 25 characters is not acceptable for Microsoft Windows platforms.</p>
AGENT_BASE_DIR	<p>Enter the absolute path to the agent base directory, a location outside the Oracle Middleware home where the Management Agent can be installed.</p> <p>For example, /oracle/agent.</p> <p>Ensure that this location is empty and has write permission. Also ensure that it is always maintained outside the Oracle Middleware home.</p> <p>Note: (Only for Microsoft Windows) Ensure that the number of characters in the agent base directory path does not exceed 25 characters.</p> <p>For example, the agent base directory path C:\Oracle\Agent\ containing only 16 characters is acceptable. However, C:\Oracle\ManagementAgent\12c\new containing more than 25 characters is not acceptable.</p>
ORACLE_HOSTNAME	<p>Enter a fully qualified domain name that is registered in DNS and is accessible from other network hosts. Oracle recommends that you use a fully qualified domain name.</p> <p>The host name must resolve to the local host because the host name is used for the local Oracle WebLogic Server as well as the Oracle Management Service. Do not provide a remote host or a load balancer virtual host in this field. Do not enter an IP address. Do not use underscores in the name. Short names are allowed, but you will see a warning, so Oracle recommends that you enter a fully qualified domain name instead.</p> <p>If you do not mention the host name, the installation wizard will proceed further, honoring the host name it automatically detects for that host.</p>

Table 3–3 (Cont.) Editing Response File for Installing Enterprise Manager System

Parameter	Description
WLS_ADMIN_SERVER_USERNAME	By default, <code>weblogic</code> is the name assigned to the default user account that is created for the Oracle WebLogic Domain. If you want to accept the default name, then skip this variable. However, if you want to have a custom name, then enter the name of your choice.
WLS_ADMIN_SERVER_PASSWORD	Enter a password for the WebLogic user account. Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.
WLS_ADMIN_SERVER_CONFIRM_PASSWORD	Confirm the password for the WebLogic user account.
NODE_MANAGER_PASSWORD	By default, <code>nodemanager</code> is the name assigned to the default user account that is created for the node manager. Enter a password for this node manager user account. Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.
NODE_MANAGER_CONFIRM_PASSWORD	Confirm the password for the node manager user account.
ORACLE_INSTANCE_HOME_LOCATION	By default, <code>gc_inst</code> is considered as the OMS Instance Base directory for storing all OMS-related configuration files. Enter the absolute path to a location outside the middleware home leading up to the directory name. For more information about this location, see Section 2.3.3 . Note: If you are creating the OMS instance base directory (<code>gc_inst</code>) on an NFS-mounted drive, then after you install, move the lock files from the NFS-mounted drive to a local file system location. Modify the lock file location in the <code>httpd.conf</code> file to map to a location on a local file system. For instructions, refer to Section 3.5 .

Table 3–3 (Cont.) Editing Response File for Installing Enterprise Manager System

Parameter	Description
DATABASE_HOSTNAME	<p>Enter the fully qualified name of the host where the existing database resides. Ensure that the host name does not have underscores.</p> <p>For example, <code>example.com</code></p> <p>If you have already created a database instance with a preconfigured Management Repository using the database templates offered by Oracle, then provide details about that database instance.</p> <p>If you are connecting to an Oracle RAC Database, and if the nodes have virtual host names, then enter the virtual host name of one of its nodes.</p> <p>The connection to the database is established with a connect string that is formed using only this virtual host name, and the installation ends successfully.</p> <p>However, if you want to update the connect string with other nodes of the cluster, then after the installation, run the following command:</p> <pre>\$<OMS_HOME>/bin/emctl config oms -store_repos_details -repos_conn_desc "(DESCRIPTION= (ADDRESS_LIST= (FAILOVER=ON) (ADDRESS= (PROTOCOL=TCP) (HOST=node1-vip.example.com) (PORT=1521)) (ADDRESS= (PROTOCOL=TCP) (HOST=node2-vip.example.com) (PORT=1521))) (CONNECT_DATA= (SERVICE_NAME=EMREP)))" -repos_user sysman</pre> <p>If your Oracle RAC database 11.2 or higher is configured with Single Client Access Name (SCAN) listener, then you can enter a connection string using the SCAN listener.</p> <p>Note: If you connect to a database instance that was created using the database template offered by Oracle, then note that the password assigned to the user accounts SYSMAN_MDS, SYSMAN_APM, and SYSMAN_OPSS, which were created while preconfiguring the Management Repository, are automatically reset with the SYSMAN password you enter for the SYSMAN_PASSWORD parameter.</p>
LISTENER_PORT	<p>Enter the listener port to connect to the existing database.</p> <p>For example, <code>1521</code></p>
SERVICENAME_OR_SID	<p>Enter the service name or the system ID (SID) of the existing database.</p> <p>For example, <code>orcl</code></p>
SYS_PASSWORD	<p>Enter the SYS user account's password.</p>

Table 3–3 (Cont.) Editing Response File for Installing Enterprise Manager System

Parameter	Description
DEPLOYMENT_SIZE	<p>Set one of the following values to indicate the number of targets you plan to monitor, the number of Management Agents you plan to have, and the number of concurrent user sessions you plan to have.</p> <ul style="list-style-type: none"> ■ Small, to monitor up to 999 targets, with up to 99 Management Agents and up to 10 concurrent user sessions ■ Medium, to monitor about 1000 to 9999 targets, with about 100 to 999 Management Agents and about 10 to 24 concurrent user sessions ■ Large, to monitor 10,000 or more targets, with 1000 or more Management Agents, and with about 25 to 50 concurrent user sessions <p>The prerequisite checks are run regardless of the selection you make, but the values to be set for the various parameters checked depend on the selection you make.</p> <p>You can also modify the deployment size after the installation. For more information on deployment sizes, the prerequisite checks that are run, the database parameters that are set, and how you can modify the deployment size after installation, refer to Section 2.1.6.</p> <p>Note:</p> <p>If the database you are connecting to is a database instance created with a preconfigured Management Repository using the database templates offered by Oracle, then make sure the deployment size you set here matches with the deployment size you selected on the Step 2 of 12: Database Templates screen of Oracle Database Configuration Assistant (DBCA) while creating the database instance.</p> <p>If you want to select a deployment size different from the deployment size you had selected while creating the database instance using DBCA, then do one of the following:</p> <ul style="list-style-type: none"> ■ Create another database instance with a template for the desired deployment size, then return to this response file and set the same deployment size to this parameter. For instructions to create a database instance with an Oracle-supplied template, see <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>. ■ In the database instance you have created, fix the parameters to support the deployment size you want to set here in the response file. To automatically fix the database parameters using Oracle-supplied SQL scripts, see <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>.

Table 3–3 (Cont.) Editing Response File for Installing Enterprise Manager System

Parameter	Description
SYSMAN_PASSWORD	<p>Enter a password for creating a SYSMAN user account. This password is used to create the SYSMAN user, which is the primary owner of the Management Repository schema.</p> <p>Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.</p> <p>If you connect to a database instance that was created using the database template offered by Oracle, then note that the password assigned to the user accounts SYSMAN_MDS, SYSMAN_APM, and SYSMAN_OPSS, which were created while preconfiguring the Management Repository, are automatically reset with the SYSMAN password you enter for this parameter.</p>
SYSMAN_CONFIRM_PASSWORD	Confirm the SYSMAN user account's password.
MANAGEMENT_TABLESPACE_LOCATION	<p>Enter the absolute path to the location where the data file (mgmt.dbf) for management tablespace can be stored. Ensure that the specified path leads up to the file name.</p> <p>For example:</p> <ul style="list-style-type: none"> ■ If the database is on a file system, then the path must look like <code>/u01/oracle/prod/oradata/mgmt.dbf</code> ■ If the database is on Automatic Storage Management (ASM), then the path must look like <code>+<disk_group1>/prod/oradata/mgmt.dbf</code>, where <code>disk_group1</code> is a diskgroup created on ASM and <code>prod</code> is the Service ID (SID). ■ If the database is on a raw device, then the path must look like <code></dev/raw1>/prod/oradata/mgmt.dbf</code>, where <code>/dev/raw1</code> is the raw device and <code>prod</code> is the SID. <p>Enterprise Manager Cloud Control requires this data file to store information about the monitored targets, their metrics, and so on. Essentially, everything else other than configuration data, software library data, and audit data.</p>
CONFIGURATION_DATA_TABLESPACE_LOCATION	<p>Enter the absolute path to the location where the data file (mgmt_ecm_depot1.dbf) for configuration data tablespace can be stored. Ensure that the specified path leads up to the file name.</p> <p>For example, <code>/home/john/oradata/mgmt_ecm_depot1.dbf</code></p> <p>Enterprise Manager Cloud Control requires this data file to store configuration information collected from the monitored targets.</p>
JVM_DIAGNOSTICS_TABLESPACE_LOCATION	<p>Enter the absolute path to a location where the data file (mgmt_deepdive.dbf) for JVM Diagnostics data tablespace can be stored. Ensure that the specified path leads up to the file name.</p> <p>For example, <code>/home/john/oradata/mgmt_deepdive.dbf</code></p> <p>Enterprise Manager Cloud Control requires this data file to store monitoring data related to JVM Diagnostics and Application Dependency Performance (ADP).</p>

Table 3–3 (Cont.) Editing Response File for Installing Enterprise Manager System

Parameter	Description
AGENT_REGISTRATION_PASSWORD	Enter a password to secure the communication between the OMS and the Management Agents. Note that you have to provide the same registration password for securing your Management Agents.
AGENT_REGISTRATION_CONFIRM_PASSWORD	Confirm the agent registration password.
CONFIGURE_ORACLE_SOFTWARE_LIBRARY	<p>If you want to configure the Software Library at the time of installation, set this parameter to <code>TRUE</code>. Otherwise, set it to <code>FALSE</code>.</p> <p>Even if you do not configure it at the time of installation, your installation will succeed, and you can always configure it later from the Enterprise Manager Cloud Control Console. However, Oracle recommends that you configure it at the time of installation so that it is automatically configured by the installer, thus saving your time and effort.</p>
SOFTWARE_LIBRARY_LOCATION	<p>If you have set <code>CONFIGURE_ORACLE_SOFTWARE_LIBRARY</code> to <code>TRUE</code>, then enter the absolute path leading up to a unique directory name on the OMS host where the Software Library can be configured. Ensure that the location you enter is a mounted location on the OMS host, and is placed outside the Middleware Home. Also ensure that the OMS process owner has read/write access to that location. Configuring on a mounted location helps when you install additional OMS instances as they will require read/write access to the same <i>OMS Shared File System</i> storage location.</p>
STATIC_PORTS_FILE	<p>By default, ports described in Section 2.1.9 are honored. If you want to accept the default ports, then leave this field blank.</p> <p>If you want to use custom ports, then enter the absolute path to the <code>staticports.ini</code> file that lists the custom ports to be used for the installation.</p>

Table 3–3 (Cont.) Editing Response File for Installing Enterprise Manager System

Parameter	Description
PLUGIN_SELECTION	<p>By default, mandatory plug-ins such as Oracle Database Management Plug-In, Oracle Fusion Middleware Management Plug-In, Oracle My Oracle Support Management Plug-In, and Oracle Exadata Management Plug-In get automatically installed with the Enterprise Manager system.</p> <p>However, if you want to install any of the other optional plug-ins that are available in the software kit (DVD or downloaded software), then enter the names of those plug-ins for this variable.</p> <p>For example,</p> <pre> PLUGIN_ SELECTION={ "oracle.sysman.empa" , "oracle.sysman.vt" } </pre> <p>If you want to install any plug-in that is not available in the software kit, then do the following:</p> <ol style="list-style-type: none"> 1. Manually download the plug-ins from the Enterprise Manager download page on OTN, and store them in an accessible location: http://www.oracle.com/technetwork/oem/grid-control/downloads/oem-upgrade-console-502238.html 2. Update this variable (PLUGIN_SELECTION) to the names of those plug-ins you downloaded. 3. Invoke the installer with the following option, and pass the location where you downloaded the plug-ins: <pre>./runInstaller -pluginLocation <absolute_path_to_plugin_software_location></pre>

3.5 After You Install

Perform the post-install steps as described in the chapter on installing Enterprise Manager system that is available in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

Installing Enterprise Manager Software Now and Configuring Later

This chapter explains how you can install only the software binaries of Enterprise Manager Cloud Control at one point, and configure the installation at a later point. In particular, this chapter covers the following:

- [Overview](#)
- [Before You Begin](#)
- [Prerequisites](#)
- [Installation Procedure](#)

Note: All general purpose file systems, including OCFS2 and ACFS, are acceptable for storing Enterprise Manager Cloud Control 12c software binaries and OMS instance home files (configuration files in `gc_inst`). However, OCFS is not considered a general purpose file system, and therefore is not considered acceptable for this use.

4.1 Overview

You can choose to install only the software binaries of Enterprise Manager Cloud Control at one point and configure it at a later point in time to work with an existing, certified Oracle Database. This approach enables you to divide the installation process into two phases, mainly the installation phase and the configuration phase.

Understandably, the installation phase takes less time compared to the configuration phase because the installation phase involves only copying of binaries. This approach helps you plan your installation according to the time and priorities you have.

During the installation phase, you invoke the installer to create Oracle homes and install the following components in the Middleware home:

- Java Development Kit (JDK) 1.6.0.43.0
- Oracle WebLogic Server 11g Release 1 (10.3.6)
- Oracle Management Service 12c
- Oracle Management Agent 12c
- Oracle JRF 11g Release (11.1.1.6.0), which includes `oracle_common` directory
- Oracle Web Tier 11g Release (11.1.1.6.0), which includes `Oracle_WT` directory

Note:

- Java Development Kit (JDK) 1.6.0.43.0 and Oracle WebLogic Server 11g Release 1 (10.3.6) are installed only if you do not specify the use of existing installations. Oracle strongly recommends using the 12c installation process to install the JDK and Oracle WebLogic Server for use with Enterprise Manager 12c.
 - If you want to manually install Oracle WebLogic Server 11g Release 1 (10.3.6), then follow the guidelines outlined in [Section 4.2](#).
-

During the configuration phase, you invoke a configuration script to do the following:

- Create an Oracle WebLogic domain called `GCDomain`. For this WebLogic Domain, a default user account, `weblogic`, is used as the administrative user. You can choose to change this, if you want, in the installer.
- Create a Node Manager user account called `nodemanager`. A Node Manager enables you to start, shut down, or restart an Oracle WebLogic Server instance remotely, and is recommended for applications with high availability requirements.
- Configure an Oracle Management Service Instance Base location (`gc_inst`) outside the Middleware home, for storing all configuration details related to Oracle Management Service 12c.

For example, if the Middleware home is `/u01/app/Oracle/Middleware/`, then the instance base location is `/u01/app/Oracle/gc_inst`.

- Configures Oracle Management Repository in the existing, certified Oracle Database.
- Deploys and configures the following plug-ins:
 - Oracle Database Management Plug-In
 - Oracle Fusion Middleware Management Plug-In
 - Oracle My Oracle Support Management Plug-In
 - Oracle Exadata Management Plug-In

Note: In addition to the mandatory plug-ins listed above, you can optionally install other plug-ins available in the software kit. The installer offers a screen where you can select the optional plug-ins and install them. However, if you want to install some plug-ins that are not available in the software kit, then refer to the point about installing additional plug-ins in [Section 4.4.1.3.1](#).

- Runs the following configuration assistants to configure the installed or upgraded components:
 - Plugins Prerequisite Check
 - Repository Configuration

Note: If you use a database instance that was created with a preconfigured Management Repository using the database templates offered by Oracle, then *Repository Out-of-Box Configuration Assistant* is run instead of *Repository Configuration Assistant*.

- MDS Schema Configuration
- OMS Configuration
- Plugins Deployment and Configuration
- Start Oracle Management Service
- Oracle Configuration Manager Repeater Configuration
- Agent Configuration Assistant

4.2 Before You Begin

Before you begin, keep these points in mind:

- You must ensure that you have the latest Enterprise Manager Cloud Control software.

To download the latest software, access the following URL:

<http://www.oracle.com/technetwork/oem/enterprise-manager/downloads/index.html>

For information about downloading the latest software, refer to [Section 1.2.2](#).

- Ensure that there are no white spaces in the name of the directory where you download and run the Enterprise Manager Cloud Control software from. For example, do not download and run the software from a directory titled `EM Software` because there is a white space between the two words of the directory name.
- You can install Enterprise Manager Cloud Control using the installation wizard only on a single host, that is, locally on the server where the wizard is invoked. You cannot install on remote hosts.
- To invoke the installation wizard on UNIX platforms, run `runInstaller`. To invoke on Microsoft Windows platforms, run `setup.exe`.
- Oracle Management Service 12c can communicate only with the following versions of Oracle Management Agent 12c:

Table 4–1 OMS and Management Agent Compatibility for 12c Release

	Oracle Management Agent 12c Release 3 (12.1.0.3)	Oracle Management Agent 12c Release 2 (12.1.0.2)	Oracle Management Agent 12c Release 1 (12.1.0.1) + Bundle Patch 1 <i>(Refers to agents and their plug-ins patched or upgraded to, or installed with Bundle Patch 1)</i>

Table 4–1 (Cont.) OMS and Management Agent Compatibility for 12c Release

Oracle Management Service 12c Release 3 (12.1.0.3)	Yes	Yes	Yes
Oracle Management Service 12c Release 2 (12.1.0.2)	No	Yes	Yes
Oracle Management Service 12c Release 1 (12.1.0.1)	No	No	Yes

- You must not set the ORACLE_HOME and ORACLE_SID environment variables. You must ensure that the Oracle directories do NOT appear in the PATH.
- Do not install on a symlink. Installing in such a location may impact life cycle operations such as patching and scaling out.
- The Enterprise Manager Cloud Control Installation Wizard installs Java Development Kit (JDK) 1.6.0.43.0 and Oracle WebLogic Server 11g Release 1 (10.3.6), but only if you do not specify the use of existing installations. Oracle strongly recommends using the 12c installation process to install the JDK and Oracle WebLogic Server for use with Enterprise Manager 12c.
- *(Only for Graphical Mode)* You must set the DISPLAY environment variable.
 - In bash terminal, run the following command:

```
export DISPLAY=<hostname>:<vnc port>.0
```

 For example, `export DISPLAY=example.com:1.0`
 - In other terminals, run the following command:

```
setenv DISPLAY <hostname>:1.0
```

 For example, `setenv DISPLAY example.com:1.0`
- If Oracle WebLogic Server 11g Release 1 (10.3.6) does not exist and if you choose to manually install it, then ensure that you install it using JDK 1.6.0.43.0 (64-bit version for 64-bit platforms and 32-bit version for 32-bit platforms).
 - Download JDK 1.6.0.43.0 for your platform from the platform vendor's Web site.
 For example, download SUN JDK 1.6.0.43.0 for Linux platforms from the following Oracle Web site URL:
<http://www.oracle.com/technetwork/java/javase/downloads/index.html>
 - If you already have JDK, then verify its version by navigating to the <JDK_Location>/bin directory and running the following command:

```
"./java -fullversion"
```

 To verify whether it is a 32-bit or a 64-bit JDK, run the following command:

```
"file *"
```
 - JROCKIT is not supported.
 - If you want to manually install Oracle WebLogic Server 11g Release 1 (10.3.6) on Linux 64-bit platforms, first install the 64-bit JDK for your platform, and

then download and use the `wls1036_generic.jar` file to install Oracle WebLogic Server.

For example,

```
<JDK home>/bin/java -d64 -jar <absolute_path_to_wls1036_generic.jar>
```

- If you want to manually install Oracle WebLogic Server 11g Release 1 (10.3.6) on Linux 32-bit platforms, then download and use either the `wls1036_linux32.bin` file or the `wls1036_generic.jar` file.

For example,

```
<JDK home>/bin/java -jar <absolute_path_to_wls1036_generic.jar>
```

- You must follow the instructions outlined in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server* to install Oracle WebLogic Server. The guide is available in the Fusion Middleware documentation library available at:

<http://www.oracle.com/technetwork/middleware/weblogic/documentation/index.html>

- You must ensure that the Oracle WebLogic Server installation is a typical installation, and even if you choose to perform a custom installation, ensure that components chosen for custom installation are the same as the ones associated with a typical installation.
- You must ensure that the user installing the WebLogic Server is the same as the one installing Enterprise Manager Cloud Control.
- After installing Oracle WebLogic Server, make sure you apply patch 14482558 and patch 13349651 on it. For instructions, see the following URL:

http://docs.oracle.com/cd/E14759_01/doc.32/e14143/intro.htm#CHDCAJFC

For more information on Oracle WebLogic Server downloads and demos, access the following URL:

<http://www.oracle.com/technology/products/weblogic/index.html>

- You must ensure that the Oracle WebLogic Server 11g Release 1 (10.3.6) installed by the Enterprise Manager Cloud Control Installation Wizard or by you is dedicated for Enterprise Manager Cloud Control. You must not have any other Oracle Fusion Middleware product installed in that Middleware home.

Enterprise Manager Cloud Control cannot coexist with any Oracle Fusion Middleware product in the same Middleware home because the `ORACLE_COMMON` property is used by both the products.

- You can optionally use the database templates offered by Oracle to create a database instance with a preconfigured Management Repository. To do so, refer to *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

However, note that the database templates are essentially designed for simple installation, although they can be used for advanced installation. Therefore, while performing an advanced installation (possibly with small, medium, or large deployment size selection), when you provide the details of such a database, you will be prompted that the database parameters need to be modified to suit the deployment size you selected. You can confirm the message to proceed further. The installation wizard will automatically set the database parameters to the required values.

- Enterprise Manager is not affected when you enable or disable features such as XML DB on the Oracle Database in which you plan to configure the Management Repository. Therefore, you can enable or disable any feature in the database because Enterprise Manager does not rely on them.
- If you want to optionally follow the configuration guidelines for deploying the Management Repository so that your management data is secure, reliable, and always available, refer to the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.
- *(Only for Silent Mode)* By default, the software updates cannot be applied during installation because the `INSTALL_UPDATES_SELECTION` variable in the response file is set to "skip". However, if you want to apply them during installation, then you can modify this variable as described in [Section 4.4.2.1.1](#).
- If you are creating the OMS instance base directory (`gc_inst`) on an NFS-mounted drive, then after you install, move the lock files from the NFS-mounted drive to a local file system location. Modify the lock file location in the `httpd.conf` file to map to a location on a local file system. For instructions, refer to [Section 4.4.1.4](#) or [Section 4.4.2.4](#) depending on the approach you adopt.
- By default, the upload ports and console ports as described in [Section 2.1.9](#) are used.
- Oracle offers bug fixes for a product based on the *Oracle Lifetime Support Policy*. When the license period expires for a particular product, the support for bug fixes offered by Oracle also ends. For more information, see the *Oracle Lifetime Support Policy* available at:

<http://www.oracle.com/support/library/brochure/lifetime-support-technology.pdf>

When determining supportability and certification combinations for an Enterprise Manager Cloud Control installation, you must consider Enterprise Manager Cloud Control's framework components as well as the targets monitored by Enterprise Manager Cloud Control. Oracle recommends keeping your Cloud Control components and targets updated to the latest certified versions in order to receive code fixes without having to purchase an Extended Support license.

- You can find the OMS and Management Agent entries in the `/etc/oragchomelist` file for all UNIX platforms except HPUNIX, HPia64, Solaris Sparc.
On HPUNIX, HPia64, Solaris Sparc platforms, the entries are present in `/var/opt/oracle/oragchomelist`.
- As a prerequisite, you must have an existing Oracle Database to configure the Management Repository. This database can also have the Automatic Memory Management (AMM) feature enabled.
- The locale-specific data is stored in the `<OMS_Oracle_Home>/nls/data` directory. Oracle strongly recommends that you either set the environment variable `ORA_NLS10` to `<OMS_Oracle_Home>/nls/data` or do not set at all.
- If you install the OMS and the Oracle Database, which houses the Management Repository, on the same host, then when you reboot the host, the OMS and the Management Agent installed with it will not automatically start up. You will have to manually start them.

4.3 Prerequisites

Meet the prerequisites described in the chapter on installing Enterprise Manager system that is available in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

4.4 Installation Procedure

This section describes the following:

- [Installing in Graphical Mode](#)
- [Installing in Silent Mode](#)

4.4.1 Installing in Graphical Mode

This section explains how you can install only the software binaries of Enterprise Manager Cloud Control at one point in graphical mode, and configure the installation at a later point. In particular, this section covers the following:

- [Installing Software](#)
- [Running Root Script](#)
- [Configure Software](#)
- [Performing Post-Configuration Tasks](#)

4.4.1.1 Installing Software

To install only the software binaries of Enterprise Manager Cloud Control in graphical mode, follow these steps:

Note: Oracle recommends you to run the EM Prerequisite Kit before invoking the installer to ensure that you meet all the repository requirements beforehand. Even if you do not run it manually, the installer anyway runs it in the background while installing the product. However, running it manually beforehand sets up your Management Repository even before you can start the installation or upgrade process. For information on the kit, to understand how to run it, and to know about the prerequisite checks it runs, see *Oracle Enterprise Manager Basic Installation Guide*.

1. Invoke the Enterprise Manager Cloud Control Installation Wizard

Invoke the installer. (On Unix, make sure you invoke the installer as a user who belongs to the `oinstall` group you created. For information about creating operating system groups and users, see the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.)

```
<Software_Location>/runInstaller [-invPtrLoc <absolute_path_to_oraInst.loc>]
```

Note:

- In this command, <Software_Location> refers to either the DVD or the location where you have downloaded software kit.
- To invoke the installation wizard on UNIX platforms, run `runInstaller`. To invoke on Microsoft Windows platforms, run `setup.exe`.
- The `-invPtrLoc` parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
- For information about the additional, advanced options you can pass while invoking the installer, refer to [Section 4.4.1.1.1](#).

Note: When you invoke `runInstaller` or `setup.exe`, if the Enterprise Manager Cloud Control Installation Wizard does not appear, then it is possible that you do not have read and write access to `/stage`, which is a subdirectory in the `Disk1` directory of the Enterprise Manager software.

There is a classpath variable that the installation wizard computes for `OPatch` as `../stage/Components/`, and when the `TEMP` variable is set to `/tmp`, the installation wizard tries to look for the `opatch` JAR file in the `/tmp/ ../stage` directory, which is equivalent to `/stage`.

However, if you do not have read and write permission on `/stage`, then the installation wizard can hang. Under such circumstances, verify if you have read and write access to the `/stage` directory. If you do not have, then set the `TEMP` variable to a location where the install user has access to, and then relaunch the installation wizard.

2. (Optional) Enter My Oracle Support Details

On the My Oracle Support Details screen, enter your *My Oracle Support* credentials to enable Oracle Configuration Manager. If you do not want to enable Oracle Configuration Manager now, go to Step (3).

If the host from where you are running the installation wizard does not have a connection to the Internet, then enter only the e-mail address and leave the other fields blank. After you complete the installation, manually collect the configuration information and upload it to *My Oracle Support*.

Note: For information about manually collecting the configuration information and uploading it to *My Oracle Support*, see [Section 2.1.4.1](#).

Note: Beginning with Enterprise Manager Cloud Control 12c Release 3 (12.1.0.3), My Oracle Support accesses support.oracle.com directly. This means that you must provide network access to this URL, or grant proxy access to it from any client that will access My Oracle Support.

3. Click **Next**.
4. **(Recommended) Install Software Updates**

On the Software Updates screen, select either **Search for Updates** or **My Oracle Support**, and apply the latest software updates.

You can download the software updates in offline mode (if you do not have Internet connectivity) or online mode (if you have Internet connectivity). For more information on these options, and for instructions to download and apply the software updates using these options, see [Section 2.1.5.5](#).

Note: The Software Updates screen uses the built-in feature *Software Update* to automatically download and deploy the latest recommended patches while installing or upgrading Enterprise Manager Cloud Control. This way, you do not have to keep a manual check on the patches released by Oracle. All patches required by the installer for successful installation and upgrade are automatically detected and downloaded from My Oracle Support, and applied during the installation or upgrade, thus reducing the known issues and potential failures. Oracle strongly recommends using this feature, and applying the software updates while the installation is in progress. For more information, see [Section 2.1.5.1](#).

5. Click Next.

If Enterprise Manager Cloud Control is the first Oracle product you are installing on the host that is running on UNIX operating system, then the Oracle Inventory screen appears. For details, see step (6). Otherwise, the Check Prerequisites screen appears. For details, see step (8).

If Enterprise Manager Cloud Control is the first Oracle product you are installing on the host that is running on Microsoft Windows operating system, then the Oracle Inventory screen does not appear. On Microsoft Windows, the following is the default inventory directory:

```
<system drive>\Program Files\Oracle\Inventory
```

6. Enter Oracle Inventory Details

On the Oracle Inventory screen, do the following. You will see this screen only if this turns out to be your first ever installation of an Oracle product on the host.

- a. Enter the full path to a directory where the inventory files and directories can be placed.

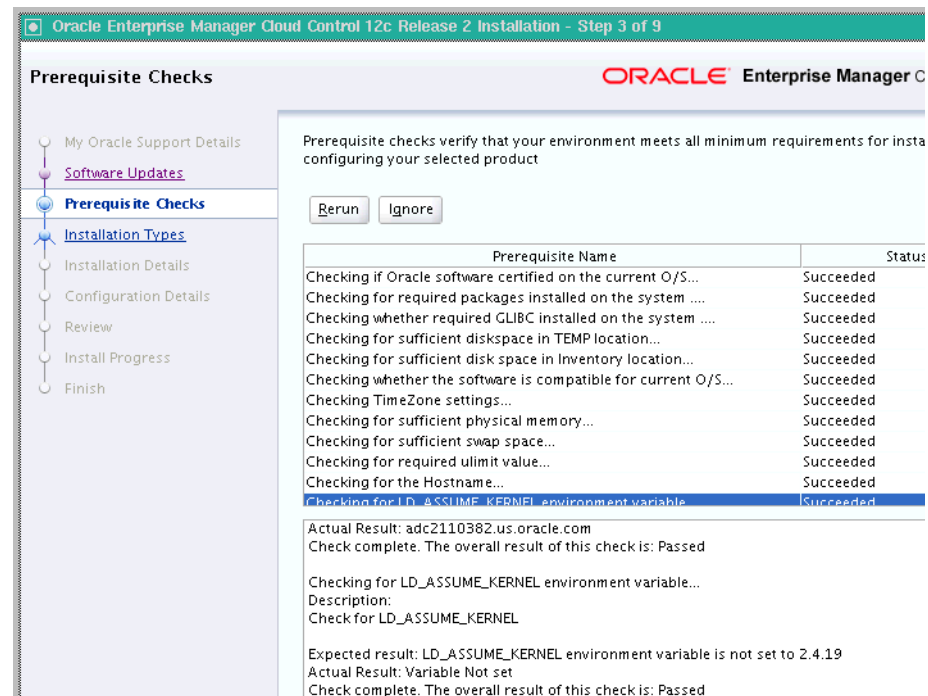
Note:

If this is the first Oracle product on the host, then the default central inventory location is `/home/<user_name>/oraInventory`. However, if you already have some Oracle products on the host, then the central inventory location can be found in the `oraInst.loc` file. The `oraInst.loc` file is located in the `/etc` directory for Linux and AIX, and in the `/var/opt/oracle` directory for Solaris, HP-UX, and Tru64.

- b. Select the appropriate operating system group name that will own the Oracle inventory directories. The group that you select must have *write* permissions on the Oracle Inventory directories.

7. Click Next.

8. Check Prerequisites



On the Prerequisite Checks screen, check the status of the prerequisite checks run by the installation wizard, and verify whether your environment meets all the minimum requirements for a successful installation.

The installation wizard runs the prerequisite checks automatically when you come to this screen. It checks for the required operating system patches, operating system packages, and so on.

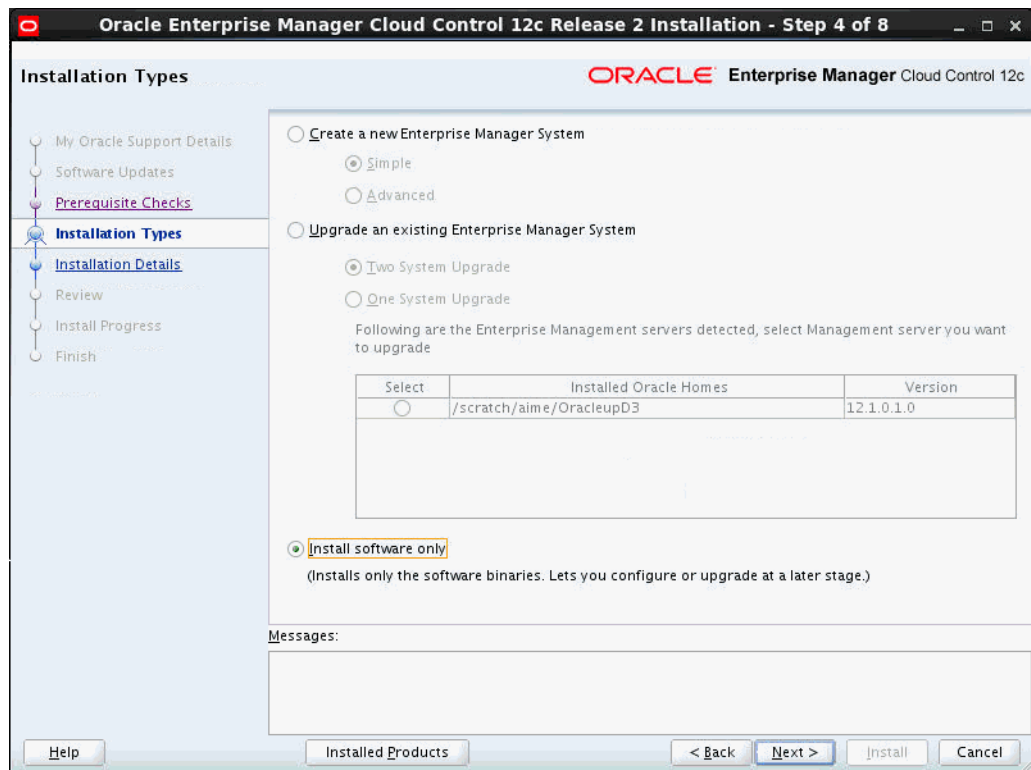
The status of the prerequisite check can be either **Warning**, **Failed**, or **Succeeded**.

- If some checks result in **Warning** or **Failed** status, then investigate and correct the problems before you proceed with the installation. The screen provides details on why the prerequisites failed and how you can resolve them. After you correct the problems, return to this screen and click **Rerun** to check the prerequisites again.
- However, all package requirements must be met or fixed before proceeding any further. Otherwise, the installation might fail.

9. Click Next.

Note: If a prerequisite check fails reporting a missing package, then make sure you install the required package, and click **Rerun**. The installation wizard validates the package name as well as the version, so make sure you install the packages of the minimum versions mentioned in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. To understand the logic the installation wizard uses to verify these packages, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

10. Select Installation Type



On the Installation Types screen, select **Install software only**.

11. Click **Next**.

12. **Enter Installation Details**

On the Installation Details screen, do the following:

- a. Enter or validate or enter the Middleware home where you want to install the OMS and other core components.

Note:

- If Oracle WebLogic Server 11g Release 1 (10.3.6) and Java Development Kit 1.6.0.43.0 are already installed in your environment, then the installer automatically detects them and displays the absolute path to the Middleware home where they are installed. In this case, validate the Middleware home location that is detected and displayed by default. If the location is incorrect, then enter the path to the correct location. Ensure that the Middleware home location you select or enter is a Middleware home location that does not have any Oracle homes.

Also make sure you have applied patch 14482558 and patch 13349651 on the Oracle WebLogic Server. For instructions, see the following URL:

http://docs.oracle.com/cd/E14759_01/doc.32/e14143/intro.htm#CHDCAJFC

For more information on Oracle WebLogic Server downloads and demos, access the following URL:

<http://www.oracle.com/technology/products/weblogic/index.html>

- If Oracle WebLogic Server 11g Release 1 (10.3.6) and Java Development Kit 1.6.0.43.0 are NOT already installed in your environment, then the installer automatically installs them for you while installing the Enterprise Manager system. In this case, enter the absolute path to a directory where you want to have them installed. For example, /oracle/software/. Ensure that the directory you enter does not contain any files or subdirectories.
- Ensure that the number of characters in the middleware home path does not exceed 70 characters for Unix platforms and 25 characters for Microsoft Windows platforms.

For example, the middleware home path C:\Oracle\MW\EM containing only 15 characters is acceptable. However, C:\OracleSoftware\OracleMiddleware\OracleEnterpriseManager\OMS\newrelease\oms containing more than 25 characters is not acceptable for Microsoft Windows platforms.

- b. Enter the absolute path to the agent base directory, a location outside the Oracle Middleware home where the Management Agent can be installed. For example, if the middleware home is /u01/app/Oracle/Middleware/, then you can specify the agent base directory as /u01/app/Oracle/agent12c.

Ensure that this location is empty and has write permission. Also ensure that it is always maintained outside the middleware home.

Note: Ensure that the number of characters in the middleware home path does not exceed 70 characters for Unix platforms and 25 characters for Microsoft Windows platforms.

For example, the middleware home path `C:\Oracle\MW\EM` containing only 15 characters is acceptable. However, `C:\OracleSoftware\OracleMiddleware\OracleEnterpriseManager\OMS\newrelease\oms` containing more than 25 characters is not acceptable for Microsoft Windows platforms.

- c. Validate the name of the host where you want to configure the OMS.

The host name appears as a fully qualified name, or as a virtual host name if your host is configured with virtual machine. If the installation wizard was invoked with a value for `ORACLE_HOSTNAME`, then this field is prepopulated with that name.

Accept the default host name, or enter a fully qualified domain name that is registered in DNS and is accessible from other network hosts. Oracle recommends that you use a fully qualified domain name.

Note: The host name must resolve to the local host because the host name is used for the local Oracle WebLogic Server as well as the Oracle Management Service. Do not provide a remote host or a load balancer virtual host in this field. Do not enter an IP address. Do not use underscores in the name. Short names are allowed, but you will see a warning, so Oracle recommends that you enter a fully qualified domain name instead.

13. Click Next.

14. Review and Install

On the Review screen, review the details you provided for the selected installation type.

- If you want to change the details, click **Back** repeatedly until you reach the screen where you want to make the changes.
- After you verify the details, if you are satisfied, click **Install** to begin the installation process.

15. Track the Progress

On the Install Progress screen, view the overall progress (in percentage) of the installation.

16. End the Installation

On the Finish screen, you should see information pertaining to the installation of Enterprise Manager. Review the information and click **Close** to exit the installation wizard.

4.4.1.1.1 Using Advanced Installer Options The following are some additional, advanced options you can pass while invoking the installer:

- By default, GCDomain is the default name used for creating the WebLogic Domain. To override this and use a custom WebLogic Domain name, invoke the installation wizard with the `WLS_DOMAIN_NAME` option, and enter a unique custom name.

Note: Ensure that the `WLS_DOMAIN_NAME` option is used even when the `ConfigureGC.sh` is invoked to configure the software binaries as described in [Section 4.4.1.3](#).

For example, if you want to use the custom name `EMDomain`, then run the following command:

```
$<MIDDLEWARE_HOME>/oms/sysman/install/ConfigureGC.sh WLS_DOMAIN_NAME=EMDomain
```

- If you want to set the Central Inventory, then pass the `-invPtrLoc` parameter. This parameter considers the path to a location where the inventory pointer file (`oraInst.loc`) is available. However, this parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.

For example,

```
./runInstaller -invPtrLoc /scratch/OracleHomes/oraInst.loc -silent -responseFile <absolute_path_response_file>
```

- After you install the software binaries, you will configure the binaries. And after the configuration ends successfully, by default, the OMS and the Management Agent start automatically. If you do not want them to start automatically, then invoke the installation wizard with `START_OMS` and `b_startAgent` options, and set them to true or false depending on what you want to control.

Note: Ensure that the `START_OMS` and `b_startAgent` options are used even when the `ConfigureGC.sh` is invoked to configure the software binaries as described in [Section 4.4.1.3](#).

For example, if you do not want the Management Agent to start automatically, then run the following command:

```
$<MIDDLEWARE_HOME>/oms/sysman/install/ConfigureGC.sh START_OMS=true b_startAgent=false
```

To understand the limitations involved with this advanced option, see [Section 3.4.3](#).

4.4.1.2 Running Root Script

(For UNIX Only) After you install the software binaries of Enterprise Manager Cloud Control, log in as a `root` user in a new terminal and run the following scripts:

- If this is the first Oracle product you just installed on the host, then run the `oraInstroot.sh` script from the inventory location specified in the `oraInst.loc` file that is available in the Management Agent home.

For example, if the inventory location specified in the `oraInst.loc` file is `$HOME/oraInventory`, then run the following command:

```
$HOME/oraInventory/oraInstRoot.sh
```

Note: If you are not a *root* user, then use SUDO to change to a *root* user. For example, run the following command:

```
/usr/local/bin/sudo $HOME/oraInventory/oraInstRoot.sh
```

- Run the `allroot.sh` script from the OMS home:

```
$<OMS_HOME>/allroot.sh
```

Note: If you are not a *root* user, then use SUDO to change to a *root* user. For example, run the following command:

```
/usr/local/bin/sudo $<OMS_HOME>/allroot.sh
```

4.4.1.3 Configure Software

To configure Enterprise Manager Cloud Control, follow these steps:

1. Invoke the Enterprise Manager Cloud Control Installation Wizard

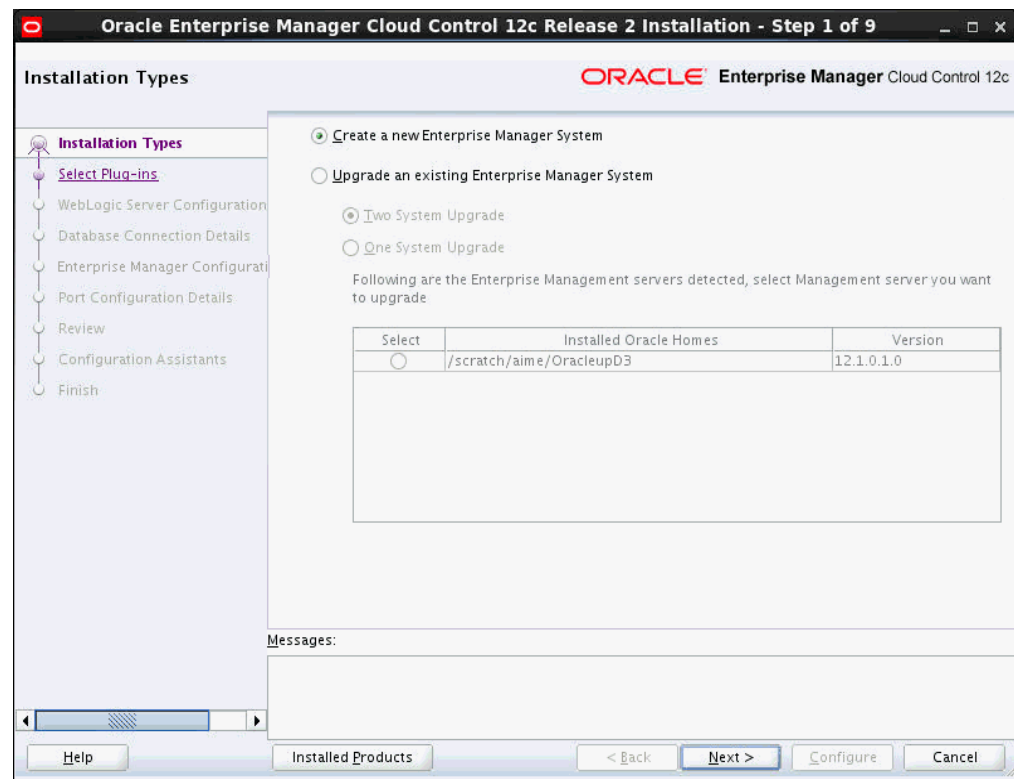
Invoke the installation wizard. (On Unix, make sure you invoke the installation wizard as a user who belongs to the `oinstall` group you created. For information about creating operating system groups and users, see the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.)

```
$<MIDDLEWARE_HOME>/oms/sysman/install/ConfigureGC.sh [-invPtrLoc  
<absolute_path_to_orainst.loc>]
```

Note:

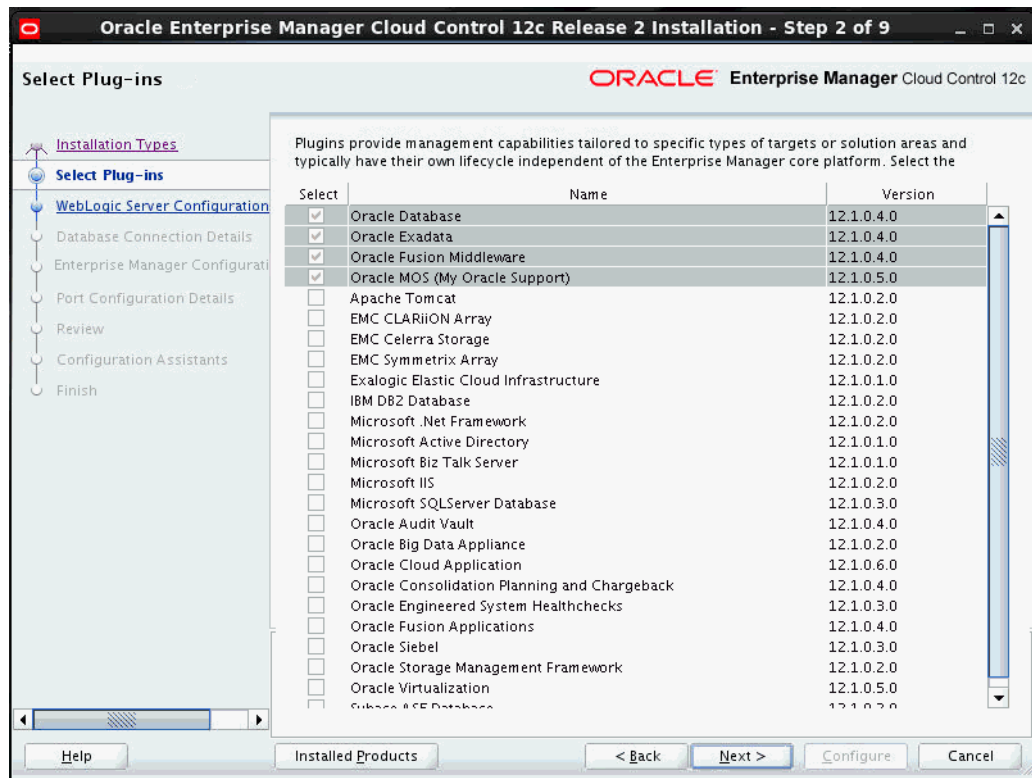
- While installing the software binaries as described in [Section 4.4.1.1](#), if you had passed the argument `-invPtrLoc`, then pass the same argument here as well.
 - The `-invPtrLoc` parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
 - For information about the additional, advanced options you can pass while invoking the script, refer to [Section 4.4.1.3.1](#).
 - The only way to configure a software-only installation is to run the `ConfigureGC.sh` (or `ConfigureGC.bat` on Microsoft Windows) script. DO NOT run the individual configuration assistants to configure a software-only installation. If you want to run the individual configuration assistants to configure the installation for some reason, then contact Oracle Support.
 - If you have already configured a software-only installation (the Oracle home) using the `ConfigureGC.sh` script (or `ConfigureGC.bat` on Microsoft Windows), then DO NOT try to reconfigure it—either using the script or using the individual configuration assistants.
-

2. Select Installation Type



In the installation wizard, on the Installation Types screen, select **Create a New Enterprise Manager System**.

3. Click **Next**.
4. **Deploy Plug-Ins**



On the Plug-In Deployment screen, select the optional plug-ins you want to install from the software kit (DVD, downloaded software) while installing the Enterprise Manager system.

The pre-selected rows are mandatory plug-ins that will be installed by default. Select the optional ones you want to install.

Note: During installation, if you want to install a plug-in that is not available in the software kit, then refer to the point about installing additional plug-ins in [Section 4.4.1.1.1](#).

5. Click **Next**.
6. Enter **WebLogic Server Configuration Details**

On the WebLogic Server Configuration Details screen, enter the credentials for the WebLogic Server user account and the Node Manager user account, and validate the path to the Oracle Management Service instance base location. Ensure that the Oracle Management Service instance base location is outside the middleware home

Note: Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.

Note: Ensure that the Oracle Management Service instance base location is outside the middleware home.

By default, the WebLogic Domain name is GCDomain, and the Node Manager name is nodemanager. These are non-editable fields. The installer uses this information for creating Oracle WebLogic Domain and other associated components such as the admin server, the managed server, and the node manager.

A Node Manager enables you to start, shut down, or restart an Oracle WebLogic Server instance remotely, and is recommended for applications with high availability requirements.

By default, the Oracle Management Service instance base location is gc_inst, which is created outside the Middleware home for storing all configuration details related to the OMS.

7. Click Next.

8. Enter Database Connection Details

The screenshot shows the 'Database Connection Details' window in the Oracle Enterprise Manager Cloud Control 12c Release 2 installer. The window title is 'Oracle Enterprise Manager Cloud Control 12c Release 2 Installation - Step 4 of 9'. The left sidebar contains a navigation tree with the following items: 'Installation Types', 'Select Plug-ins', 'WebLogic Server Configuration', 'Database Connection Details' (highlighted), 'Enterprise Manager Configuration', 'Port Configuration Details', 'Review', 'Configuration Assistants', and 'Finish'. The main area contains the following fields:

- Database Host Name:
- Port:
- Service/SID:
- SYS Password:
- Deployment Size:

At the bottom of the main area is a 'Messages:' label and a text area. The bottom of the window has a navigation bar with the following buttons: 'Help', 'Installed Products', '< Back', 'Next >', 'Configure', and 'Cancel'.

On the Database Connection Details screen, do the following:

- a. Provide details of the existing, certified database where the Management Repository needs to be created. If you have already created a database instance with a preconfigured Management Repository using the database templates offered by Oracle, then provide details about that database instance.

The installer uses this information to connect to the existing database for creating the SYSMAN schema and plug-in schemas. If you provide details of a database that already has a preconfigured Management Repository, then the installer only creates plug-in schemas.

Note:

- For information about creating a database instance with a preconfigured Management Repository using the database templates offered by Oracle, refer to *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
- If you connect to a database instance that was created using the database template offered by Oracle, then note that the password assigned to the user accounts SYSMAN_MDS, SYSMAN_APM, and SYSMAN_OPSS, which were created while preconfiguring the Management Repository, are automatically reset with the SYSMAN password you enter on the Repository Configuration Details screen (as described in Step (10)).
- To identify whether your database is a certified database listed in the certification matrix, access the certification matrix as described in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
- If you see a warning stating that the database you have provided already has Enterprise Manager schemas configured, then make sure you drop those schemas first, then deinstall the Enterprise Manager software that had created those schemas, and then return to the installer to proceed with the new installation. For instructions to drop the schemas and deinstall the software, see [Chapter 17](#).
- For information on all the database initialization parameters that are set, and all the prerequisite checks that are run, and for instructions to run the prerequisite checks manually if they fail, the appendix on EM Prerequisite Kit in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
- Oracle Real Application Cluster (Oracle RAC) nodes are referred to by their virtual IP (vip) names. The `service_name` parameter is used instead of the system identifier (SID) in `connect_data` mode, and failover is turned on. For more information, refer to *Oracle Database Net Services Administrator's Guide*.

- b. Select the deployment size from the **Deployment Size** list to indicate the number of targets you plan to monitor, the number of Management Agents you plan to have, and the number of concurrent user sessions you plan to have.

The prerequisite checks are run regardless of the selection you make, but the values to be set for the various parameters checked depend on the selection you make.

For more information on deployment sizes, the prerequisite checks that are run, the database parameters that are set, and how you can modify the deployment size after installation, refer to [Section 2.1.6](#).

[Table 4–2](#) describes each deployment size.

Table 4–2 Deployment Size

Deployment Size	Targets Count	Management Agents Count	Concurrent User Session Count
Small	Up to 999	Up to 99	Up to 10
Medium	Between 1000 and 9999	Between 100 and 999	Between 10 and 24
Large	10,000 or more	1000 or more	Between 25 and 50

9. Click Next.

Note: If the database you are connecting to is a database instance created with a preconfigured Management Repository using the database templates offered by Oracle, then make sure the deployment size you select on this screen matches with the deployment size you selected on the Step 2 of 12: Database Templates screen of Oracle Database Configuration Assistant (DBCA) while creating the database instance.

If you want to select a deployment size different from the deployment size you had selected while creating the database instance using DBCA, then do one of the following:

- Select the deployment size of your choice on this screen, and click **Next**. When you see errors, fix the parameters in the database, then return to this screen to continue with the installation. To automatically fix the parameters using Oracle-supplied SQL scripts, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
 - Minimize the installer, create another database instance with a template for the desired deployment size, then return to this screen and select the matching deployment size. For instructions, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
-

Note:

If you are connecting to an Oracle RAC database, and if you have entered the virtual host name of one of its nodes, then the installation wizard prompts you with a Connection String dialog and requests you to update the connect string with information about the other nodes that are part of the cluster. Update the connect string and click **OK**. If you want to test the connection, click **Test Connection**.

If your Oracle RAC database 11.2. or higher is configured with Single Client Access Name (SCAN) listener, then you can enter a connection string using the SCAN listener.

Oracle Real Application Cluster (Oracle RAC) nodes are referred to by their virtual IP (vip) names. The `service_name` parameter is used instead of the system identifier (SID) in `connect_data` mode, and failover is turned on. For more information, refer to *Oracle Database Net Services Administrator's Guide*.

Note: If you are connecting to an Oracle Database that already has a Database Control configured, then you will see an error message with instructions to deconfigure it. Ensure that you follow the instructions outlined in the message to deconfigure the Database Control.

10. Enter Enterprise Manager Configuration Details

On the Repository Configuration Details screen, do the following:

- a. For **SYSMAN Password**, enter a password for creating the SYSMAN user account. The SYSMAN user account is used for creating the SYSMAN schema, which holds most of the relational data used in managing Enterprise Manager Cloud Control. SYSMAN is also the super administrator for Enterprise Manager Cloud Control.

Note:

- Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.
 - If you connect to a database instance that was created using the database template offered by Oracle, then note that the password assigned to the user accounts SYSMAN_MDS, SYSMAN_APM, and SYSMAN_OPSS, which were created while preconfiguring the Management Repository, are automatically reset with the SYSMAN password you enter on this screen.
-

- b. For **Registration Password**, enter a password for registering the new Management Agents that join the Enterprise Manager system.

Note: Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.

- c. For **Management Tablespace**, enter the absolute path to the location where the data file for management tablespace (`mgmt.dbf`) can be stored. The installer uses this information for storing data about the monitored targets, their metrics, and so on. Ensure that the specified path leads up to the file name.

For example, `/u01/oracle/prod/oradata/mgmt.dbf`

- d. For **Configuration Data Tablespace**, enter the absolute path to the location where the data file for configuration data tablespace (`mgmt_ecm_depot1.dbf`) can be stored. This is required for storing configuration information collected from the monitored targets. Ensure that the specified path leads up to the file name.

For example, `/u01/oracle/prod/oradata/mgmt_ecm_depot1.dbf`

- e. For **JVM Diagnostics Data Tablespace**, enter the absolute path to a location where the data file for JVM Diagnostics data tablespace (`mgmt_deepdive.dbf`) can be stored. Ensure that the specified path leads up to the file name. Enterprise Manager Cloud Control requires this data file to store monitoring data related to JVM Diagnostics and Application Dependency Performance (ADP).

For example, `/u01/oracle/prod/oradata/mgmt_deepdive.dbf`

- f. If you want to configure Oracle Software Library (Software Library), select **Configure Oracle Software Library**. Enter the absolute path leading up to a unique directory name on the OMS host where the Software Library can be configured.

By default, an *OMS Shared File System* storage location is configured, so ensure that the location you enter is a mounted location on the OMS host, and is placed outside the Middleware Home. Also ensure that the OMS process owner has read/write access to that location. Configuring on a mounted location helps when you install additional OMS instances as they will require read/write access to the same *OMS Shared File System* storage location.

Note:

- Oracle recommends that you maintain the Software Library outside the Middleware Home. For example, if the middleware home is `/u01/software/oracle/middleware`, then you can maintain the Software Library in `/u01/software/oracle`.
- Oracle strongly recommends that you enter a mounted location on the OMS host so that the same location can be used when you install additional OMS instances. However, if you are unable to provide a mounted location or if you are testing the installation in a test environment and do not want to provide a mounted location, then you can provide a local file system location. In this case, after the installation, make sure you migrate to a mounted location.

For information about the Software Library storage locations, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*. For instructions to migrate to an *OMS Agent File System* storage location, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

- On Microsoft Windows, if you are unable to provide a mounted location, then enter a local file system location at the time of installing the product, and migrate to an *OMS Agent File System* storage location later. The *OMS Agent File System* storage location is the recommend storage type on Microsoft Windows.

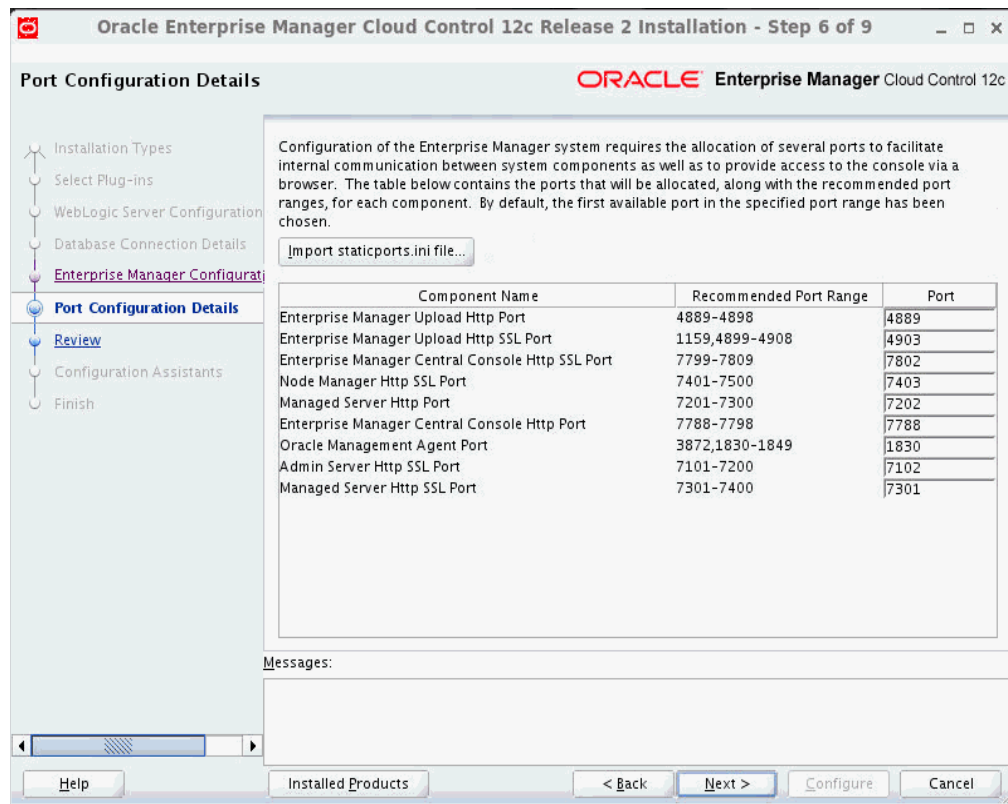
For information about the Software Library storage locations, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*. For instructions to migrate to an *OMS Agent File System* storage location, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

- Configuring the Software Library at the time of installation is optional. Even if you do not select this option and configure it now, your installation will succeed. You always have the option of configuring the Software Library later from the Enterprise Manager Cloud Control Console. However, Oracle strongly recommends that you select this option and configure it at the time of installation so that the installer can automatically configure it for you, thus saving your time and effort.
 - Once the Software Library is configured, you can view the location details in the Software Library Console. To access the Software Library Console, in Cloud Control, from the **Setup** menu, select **Provisioning and Patching**, then select **Software Library**.
-

Note: If you are configuring the Management Repository on a database that uses Oracle Automatic Storage Management (Oracle ASM) for storage, then when you enter the data file location, only the disk group is used for creating the tablespaces. For example, if you specify `+DATA/a.dbf`, then only `+DATA` is used for creating the tablespaces on Oracle ASM, and the exact location of the data file on the disk group is decided by Oracle Managed Files.

11. Click Next.

12. Customize Ports



On the Port Configuration Details screen, customize the ports to be used for various components.

You can enter a free custom port that is either within or outside the port range recommended by Oracle.

To verify if a port is free, run the following command:

- On Unix:


```
netstat -anp | grep <port no>
```
- On Microsoft Windows:


```
netstat -an|findstr <port_no>
```

However, the custom port must be greater than 1024 and lesser than 65535. Alternatively, if you already have the ports predefined in a `staticports.ini` file and if you want to use those ports, then click **Import staticports.ini file** and select the file.

Note: If the `staticports.ini` file is passed during installation, then by default, the ports defined in the `staticports.ini` file are displayed. Otherwise, the first available port from the recommended range is displayed.

The `staticports.ini` file is available in the following location:

```
<Software_Extracted_Location>/response
```

13. Click Next.**14. Review and Configure**

On the Review screen, review the details you provided for the selected installation type.

- If you want to change the details, click **Back** repeatedly until you reach the screen where you want to make the changes.
- After you verify the details, if you are satisfied, click **Configure** to begin the installation process.

15. Track the Progress

On the Install Progress screen, view the overall progress (in percentage) of the installation.

Note:

- If a configuration assistant fails, the installer stops and none of the subsequent configuration assistants are run. Resolve the issue and retry the configuration assistant. For more information, see [Appendix I](#).
- If you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.sh` script from the OMS home to rerun the Configuration Assistant in silent mode. For Microsoft Windows platforms, invoke `runConfig.bat` script.

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<absolute_
path_to_OMS_home> MODE=perform ACTION=configure
COMPONENT_XML={encap_oms.1_0_0_0.xml}
```

If the `runConfig.sh` script fails, then clean up your environment and redo the installation.

16. End the Installation

On the Finish screen, you should see information pertaining to the installation of Enterprise Manager. Review the information and click **Close** to exit the installation wizard.

4.4.1.3.1 Using Advanced Script Options

The following are some additional, advanced options you can pass while invoking the `configureGC.sh` script (or `configureGC.bat` on Microsoft Windows):

- By default, `GCDomain` is the default name used for creating the WebLogic Domain. To override this and use a custom WebLogic Domain name, invoke the script with the `WLS_DOMAIN_NAME` option, and enter a unique custom name.

Note: Ensure that the `WLS_DOMAIN_NAME` option was used even when the installation wizard was invoked to install the software binaries as described in [Section 4.4.1.1](#).

For example, if you want to use the custom name `EMDomain`, then run the following command:

```
$<MIDDLEWARE_HOME>/oms/sysman/install/ConfigureGC.sh WLS_DOMAIN_
NAME=EMDomain
```

- If you want to install some plug-ins that are not in the software kit, then follow these steps:
 1. Manually download the plug-ins from the Enterprise Manager Download page on OTN, and store them in an accessible location.
<http://www.oracle.com/technetwork/oem/grid-control/downloads/oem-upgrade-console-502238.html>
 2. Invoke the `ConfigureGC.sh` script (or `ConfigureGC.bat` on Microsoft Windows) with the following option, and pass the location where the plug-ins you want to install are available:

```
./ConfigureGC.sh -pluginLocation <absolute_path_to_plugin_software_location>
```

The Plug-In Deployment screen of the installation wizard displays a list of plug-ins available in the software kit as well as the plug-ins available in this custom location. You can choose the ones you want to install.
- After the configuration ends successfully, the OMS and the Management Agent start automatically. If you do not want them to start automatically, then invoke the script with `START_OMS` and `b_startAgent` options, and set them to `true` or `false` depending on what you want to control.

Note: Ensure that the `START_OMS` and `b_startAgent` options are used even when the installation wizard was invoked to install the software binaries as described in [Section 4.4.1.1](#).

For example, if you do not want the Management Agent to start automatically, then run the following command:

```
$<MIDDLEWARE_HOME>/oms/sysman/install/ConfigureGC.sh START_OMS=true b_
startAgent=false
```

To understand the limitations involved with this advanced option, see [Section 3.4.3](#).

4.4.1.4 Performing Post-Configuration Tasks

Perform the post-install steps as described in the chapter on installing Enterprise Manager system that is available in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

4.4.2 Installing in Silent Mode

This section explains how you can install only the software binaries of Enterprise Manager Cloud Control at one point in silent mode, and configure the installation at a later point. In particular, this section covers the following:

- [Installing Software](#)
- [Running Root Script](#)
- [Configuring Software](#)
- [Performing Post-Configuration Tasks](#)

4.4.2.1 Installing Software

To install only the software binaries of Enterprise Manager Cloud Control in silent mode, follow these steps:

Note: Oracle recommends you to run the EM Prerequisite Kit before invoking the installer to ensure that you meet all the repository requirements beforehand. Even if you do not run it manually, the installer anyway runs it in the background while installing the product. However, running it manually beforehand sets up your Management Repository even before you can start the installation or upgrade process. For information on the kit, to understand how to run it, and to know about the prerequisite checks it runs, see *Oracle Enterprise Manager Basic Installation Guide*.

1. Copy the following response file to an accessible location on your local host:

```
<Software_Location>/response/software_only.rsp
```

In this command, <Software_Location> refers to either the DVD or the location where you have downloaded software kit.

2. Edit the response file and enter appropriate values for the variables described in [Table 4-3](#).
3. Invoke the installer. (On Unix, make sure you invoke the installer as a user who belongs to the oinstall group you created. For information about creating operating system groups and users, see the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.)

- If this is the first Oracle product you are installing on the host, then run the following command:

```
./runInstaller -silent -responseFile <absolute_path>/software_only.rsp [-invPtrLoc <absolute_path_to_oraInst.loc>]
```

- Otherwise, run the following command:

```
./runInstaller -silent -responseFile <absolute_path>/software_only.rsp
```

Note:

- To invoke the installation wizard on UNIX platforms, run `runInstaller`. To invoke on Microsoft Windows platforms, run `setup.exe`.
 - For information about the additional, advanced options you can pass while invoking the installer, refer to [Section 3.4.2](#).
-

Note: When you invoke `runInstaller` or `setup.exe`, if the Enterprise Manager Cloud Control Installation Wizard does not appear, then it is possible that you do not have read and write access to `/stage`, which is a subdirectory in the `Disk1` directory of the Enterprise Manager software.

There is a classpath variable that the installation wizard computes for OPatch as `../stage/Components/`, and when the `TEMP` variable is set to `/tmp`, the installation wizard tries to look for the `opatch` JAR file in the `/tmp/./stage` directory, which is equivalent to `/stage`.

However, if you do not have read and write permission on `/stage`, then the installation wizard can hang. Under such circumstances, verify if you have read and write access to the `/stage` directory. If you do not have, then set the `TEMP` variable to a location where the install user has access to, and then relaunch the installation wizard.

4.4.2.1.1 Editing Response File for Installing Software

Table 4–3 describes what variables you must edit and how you must edit them in the `software_only.rsp` response file for installing the software binaries.

Table 4–3 Editing Response File for Installing Enterprise Manager Software

Parameter	Description
UNIX_GROUP_NAME	(Required only when central inventory does not exist) Enter the name of the UNIX group you belong to. For example, "dba" Note: This parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
INVENTORY_LOCATION	(Required only when central inventory does not exist) Enter the absolute path to the Central Inventory. For example, <code>/scratch/oracle/oraInventory</code> Note: This parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
SECURITY_UPDATES_VIA_MYORACLESUPPORT	<ul style="list-style-type: none"> Enter <code>TRUE</code> if you want to download and install security updates. Then, enter the credentials for the following variables: <code>MYORACLESUPPORT_USERNAME</code> <code>MYORACLESUPPORT_PASSWORD</code> Enter <code>FALSE</code> if you do not want to download and install security updates:
DECLINE_SECURITY_UPDATES	<ul style="list-style-type: none"> Enter <code>TRUE</code> if you want to decline the security updates. In this case, you should have entered <code>False</code> for <code>SECURITY_UPDATES_VIA_MYORACLESUPPORT</code>. Enter <code>FALSE</code> if you do not want to decline the security updates. In this case, you should have entered <code>TRUE</code> for <code>SECURITY_UPDATES_VIA_MYORACLESUPPORT</code>.

Table 4–3 (Cont.) Editing Response File for Installing Enterprise Manager Software

Parameter	Description
INSTALL_UPDATES_SELECTION	<p>By default, this variable is set to "skip" indicating that the software updates will not be installed during installation.</p> <ul style="list-style-type: none"> ■ If you want to install the software updates from My Oracle Support, then set this variable to "download". Then, enter the credentials for the following parameters: MYORACLESUPPORT_USERNAME_FOR_SOFTWAREUPDATES MYORACLESUPPORT_PASSWORD_FOR_SOFTWAREUPDATES ■ If you want to install the software updates from a staged location, then set this variable to "staged". Then, for the <code>STAGE_LOCATION</code> parameter, enter the absolute path, which leads to the Updates directory, where the software updates are available.
ORACLE_MIDDLEWARE_HOME_LOCATION	<p>Enter the location where you want the installer to install Oracle WebLogic Server 11g Release 1 (10.3.6) and Java Development Kit 1.6.0.43.0.</p> <p>For example, <code>/u01/app/Oracle/Middleware</code>.</p> <p>Ensure that the middleware location has <i>write</i> permission to create the OMS home.</p> <p>If you have already installed them manually, then enter the location where you have installed them. Also make sure you have applied patch 14482558 and patch 13349651 on the Oracle WebLogic Server. For instructions, see the following URL:</p> <p>http://docs.oracle.com/cd/E14759_01/doc.32/e14143/intro.htm#CHDCAJFC</p> <p>For more information about Oracle Middleware home, see Section 2.3.2.</p> <p>Note: Ensure that the Middleware home you enter here is used only for Enterprise Manager Cloud Control. Ensure that no other Oracle Fusion Middleware products or components are installed in the same Middleware home.</p> <p>Note: Ensure that the number of characters in the middleware home path does not exceed 70 characters for Unix platforms and 25 characters for Microsoft Windows platforms.</p> <p>For example, the middleware home path <code>C:\Oracle\MW\EM</code> containing only 15 characters is acceptable. However, <code>C:\OracleSoftware\OracleMiddleware\OracleEnterpriseManager\OMS\newrelease\oms</code> containing more than 25 characters is not acceptable for Microsoft Windows platforms.</p>

Table 4–3 (Cont.) Editing Response File for Installing Enterprise Manager Software

Parameter	Description
AGENT_BASE_DIR	<p>Enter the absolute path to the agent base directory, a location outside the Oracle Middleware home where the Management Agent can be installed.</p> <p>For example, <code>/oracle/agent</code>.</p> <p>Ensure that this location is empty and has write permission. Also ensure that it is always maintained outside the Oracle Middleware home.</p> <p>Note: (Only for Microsoft Windows) Ensure that the number of characters in the agent base directory path does not exceed 25 characters.</p> <p>For example, the agent base directory path <code>C:\Oracle\Agent\</code> containing only 16 characters is acceptable. However, <code>C:\Oracle\ManagementAgent\12c\new</code> containing more than 25 characters is not acceptable.</p>
ORACLE_HOSTNAME	<p>Enter a fully qualified domain name that is registered in DNS and is accessible from other network hosts. Oracle recommends that you use a fully qualified domain name.</p> <p>The host name must resolve to the local host because the host name is used for the local Oracle WebLogic Server as well as the Oracle Management Service. Do not provide a remote host or a load balancer virtual host in this field. Do not enter an IP address. Do not use underscores in the name. Short names are allowed, but you will see a warning, so Oracle recommends that you enter a fully qualified domain name instead.</p> <p>If you do not mention the host name, the installation wizard will proceed further, honoring the host name it automatically detects for that host.</p>

4.4.2.2 Running Root Script

(For UNIX Only) After you install the software binaries of Enterprise Manager Cloud Control, log in as a *root* user in a new terminal and run the following scripts:

- If this is the first Oracle product you just installed on the host, then run the `oraInstroot.sh` script from the inventory location specified in the `oraInst.loc` file that is available in the Management Agent home.

For example, if the inventory location specified in the `oraInst.loc` file is `$HOME/oraInventory`, then run the following command:

```
$HOME/oraInventory/oraInstRoot.sh
```

Note: If you are not a *root* user, then use SUDO to change to a *root* user. For example, run the following command:

```
/usr/local/bin/sudo $HOME/oraInventory/oraInstRoot.sh
```

- Run the `allroot.sh` script from the OMS home:

```
$<OMS_HOME>/allroot.sh
```

Note: If you are not a *root* user, then use SUDO to change to a *root* user. For example, run the following command:

```
/usr/local/bin/sudo $<OMS_HOME>/allroot.sh
```

4.4.2.3 Configuring Software

To configure the software binaries of Enterprise Manager Cloud Control, follow these steps:

1. Copy the following response file to an accessible location on the host where you copied the software binaries of Enterprise Manager Cloud Control:

```
<Software_Location>/response/new_install.rsp
```

In this command, *<Software_Location>* refers to either the DVD or the location where you have downloaded software kit.

2. Edit the response file and enter appropriate values for the variables described in [Table 4-4](#).
3. Configure the software binaries by invoking the `ConfigureGC.sh` script (or `ConfigureGC.bat` on Microsoft Windows) passing the response you edited in the previous step:

```
$<MIDDLEWARE_HOME>/oms/sysman/install/ConfigureGC.sh -silent  
-responseFile <absolute_path>/new_install.rsp [-invPtrLoc <absolute_  
path_to_inventory_directory>]
```

Note:

- While installing the software binaries as described in [Section 4.4.2.1](#), if you had passed the argument `-invPtrLoc`, then pass the same argument here as well.
 - The `-invPtrLoc` parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
 - For information about the additional, advanced options you can pass while invoking the script, refer to [Section 4.4.1.3.1](#).
 - The only way to configure a software-only installation is to run the `ConfigureGC.sh` script (or `ConfigureGC.bat` on Microsoft Windows). DO NOT run the individual configuration assistants to configure a software-only installation. If you want to run the individual configuration assistants to configure the installation for some reason, then contact Oracle Support.
 - If you have already configured a software-only installation (the Oracle home) using the `ConfigureGC.sh` script (or `ConfigureGC.bat` on Microsoft Windows), then DO NOT try to reconfigure it—either using the script or using the individual configuration assistants.
 - If you connect to a database instance that was created using the database template offered by Oracle, then you will be prompted that the database parameters need to be modified to suit the deployment size you selected. This is because the templates are essentially designed for simple installation, and the database parameters are set as required for simple installation. Since it is used for advanced installation, the parameters must be set to different values. You can confirm the message to proceed further. The installation wizard will automatically set the parameters to the required values.
-

Note:

- If a prerequisite check fails reporting a missing package, then make sure you install the required package, and retry the installation. The installer validates the package name as well as the version, so make sure you install the packages of the minimum versions mentioned in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. To understand the logic the installer uses to verify these packages, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
 - If any repository-related prerequisite check fails, then run the check manually. For instructions, see the appendix on EM Prerequisite Kit in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
 - If a configuration assistant fails, the installer stops and none of the subsequent configuration assistants are run. Resolve the issue and rerun the configuration assistant. For more information, see [Appendix I](#).
-

4.4.2.3.1 Editing Response File for Configuring Software

Table 4–4 describes what variables you must edit and how you must edit them in the `new_install.rsp` file for configuring the software binaries.

Table 4–4 Editing Response File for Configuring Enterprise Manager Software

Parameter	Description
PLUGIN_SELECTION	<p>By default, mandatory plug-ins such as Oracle Database Management Plug-In, Oracle Fusion Middleware Management Plug-In, Oracle My Oracle Support Management Plug-In, and Oracle Exadata Management Plug-In get automatically installed with the Enterprise Manager system.</p> <p>However, if you want to install any of the other optional plug-ins that are available in the software kit (DVD or downloaded software), then enter the names of those plug-ins for this variable.</p> <p>For example,</p> <pre>PLUGIN_SELECTION={"oracle.sysman.empa", "oracle.sysman.vt" }</pre> <p>If you want to install any plug-in that is not available in the software kit, then do the following:</p> <ol style="list-style-type: none"> 1. Manually download the plug-ins from the Enterprise Manager download page on OTN, and store them in an accessible location: http://www.oracle.com/technetwork/oem/grid-control/downloads/oem-upgrade-console-502238.html 2. Update this variable (PLUGIN_SELECTION) to the names of those plug-ins you downloaded. 3. Invoke the installer with the following option, and pass the location where you downloaded the plug-ins: <pre>./runInstaller -pluginLocation <absolute_path_to_plugin_software_location></pre>
WLS_ADMIN_SERVER_USERNAME	By default, weblogic is the name assigned to the default user account that is created for the Oracle WebLogic Domain. If you want to accept the default name, then blank. However, if you want to have a custom name, then enter the name of your choice.
WLS_ADMIN_SERVER_PASSWORD	<p>Enter a password for the WebLogic user account.</p> <p>Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.</p>
WLS_ADMIN_SERVER_CONFIRM_PASSWORD	Confirm the password for the WebLogic user account.
NODE_MANAGER_PASSWORD	<p>By default, nodemanager is the name assigned to the default user account that is created for the node manager. Enter a password for this node manager user account.</p> <p>Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.</p>
NODE_MANAGER_CONFIRM_PASSWORD	Confirm the password for the node manager user account.

Table 4–4 (Cont.) Editing Response File for Configuring Enterprise Manager Software

Parameter	Description
ORACLE_INSTANCE_HOME_LOCATION	<p>By default, <code>gc_inst</code> is considered as the OMS Instance Base directory for storing all OMS-related configuration files. Enter the absolute path to a location outside the middleware home leading up to the directory name.</p> <p>For more information about this location, see Section 2.3.3.</p>
DATABASE_HOSTNAME	<p>Enter the fully qualified name of the host where the existing database resides. Ensure that the host name does not have underscores.</p> <p>For example, <code>example.com</code></p> <p>If you have already created a database instance with a preconfigured Management Repository using the database templates offered by Oracle, then provide details about that database instance.</p> <p>If you are connecting to an Oracle RAC Database, and if the nodes have virtual host names, then enter the virtual host name of one of its nodes.</p> <p>The connection to the database is established with a connect string that is formed using only this virtual host name, and the installation ends successfully.</p> <p>However, if you want to update the connect string with other nodes of the cluster, then after the installation, run the following command:</p> <pre>\$<OMS_HOME>/bin/emctl config oms -store_repos_details -repos_conn_desc "(DESCRIPTION= (ADDRESS_LIST= (FAILOVER=ON) (ADDRESS= (PROTOCOL=TCP) (HOST=node1-vip.example.com) (PORT=1521)) (ADDRESS= (PROTOCOL=TCP) (HOST=node2-vip.example.com) (PORT=1521))) (CONNECT_DATA= (SERVICE_NAME=EMREP)))" -repos_user sysman</pre> <p>If your Oracle RAC database 11.2 or higher is configured with Single Client Access Name (SCAN) listener, then you can enter a connection string using the SCAN listener.</p> <p>Note: If you connect to a database instance that was created using the database template offered by Oracle, then note that the password assigned to the user accounts <code>SYSMAN_MDS</code>, <code>SYSMAN_APM</code>, and <code>SYSMAN_OPSS</code>, which were created while preconfiguring the Management Repository, are automatically reset with the <code>SYSMAN</code> password you enter for the <code>SYSMAN_PASSWORD</code> parameter.</p>
LISTENER_PORT	<p>Enter the listener port to connect to the existing database.</p> <p>For example, <code>1521</code></p>
SERVICENAME_OR_SID	<p>Enter the service name or the system ID (SID) of the existing database.</p> <p>For example, <code>orcl</code></p>
SYS_PASSWORD	<p>Enter the SYS user account's password.</p>

Table 4–4 (Cont.) Editing Response File for Configuring Enterprise Manager Software

Parameter	Description
DEPLOYMENT_SIZE	<p>Set one of the following values to indicate the number of targets you plan to monitor, the number of Management Agents you plan to have, and the number of concurrent user sessions you plan to have.</p> <ul style="list-style-type: none"> ■ Small, to monitor up to 999 targets, with up to 99 Management Agents and up to 10 concurrent user sessions ■ Medium, to monitor about 1000 to 9999 targets, with about 100 to 999 Management Agents and about 10 to 24 concurrent user sessions ■ Large, to monitor 10,000 or more targets, with 1000 or more Management Agents, and with about 25 to 50 concurrent user sessions <p>If the database you are connecting to is a database instance created with a preconfigured Management Repository using the database templates offered by Oracle, then make sure the deployment size you set here matches with the deployment size you selected on the Step 2 of 12: Database Templates screen of Oracle Database Configuration Assistant (DBCA) while creating the database instance.</p> <p>If you want to select a deployment size different from the deployment size you had selected while creating the database instance using DBCA, then do one of the following:</p> <ul style="list-style-type: none"> ■ Create another database instance with a template for the desired deployment size, then return to this response file and set the same deployment size to this parameter. For instructions to create a database instance with an Oracle-supplied template, see <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>. ■ In the database instance you have created, fix the parameters to support the deployment size you want to set here in the response file. To automatically fix the database parameters using Oracle-supplied SQL scripts, see <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>.
SYSMAN_PASSWORD	<p>Enter a password for creating a SYSMAN user account. This password is used to create the SYSMAN user, which is the primary owner of the Management Repository schema.</p> <p>Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.</p> <p>Note: If you connect to a database instance that was created using the database template offered by Oracle, then note that the password assigned to the user accounts SYSMAN_MDS, SYSMAN_APM, and SYSMAN_OPSS, which were created while preconfiguring the Management Repository, are automatically reset with the SYSMAN password you enter for this parameter.</p>
SYSMAN_CONFIRM_PASSWORD	Confirm the SYSMAN user account's password.

Table 4–4 (Cont.) Editing Response File for Configuring Enterprise Manager Software

Parameter	Description
MANAGEMENT_TABLESPACE_LOCATION	<p>Enter the absolute path to the location where the data file for management tablespace (mgmt.dbf) can be stored. Ensure that the specified path leads up to the file name.</p> <p>For example:</p> <ul style="list-style-type: none"> ■ If the database is on a file system, then the path must look like /u01/oracle/prod/oradata/mgmt.dbf ■ If the database is on Automatic Storage Management (ASM), then the path must look like +<disk_group1>/prod/oradata/mgmt.dbf, where disk_group1 is a diskgroup created on ASM and prod is the Service ID (SID). ■ If the database is on a raw device, then the path must look like </dev/raw1>/prod/oradata/mgmt.dbf, where /dev/raw1 is the raw device and prod is the SID. <p>Enterprise Manager Cloud Control requires this data file to store information about the monitored targets, their metrics, and so on. Essentially, everything else other than configuration data, software library data, and audit data.</p>
CONFIGURATION_DATA_TABLESPACE_LOCATION	<p>Enter the absolute path to the location where the data file for configuration data tablespace (mgmt_ecm_depot1.dbf) can be stored. Ensure that the specified path leads up to the file name.</p> <p>For example, /home/john/oradata/mgmt_ecm_depot1.dbf</p> <p>Enterprise Manager Cloud Control requires this data file to store configuration information collected from the monitored targets.</p>
JVM_DIAGNOSTICS_TABLESPACE_LOCATION	<p>Enter the absolute path to a location where the data file for JVM Diagnostics data tablespace (mgmt_deepdive.dbf) can be stored. Ensure that the specified path leads up to the file name.</p> <p>For example, /home/john/oradata/mgmt_deepdive.dbf</p> <p>Enterprise Manager Cloud Control requires this data file to store monitoring data related to JVM Diagnostics and Application Dependency Performance (ADP).</p>
AGENT_REGISTRATION_PASSWORD	Enter a password to secure the communication between the OMS and the Management Agents. Note that you have to provide the same registration password for securing your Management Agents.
AGENT_REGISTRATION_CONFIRM_PASSWORD	Confirm the agent registration password.
CONFIGURE_ORACLE_SOFTWARE_LIBRARY	<p>If you want to configure the Software Library at the time of installation, set this parameter to TRUE. Otherwise, set it to FALSE.</p> <p>Even if you do not configure it at the time of installation, your installation will succeed, and you can always configure it later from the Enterprise Manager Cloud Control Console. However, Oracle recommends that you configure it at the time of installation so that it is automatically configured by the installer, thus saving your time and effort.</p>

Table 4–4 (Cont.) Editing Response File for Configuring Enterprise Manager Software

Parameter	Description
SOFTWARE_LIBRARY_LOCATION	If you have set <code>CONFIGURE_ORACLE_SOFTWARE_LIBRARY</code> to <code>TRUE</code> , then enter the absolute path leading up to a unique directory name on the OMS host where the Software Library can be configured. Ensure that the location you enter is a mounted location on the OMS host, and is placed outside the Middleware Home. Also ensure that the OMS process owner has read/write access to that location. Configuring on a mounted location helps when you install additional OMS instances as they will require read/write access to the same <i>OMS Shared File System</i> storage location.
STATIC_PORTS_FILE	By default, ports described in Section 2.1.9 are honored. If you want to accept the default ports, then leave this field blank. If you want to use custom ports, then enter the absolute path to the <code>staticports.ini</code> file that lists the custom ports to be used for the installation.

4.4.2.4 Performing Post-Configuration Tasks

Perform the post-install steps as described in the chapter on installing Enterprise Manager system that is available in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

Part III

Installing Additional Oracle Management Service

This part contains the following chapters:

- [Chapter 5, "Installing Additional Oracle Management Service in Silent Mode"](#)

Installing Additional Oracle Management Service in Silent Mode

Oracle recommends you to use the Add Management Service deployment procedure to install an additional Oracle Management Service (OMS). The Add Management Service deployment procedure offers a GUI-rich, interactive way of installing an additional OMS. For instructions, refer to *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

However, if you have any security restrictions or audit demands in your environment, or if you are not permitted to use Oracle credentials to log in over the network for installation, then follow these steps to manually install an additional OMS in silent, non-interactive mode.

1. If Oracle Software Library (Software Library) is configured on the main OMS, which comes with Enterprise Manager Cloud Control, then do the following:
 - **On Unix Platforms:** Ensure that Software Library is read-write accessible from the remote host where you plan to install the additional OMS.
 - **On Microsoft Windows Platforms:** If you do not have an option to share or mount the Software Library, then copy the Software library from the main, source OMS host to the destination host where you plan to install the additional OMS.

In this procedure, for easy understanding, the OMS that comes with Enterprise Manager Cloud Control is referred to as the *first OMS*, and the additional OMS you install is referred to as the *additional OMS*.

2. On the remote host, perform a software-only installation of the additional OMS as described in [Section 4.4.1](#).

Note:

- Ensure that you install the software binaries as the same user as the one used for installing the first OMS. You must be able to access the Software Library files.
 - Ensure that you install the software binaries in the same middleware location as that of the first OMS.
 - At the end of the software-only installation, do NOT run the `ConfigureGC.sh` (for Unix platforms) or `ConfigureGC.bat` script (for Microsoft Windows) as prompted by the installer. That file must be run only when you are performing a fresh installation.
-

3. Deploy the plug-ins:

- **In GUI Mode (using the installer screen)**

Invoke the `PluginInstall.sh` script from the following location:

```
$<OMS_HOME>/sysman/install/PluginInstall.sh
```

On the Plug-In Deployment screen, select the optional plug-ins you want to install.

The screen displays only those plug-ins that were available in the software kit (DVD, downloaded software) you used in the previous step for installing the software binaries.

The pre-selected rows on this screen are mandatory plug-ins that will be installed by default. Select the optional ones you want to install.

- **In Silent Mode (command line):**

Invoke the `PluginInstall.sh` script from the following location:

```
$<OMS_HOME>/sysman/install/PluginInstall.sh -silent PLUGIN_
SELECTION="{PLUGIN_ID1,PLUGIN_ID2}"
```

For example,

```
$<OMS_HOME>/sysman/install/PluginInstall.sh -silent PLUGIN_
SELECTION="{oracle.sysman.emfa,oracle.sysman.vt}"
```

Note:

- On Microsoft Windows, run `PluginInstall.bat`.
- Ensure that you select the same set of plug-ins as the ones on the source OMS (or first OMS).

To identify the plug-ins installed on the source OMS (or first OMS), follow these steps:

1. Connect to the Management Repository and run the following SQL query to retrieve a list of plug-ins installed:

```
SELECT epv.plugin_id, epv.version, epv.rev_
version FROM em_plugin_version epv, em_
current_deployed_plugin ecp WHERE epv.plugin_
type NOT IN ('BUILT_IN_TARGET_TYPE',
'INSTALL_HOME') AND ecp.dest_type='2' AND
epv.plugin_version_id = ecp.plugin_version_id
```

2. Make a note of the additional plug-ins you installed.

- To install the additional plug-ins that are installed on the source OMS (or first OMS), or to install any additional plug-ins that are not in the software kit you used for installing the binaries, follow these steps:

1. Manually download the plug-ins from the Enterprise Manager Download page on OTN, and store them in an accessible location.

<http://www.oracle.com/technetwork/oem/grid-control/downloads/oem-upgrade-console-502238.html>

2. Invoke the script with the following option, and pass the location where the plug-ins you want to install are available:

In GUI Mode (using the installer screen):

```
$<OMS_HOME>/sysman/install/PluginInstall.sh
-pluginLocation <absolute_path_to_plugin_
software_location>
```

The Plug-In Deployment screen displays a list of plug-ins that were available in the software kit as well as the downloaded plug-ins available in this custom location. You can choose the ones you want to install.

In Silent Mode (command line):

```
$<OMS_HOME>/sysman/install/PluginInstall.sh
-silent PLUGIN_SELECTION="{PLUGIN_ID1,PLUGIN_
ID2}"-pluginLocation <absolute_path_to_
plugin_software_location>
```

-
-
4. On the additional OMS, apply all the patches you applied on the first OMS so that both OMS instances are identical and are in sync. Patches include patches that

modified the Enterprise Manager system, the Software Library, the OMS files, the Management Repository, and so on.

To identify the patches you applied on the first OMS, run the following commands from its Oracle home:

```
$<OMS_HOME>/OPatch/patch lsinventory
```

5. Export the configuration details from the first OMS. To do so, run the following command from the Oracle home of the first OMS, and pass the location where the configuration details can be exported as a file.

```
$<OMS_HOME>/bin/emctl exportconfig oms -dir <absolute_path_to_directory>
```

6. Copy the exported configuration details file from the first OMS host to the additional OMS host.
7. Copy the configuration details onto the additional OMS. To do so, run the following command from the Oracle home of the additional OMS:

```
$<OMS_HOME>/bin/omsca recover -ms -backup_file <absolute_path_to_the_file_copied_in_step4> [-AS_HTTPS_PORT <port> -MSPORT <port> -MS_HTTPS_PORT <port> -EM_NODEMGR_PORT <port> -EM_UPLOAD_PORT <port> -EM_UPLOAD_HTTPS_PORT <port> -EM_CONSOLE_PORT <port> -EM_CONSOLE_HTTPS_PORT <port> -config_home <absolute_path_to_instance_dir> -EM_INSTANCE_HOST <second_oms_host_name>]
```

For example,

```
$<OMS_HOME>/bin/omsca recover -ms -backup_file /opt/oracle/product/backup/opf_ADMIN_20120504_031016.bka -AS_HTTPS_PORT 7101 -MSPORT 7202 -MS_HTTPS_PORT 7301 -EM_NODEMGR_PORT 7403 -EM_UPLOAD_PORT 4889 -EM_UPLOAD_HTTPS_PORT 4900 -EM_CONSOLE_PORT 7788 -EM_CONSOLE_HTTPS_PORT 7799 -config_home /opt/oracle/product/omsmdw/gc_inst -EM_INSTANCE_HOST example.com
```

8. (Applicable only if you do not already have a Management Agent on the host) Configure the Management Agent on the additional OMS host by running the following command from the OMS home:

```
$<AGENT_HOME>/sysman/install/agentDeploy.sh AGENT_BASE_DIR=<middleware_home>/agent OMS_HOST=<second_oms_host_name> EM_UPLOAD_PORT=<second_oms_port> AGENT_REGISTRATION_PASSWORD=<password> -configOnly
```

Note: If you have Server Load Balancer (SLB) configured, then directly enter the host name and port number of the SLB. If SLB is not configured, then enter the secure upload port of the first OMS.

9. Deploy the required plug-ins on the Management Agent.

For information about deploying plug-ins, refer to the section *Deploying and Updating Plug-ins* in the chapter *Updating Cloud Control*, in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

10. Import the trusted certificate on the additional OMS host, where you configured the Management Agent as described in Step (7). When prompted for a password, enter welcome.

```
$<AGENT_HOME>/bin/emctl secure add_trust_cert_to_jks
```

11. Manually discover the Oracle WebLogic Server target.

- a. Ensure that both the first and the additional OMS instances are up and running.
- b. In the Cloud Control console, from the **Targets** menu, select **All Targets**.
- c. On the All Targets page, search and click **/EMGC_GCDomain/GCDomain/**.
- d. On the EMGC_GCDomain home page, from the **WebLogic Domain** menu, select **Refresh WebLogic Domain**.
- e. On the Refresh WebLogic Domain page, click **Add / Update Targets**, and follow the steps guided by the wizard.

Enterprise Manager Cloud Control refreshes the WebLogic Domain and discovers the second managed server on the additional OMS host.

For information about discovering the other targets, refer to the chapter *Adding Targets* in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

For configuring the shared Oracle Software Library location and the Server Load Balancer, refer to *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

Part IV

Installing Oracle Management Agent

This part describes the different ways of installing Oracle Management Agent. In particular, this part contains the following chapters:

- [Chapter 6, "Installing Oracle Management Agent in Silent Mode"](#)
- [Chapter 7, "Cloning Oracle Management Agent"](#)
- [Chapter 8, "Installing Shared Agent"](#)
- [Chapter 9, "Installing Oracle Management Agent Software Now and Configuring Later"](#)

Installing Oracle Management Agent in Silent Mode

This chapter describes how you can install Oracle Management Agent (Management Agent) in silent mode. In particular, this chapter covers the following:

- [Overview](#)
- [Before You Begin](#)
- [Prerequisites](#)
- [Installation Procedure](#)
- [After You Install](#)

6.1 Overview

Installing a Management Agent in silent mode is only an alternative to installing it using the Add Host Targets Wizard. While the Add Host Targets Wizard requires you to use its GUI-rich interview screens for providing all installation details, the silent mode requires you to use a response file for providing installation details and deployment scripts to install Management Agents on hosts.

Installing in silent mode is useful when you want to install an additional Management Agent on a destination host from the destination host itself, without using the Add Host Targets Wizard.

You can install Management Agents in silent mode using the following methods:

Using the AgentPull Script

In this method, you do not have to use EM CLI to download the Management Agent software onto the remote destination host before executing the script to install the Management Agent. This method supports only a few additional parameters, and is ideal for a basic Management Agent install.

Using the agentDeploy Script

In this method, you must use EM CLI to download the Management Agent software onto the remote destination host before executing the script to install the Management Agent. You can either choose to use EM CLI from the OMS host, or from the remote destination host. If you choose to use EM CLI from the OMS host, you must transfer the downloaded Management Agent software to the remote destination host before executing the script to install the Management Agent. This method supports many additional parameters, and is ideal for a customized Management Agent install.

Using the RPM File

In this method, you obtain the .rpm file using EM CLI on the OMS host, then transfer the file to the remote destination host before running the file to install the Management Agent. Using the .rpm file, you can also choose to install a Management Agent while provisioning an operating system on a bare metal host. For more information, see the *Oracle Enterprise Manager Administrator's Guide for Software and Server Provisioning and Patching*. This guide is available in the Enterprise Manager documentation library at:

<http://www.oracle.com/technetwork/indexes/documentation/index.html>

Note:

- The Management Agent .rpm file can be obtained using EM CLI only for Linux x86 and Linux x86-64 platforms.
 - For Enterprise Manager 12c (12.1.0.x), installing a Management Agent by downloading the Management Agent .rpm file from Oracle Technology Network (OTN) is not supported.
-
-

Once the installation is complete, you will see the following default contents in the agent base directory:

```
<agent_base_directory>
|____core
|    |____12.1.0.3.0
|____plugins
|____plugins.txt
|____plugins.txt.status
|____agent_inst
|____sbin
|____agentimage.properties
```

Note:

- You can repoint your existing Management Agents to a new Oracle Management Service (OMS). For information on how to do this, see the Redirecting Oracle Management Agent to Another Oracle Management Service Appendix present in *Oracle Enterprise Manager Cloud Control Advanced Installation Guide*.

When you repoint your existing Management Agents to a new OMS, you cannot move the targets monitored by the Management Agents, the target history, and the Management Agent history. The monitored targets and the history data is lost.

- (For Microsoft Windows hosts) If you upgrade a 12.1.0.x Management Agent and you want to install another Management Agent on the same host, which points to a different OMS, ensure that you specify the `s_agentSrvName` parameter while installing the Management Agent, as described in [Section 6.4.5](#).
-
-

6.2 Before You Begin

Before you begin installing a Management Agent in silent mode, keep these points in mind:

- You can install a Management Agent on only one host at a time by using the silent methods. Therefore, use this approach when you want to install a Management Agent on only a few hosts.
- The Management Agent software for the platform of the host on which you want to install a Management Agent must be downloaded and applied, using Self Update. Only the Management Agent software for the OMS host platform is downloaded and applied by default. The Management Agent software contains the core binaries required for installation, the response file to be edited and passed, and the `agentDeploy.sh` script (`agentDeploy.bat` for Microsoft Windows).

For information on how to download and apply the Management Agent software for a platform using Self Update, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

- In Enterprise Manager Cloud Control 12c Release 3 (12.1.0.3.0), you can save the Management Agent one-off patches that you want to apply on a particular version of the Management Agent software, such that these patches are automatically applied on the software whenever a new Management Agent of the same version is deployed, or an old Management Agent is upgraded to that version.

For information on how to do this, see [Appendix D](#).

Also, you can apply one-off patches on a plug-in and create a custom patched plug-in, such that this custom patched plug-in is deployed on all the new Management Agents that you deploy, and all the old Management Agents that you upgrade.

For information on how to do this, see *Oracle Enterprise Manager Cloud Control Administration Guide*.

- From Enterprise Manager Cloud Control 12c Release 3 (12.1.0.3), parallel deployment of Management Agents using the `AgentPull.sh` script (`AgentPull.bat` for Microsoft Windows) is supported. This enables you to deploy Management Agents on multiple hosts, at the same time (in a parallel manner), using the `AgentPull.sh` or `AgentPull.bat` script.
- If you want to install a Management Agent on a Microsoft Windows host in silent mode, ensure that you execute the `AgentPull.bat` or `agentDeploy.bat` script from the default command prompt, which is `cmd.exe`, and not from any other command prompt.
- You cannot run any preinstallation or postinstallation scripts as part of the installation process. You can run them manually before or after the installation.
- By default, installing a Management Agent in silent mode configures only the following types of plug-ins:
 - All discovery plug-ins that were configured with the OMS from where the Management Agent software is being deployed.
 - Oracle Home discovery plug-in
 - Oracle Home monitoring plug-in

6.3 Prerequisites

Before installing a Management Agent in silent mode, ensure that you meet the following prerequisites:

Table 6–1 Prerequisites for Installing Oracle Management Agent in Silent Mode

Requirement	Description
Hardware Requirements	Ensure that you meet the hard disk space and physical memory requirements. For more information, see the chapter on hardware requirements in the <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i> .
Operating System Requirements	<p>Ensure that you install the Management Agent only on certified operating systems as mentioned in the Enterprise Manager certification matrix available on <i>My Oracle Support</i>.</p> <p>To access the Enterprise Manager certification matrix, follow the steps outlined in <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>.</p> <p>For information about platforms receiving future support, refer to <i>My Oracle Support</i> note 793512.1.</p>
Package Requirements	<p>Ensure that you install all the operating system-specific packages. For more information, see the chapter on package requirements in the <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>.</p> <p>If you choose to install a Management Agent using a .rpm file, ensure that the rpm-build package is installed on the host. To verify this, run the following command:</p> <pre>rpm -qa grep rpm-build</pre>
cURL Utility Requirements (For installing using the AgentPull script only)	<p>Ensure that you install the cURL utility on the destination host.</p> <p>You can download the cURL utility from the following URL: http://curl.haxx.se/dlwiz/?type=bin</p> <p>Note: For destination hosts running on Microsoft Windows, Oracle recommends that you install cURL in c:\.</p>
ZIP and UNZIP Utility Requirements	<p>Ensure that the ZIP and the UNZIP utilities are present on the destination host.</p> <p>The ZIP utility must be of version 3.0 2008 build or higher.</p> <p>The UNZIP utility must be of version 6.0 or higher.</p>
User and Operating System Group Requirement	<p>Ensure that the destination host where you want to install the Management Agent has the appropriate users and operating system groups created.</p> <p>For more information, see the chapter on creating operating system groups and users in the <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>.</p>
/etc/hosts File Requirements	<p>Ensure that the /etc/hosts file on the host has the IP address, the fully qualified name, and the short name in the following format:</p> <pre>172.16.0.0 example.com mypc</pre>

Table 6–1 (Cont.) Prerequisites for Installing Oracle Management Agent in Silent Mode

Requirement	Description
Time Zone Requirements	<p>Ensure that the host time zone has been set correctly. To verify the host time zone, run the following command:</p> <pre>echo \$TZ</pre> <p>If the time zone displayed is incorrect, run the following commands, before running the <code>agentDeploy.sh</code> or <code>agentDeploy.bat</code> scripts, to set the correct time zone:</p> <ul style="list-style-type: none"> For Korn shell: <pre>TZ=<value> export TZ</pre> For Bourne shell or Bash shell: <pre>export TZ=<value></pre> For C shell: <pre>setenv TZ <value></pre> <p>For example, in the Bash shell, run the following command to set the time zone to America/New_York:</p> <pre>export TZ='America/New_York'</pre> <p>To set the time zone on a destination host that runs on Microsoft Windows, from the Start menu, select Control Panel. Click Date and Time, then select the Time Zone tab. Select your time zone from the displayed drop down list.</p> <p>To view a list of the time zones you can use, access the <code>supportedtzs.lst</code> file present in the <code><AGENT_HOME>/sysman/admin</code> directory of the central agent (that is, the Management Agent installed on the OMS host).</p> <p>Note: If you had ignored a prerequisite check warning about wrong time zone settings during the Management Agent install, you must set the correct time zone on the host after installing the Management Agent. For information on setting time zones post install, refer Section 6.5.</p>
PATH Environment Variable Requirements (For installing using the <code>AgentPull</code> script only)	<p>Ensure that the location of <code>zip</code> and <code>unzip</code> is part of the PATH environment variable.</p> <p>For example, if <code>zip</code> and <code>unzip</code> are present in <code>/usr/bin</code>, then <code>/usr/bin</code> must be part of the PATH environment variable.</p>
Path Validation Requirements	<p>Validate the path to all command locations. For more information, refer to the appendix on validating command locations in the <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>.</p>
CLASSPATH Environment Variable Requirements	<p>Unset the CLASSPATH environment variable. You can always reset the variable to the original value after the installation is complete.</p>
Port Requirements	<p>Ensure that the default ports described in Section 2.1.9.1 are free.</p>
Temporary Directory Space Requirements	<p>Ensure that you allocate 400 MB of space for a temporary directory where the executables can be copied.</p> <p>By default, the temporary directory location set to the environment variable <code>TMP</code> or <code>TEMP</code> is honored. If both are set, then <code>TEMP</code> is honored. If none of them are set, then the following default values are honored: <code>/tmp</code> on UNIX hosts and <code>c:\Temp</code> on Microsoft Windows hosts.</p>

Table 6–1 (Cont.) Prerequisites for Installing Oracle Management Agent in Silent Mode

Requirement	Description
/var/tmp Requirements (For installing using the .rpm file only)	Ensure that the /var/tmp directory has at least 700 MB of free space.
/usr/lib/oracle Requirements (For installing using the .rpm file only)	Ensure that the /usr/lib/oracle directory exists and has at least 2 GB of free space. If it does not exist, create it, and ensure that the install user has write permissions on it.
Agent Base Directory Requirements	Ensure the following: <ul style="list-style-type: none"> ■ The agent base directory is empty and has at least 1 GB of free space. ■ The directory name does not contain any spaces. ■ The installing user owns the installation base directory. Ensure that the install user or the root user owns all the parent directories, and the parent directory has read write permissions for the install user. Ensure that the root user owns the root directory. For example, if the installation base directory is /scratch/OracleHomes/agent, and oracle is the installing user, then the /scratch/OracleHomes/agent directory must be owned by oracle, directories scratch and OracleHomes must be owned by either oracle or root user, and the root directory (/) must be owned by root user. ■ If the agent base directory is mounted, it is mounted with the setuid turned on.
Agent Instance Home Requirements (For installing using the agentDeploy script only)	Ensure that the agent instance home location you specify in the response file is empty.
Permission Requirements	<ul style="list-style-type: none"> ■ Ensure that you have <i>write</i> permission in the agent instance home. ■ Ensure that you have <i>write</i> permission in the temporary directory.
Installing User Requirements	If the central inventory owner and the user installing the Management Agent are different, then ensure that they are part of the same group, and have <i>read</i> and <i>write</i> permissions on the inventory directory. For example, if the inventory owner is <i>abc</i> and the user installing the Management Agent is <i>xyz</i> , then ensure that <i>abc</i> and <i>xyz</i> belong to the same group, and they have read and write access to the inventory.

Table 6–1 (Cont.) Prerequisites for Installing Oracle Management Agent in Silent Mode

Requirement	Description
Central Inventory (oraInventory) Requirements	<ul style="list-style-type: none"> Ensure that you allocate 100 MB of space for the Central Inventory. Ensure that the central inventory directory is not in a shared file system. If it is already in a shared file system, then create a new inventory in a non-shared file system. You can optionally migrate the products that were previously installed in the shared file system to this new inventory in the non-shared file system. Ensure that you have <i>read</i>, <i>write</i>, and <i>execute</i> permissions on oraInventory on all remote hosts. <p>If you do not have these permissions on the default inventory (typically in the location mentioned in the <code>/etc/oraInst.loc</code> file) on any remote host, then ensure that you enter the path to an alternative inventory location using the <code>INVENTORY_LOCATION</code> or <code>-invPtrLoc</code> arguments as described in Table 6–6. Note that these parameters are supported only on UNIX platforms, and not on Microsoft Windows platforms.</p>
Agent User Account Permissions and Rights (For installing using the AgentPull or agentDeploy scripts only)	<p>(For Microsoft Windows) If you are installing the Management Agent on a Microsoft Windows-based operating system, then ensure that the agent user account has permissions and rights to perform the following:</p> <ul style="list-style-type: none"> Act as part of the operating system. Adjust memory quotas for a process. Replace process level token. Log in as a batch job. <p>To verify whether the agent user has these rights, follow these steps:</p> <ol style="list-style-type: none"> Launch the Local Security Policy. From the Start menu, click Settings and then select Control Panel. From the Control Panel window, select Administrative Tools, and from the Administrative Tools window, select Local Security Policy. In the Local Security Policy window, from the tree structure, expand Local Policies, and then expand User Rights Assignment.
Permissions for cmd.exe (For installing using the AgentPull or agentDeploy scripts only)	<p>(For Microsoft Windows) If you are installing the Management Agent on a Microsoft Windows-based operating system, then ensure that you grant the <code>Cmd.exe</code> program <i>Read</i> and <i>Execute</i> permissions for the user account that the batch job runs under. This is a restriction from Microsoft.</p> <p>For more information on this restriction and to understand how you can grant these permissions, access the following URL to Microsoft Web site:</p> <p>http://support.microsoft.com/kb/867466/en-us</p>

6.4 Installation Procedure

This section describes the actions involved in installing a Management Agent in silent mode. It consists of the following:

- [Installing a Management Agent Using the AgentPull Script](#)
- [Installing a Management Agent Using the agentDeploy Script](#)
- [Installing a Management Agent Using the RPM File](#)

- [Creating a Response File for Installing Using AgentPull Script](#)
- [Using a Response File for Installing Using agentDeploy Script](#)
- [Creating a Response File for Installing Using an RPM File](#)
- [Understanding the Options Supported by the AgentPull Script](#)
- [Understanding the Options Supported by the agentDeploy Script](#)
- [Understanding the Contents of the Downloaded Management Agent Software](#)

6.4.1 Installing a Management Agent Using the AgentPull Script

To install a Management Agent using the AgentPull script, follow these steps:

1. [Acquire the Management Agent Software.](#)
2. [Install the Management Agent Using the AgentPull Script.](#)

Important: To install a Management Agent using the AgentPull script, you do not need to download the Management Agent software onto the destination host. The AgentPull script performs this action automatically.

6.4.1.1 Acquire the Management Agent Software

1. If the destination host runs on UNIX, access the following URL from the host:

```
https://<OMS_HOST>:<OMS_PORT>/em/install/getAgentImage
```

If the destination host runs on Microsoft Windows, access the following URL from the host:

```
https://<OMS_HOST>:<OMS_PORT>/em/install/getAgentImage?script=bat
```

Save the file as AgentPull.sh (AgentPull.bat for Microsoft Windows) to a temporary directory, say /tmp (c:\temp for Microsoft Windows).

Note: You can also use the following command to obtain the AgentPull.sh script:

```
curl "https://<OMS_HOST>:<OMS_PORT>/em/install/getAgentImage" --insecure  
--no-check-certificate -o AgentPull.sh
```

To use this command, ensure that you have the cURL utility installed, as described in [Table 6-1](#).

2. (Only for UNIX Operating Systems) Provide the execute permission to the AgentPull.sh script by running the following command:

```
chmod +x <absolute_path_to_AgentPull.sh>
```

For example, run the command `chmod +x /tmp/AgentPull.sh`.

3. Identify the platforms for which the Management Agent software is available on the OMS host. Run the AgentPull.sh script (AgentPull.bat for Microsoft Windows) specifying the `-showPlatforms` option to display the platforms for which the Management Agent software is available on the OMS host.

```
<absolute_path_to_AgentPull.sh> -showPlatforms
```

[Example 6-1](#) shows a sample output of the command.

Example 6-1 Output of Running AgentPull.sh Using -showPlatforms

```
Platforms Version
Linux x86-64 12.1.0.3.0
Microsoft Windows x64 (64-bit) 12.1.0.3.0
IBM AIX on POWER Systems (64-bit) 12.1.0.3.0
```

If the output lists the platform on which you want to install the Management Agent, then proceed to the next step. Otherwise, acquire and apply the Management Agent software for the required platform using Self Update.

For information on how to acquire and apply the Management Agent software for a platform using Self Update, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

Note: If you want to install a Management Agent on a host that is running on the Oracle Enterprise Linux 4.x **64-bit platform**, Red Hat Enterprise Linux 4.x **64-bit platform**, or the SUSE Linux Enterprise 10 **64-bit platform**, ensure that the **32-bit version of the Management Agent software for the platform** is available in Software Library.

6.4.1.2 Install the Management Agent Using the AgentPull Script

1. If the destination host runs on UNIX, and the OMS host runs on Microsoft Windows, run the following command:

```
dos2unix <absolute_path_to_AgentPull.sh>
```

For example, run the command `dos2unix /tmp/AgentPull.sh`.

2. Create a response file `agent.rsp` (in any location on the destination host) specifying the parameters described in [Table 6-2](#).

[Example 6-2](#) shows the contents of a sample response file.

Example 6-2 Response File Contents

```
LOGIN_USER=sysman
LOGIN_PASSWORD=welcome
PLATFORM="Linux x86-64"
AGENT_REGISTRATION_PASSWORD=wel246come
```

If you want the script to ignore a particular response file parameter, specify a '#' before the parameter. For example, `#VERSION`.

3. Run the `AgentPull.sh` script (`AgentPull.bat` for Microsoft Windows) specifying the `RSPFILE_LOC` and `AGENT_BASE_DIR` parameters.

```
<absolute_path_to_AgentPull.sh> RSPFILE_LOC=<absolute_path_to_responsefile> AGENT_BASE_DIR=<absolute_path_to_agentbasedir>
```

For example, run the following command:

```
/tmp/AgentPull.sh RSPFILE_LOC=/tmp/agent.rsp AGENT_BASE_DIR=/scratch/agent
```

The `AgentPull.sh` script (and `AgentPull.bat`) supports certain options, such as `-download_only`, which downloads the Management Agent software, but does

not deploy the Management Agent. These supported options are described in [Table 6–5](#).

If you are installing a Management Agent on a Microsoft Windows host using `AgentPull.bat`, ensure that you execute `AgentPull.bat` from the default command prompt, which is `cmd.exe`, and not from any other command prompt.

If the Management Agent install fails, diagnose the problem by viewing the Management Agent install logs. For information on the location of these logs, see [Section B.3](#).

6.4.2 Installing a Management Agent Using the agentDeploy Script

You can install a Management Agent using the `agentDeploy.sh` or `agentDeploy.bat` script in the following ways:

- [Using EM CLI from the Remote Destination Host](#)
- [Using EM CLI from the OMS Host](#)

6.4.2.1 Using EM CLI from the Remote Destination Host

To install a Management Agent using the `agentDeploy` script, and EM CLI from the destination host, follow these steps:

1. [Acquire the Management Agent Software and Download it onto the Destination Host Using EM CLI.](#)
2. [Install the Management Agent Using the agentDeploy Script.](#)

6.4.2.1.1 Acquire the Management Agent Software and Download it onto the Destination Host Using EM CLI

1. Set up EM CLI on the destination host.

For information on how to set up EM CLI on a host that is not running the OMS, refer the Command Line Interface Concepts and Installation chapter of *Oracle Enterprise Manager Command Line Interface*.

2. On the destination host, from the EM CLI install location, log in to EM CLI:

```
<emcli_install_location>/emcli login -username=<username>  
-password=<password>
```

For example,

```
<emcli_install_location>/emcli login -username=sysman  
-password=2benot2be
```

Note: Ensure that the EM CLI log in user has the `ADD_TARGET` privilege.

3. Synchronize EM CLI:

```
<emcli_install_location>/emcli sync
```

4. Identify the platforms for which the Management Agent software is available in Software Library:

```
<emcli_install_location>/emcli get_supported_platforms
```

This command lists all the platforms for which the Management Agent software is available in Software Library. [Example 6-3](#) shows a sample output of the command.

Example 6-3 Output Showing Software Availability for Different Platforms

```
-----
Version = 12.1.0.3.0
Platform Name = Linux x86-64
-----
Version = 12.1.0.3.0
Platform Name = Oracle Solaris on x86-64 (64-bit)
-----
Version = 12.1.0.3.0
Platform Name = HP-UX PA-RISC (64-bit)
-----
```

If the output lists the platform on which you want to install the Management Agent, then proceed to the next step. Otherwise, acquire and apply the Management Agent software for the required platform using Self Update.

For information on how to acquire and apply the Management Agent software for a platform using Self Update, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

Note: If you want to install a Management Agent on a host that is running on the Oracle Enterprise Linux 4.x **64-bit platform**, Red Hat Enterprise Linux 4.x **64-bit platform**, or the SUSE Linux Enterprise 10 **64-bit platform**, ensure that the **32-bit version of the Management Agent software for the platform** is available in Software Library.

5. Download the Management Agent software from Software Library to a temporary directory on the destination host:

```
<emcli_install_location>/emcli get_agentimage -destination=<download_directory> -platform="<platform>" -version=<version>
```

For example,

```
./emcli get_agentimage -destination=/tmp/agentImage -platform="Linux x86-64" -version=12.1.0.3.0
```

Important: If you use the `get_agentimage` EM CLI verb to download the Management Agent software for a platform different from the destination host platform, then you must set the `ZIP_LOC` environment variable to the location of the ZIP utility.

For example, if the ZIP utility is present in `/usr/bin/zip`, set `ZIP_LOC=usr/bin/zip`.

Also, ensure that the ZIP utility is of version 3.0 2008 build or higher.

Note: In the command, note the following:

- `-destination` is a directory on the destination host where you want the Management Agent software to be downloaded. Ensure that you have write permission on this location.
 - `-platform` is the platform for which you want to download the software; this must match one of the platforms listed in the previous step for which the software is available in Software Library.
 - `-version` is the version of the Management Agent software that you want to download; this is an optional argument. If you do not pass this argument, then the version is defaulted to the OMS version.
-

The command downloads the core Management Agent software to the destination directory you entered. For example, for Linux x86-64, you will see the file `12.1.0.3.0_AgentCore_226.zip`. For information on the contents of this core software, see [Section 6.4.9](#).

6.4.2.1.2 Install the Management Agent Using the agentDeploy Script

1. On the destination host, extract the contents of the ZIP file using the unzip utility:

```
unzip <software_zip_file_location> -d <software_extract_location>
```

For example,

```
unzip /tmp/agentImage/12.1.0.3.0_AgentCore_46.zip -d /tmp/agtImg
```

2. Edit the response file `agent.rsp` as described in [Table 6-3](#).

```
<software_extract_location>/agent.rsp
```

[Example 6-4](#) shows the contents of a sample response file.

Example 6-4 Response File Contents

```
OMS_HOST=example.com
EM_UPLOAD_PORT=14511
AGENT_REGISTRATION_PASSWORD=abc123
AGENT_PORT=1832
```

If you want the script to ignore a particular response file parameter, specify a `#` before the parameter. For example, `#AGENT_PORT`.

3. Invoke the deployment script and pass the response file:

```
<software_extract_location>/agentDeploy.sh AGENT_BASE_DIR=<absolute_
path_to_agentbasedir> RESPONSE_FILE=<software_extract_
location>/agent.rsp
```

If you are installing a Management Agent on a Microsoft Windows host using `agentDeploy.bat`, ensure that you execute `agentDeploy.bat` from the default command prompt, which is `cmd.exe`, and not from any other command prompt.

If a proxy is set up between the destination host and the OMS host, you must specify the `REPOSITORY_PROXYHOST` and `REPOSITORY_PROXYPORT` parameters in a properties file, then specify the `PROPERTIES_FILE` parameter while running `agentDeploy.sh` to install a Management Agent on the destination host:


```
<software_extract_location>/agentDeploy.sh AGENT_BASE_DIR=<absolute_
path_to_agentbasedir> RESPONSE_FILE=<absolute_path_to_responsefile>
PROPERTIES_FILE=<absolute_path_to_properties_file>
```

For example, /tmp/agtImg/agentDeploy.sh AGENT_BASE_DIR=/scratch/agent12c
 RESPONSE_FILE=/tmp/agtImg/agent.rsp PROPERTIES_
 FILE=/tmp/agent.properties

The properties file you use must have the following format:

```
REPOSITORY_PROXYHOST=<proxy_host_name>
REPOSITORY_PROXYPORT=<proxy_port>
```

Note:

- Instead of passing a response file, you can choose to pass response file parameters explicitly while invoking the deployment script.

The mandatory response file parameters are OMS_HOST, EM_UPLOAD_PORT, and AGENT_REGISTRATION_PASSWORD.

For example,

```
/tmp/agtImg/agentDeploy.sh AGENT_BASE_
DIR=/scratch/agent12c OMS_HOST=example.com EM_UPLOAD_
PORT=14511 AGENT_REGISTRATION_PASSWORD=2bornot2b
```

- When you pass the arguments while invoking the deployment script, these values need not be given with double quotes. However, when you provide them in a response file, the values need to be in double quotes (except for the argument b_startAgent).
 - In addition to passing the agent base directory and a response file (or individual mandatory arguments with installation details), you can also pass other options that are supported by the deployment script. For more information, see [Section 6.4.8](#).
-
-

4. Run the root scripts after the install. For more information, see [Section 6.5](#).

If you want to install a Management Agent on a physical host, and install another Management Agent on a virtual host that is installed on the physical host, ensuring that both the Management Agents use the same port for communication, follow these steps:

1. Install a Management Agent on the physical host. Stop the Management Agent.
2. Install a Management Agent on the virtual host. Stop the Management Agent.
3. Set AgentListenOnAllNICs=false in the \$<AGENT_HOME>/sysman/config/emd.properties file. Ensure that you perform this step for both the Management Agents.
4. Start up both the Management Agents.

If the Management Agent install fails, diagnose the problem by viewing the Management Agent install logs. For information on the location of these logs, see [Section B.3](#).

6.4.2.2 Using EM CLI from the OMS Host

To install a Management Agent using the `agentDeploy` script, and EM CLI from the OMS host, follow these steps:

1. [Acquire the Management Agent Software and Download it onto the OMS Host Using EM CLI.](#)
2. [Transfer the Management Agent Software to the Destination Host.](#)
3. [Install the Management Agent Using the agentDeploy Script.](#)

6.4.2.2.1 Acquire the Management Agent Software and Download it onto the OMS Host Using EM CLI

1. On the OMS host, from the OMS home, log in to EM CLI. EM CLI is available by default with every OMS installation, so you need not install the client separately on the OMS host.

```
$<OMS_HOME>/bin/emcli login -username=<username> -password=<password>
```

For example,

```
$<OMS_HOME>/bin/emcli login -username=sysman -password=2benot2be
```

Note:

- Ensure that the EM CLI log in user has the `ADD_TARGET` privilege.
- If you have configured a load balancer for a multiple OMS setup, ensure that you run the EM CLI commands on one of the local OMS hosts, and not on the load balancer hosts.
- If you have configured a load balancer for a multiple OMS setup, and you choose to use the EM CLI `setup` command, ensure that you pass the OMS host and port as parameters, and not the load balancer host and port.

For example, `emcli setup -url=https://<OMS_HOST>:<OMS_PORT>/em -user=sysman -password=sysman`

2. Synchronize EM CLI:

```
$<OMS_HOME>/bin/emcli sync
```

3. Identify the platforms for which the Management Agent software is available in Software Library:

```
$<OMS_HOME>/bin/emcli get_supported_platforms
```

This command lists all the platforms for which the Management Agent software is available in Software Library. [Example 6-5](#) shows a sample output of the command.

Example 6-5 Output Showing Software Availability for Different Platforms

```
-----
Version = 12.1.0.3.0
Platform Name = Linux x86-64
-----
Version = 12.1.0.3.0
Platform Name = Oracle Solaris on x86-64 (64-bit)
-----
```

```
Version = 12.1.0.3.0
Platform Name = HP-UX PA-RISC (64-bit)
```

If the output lists the platform on which you want to install the Management Agent, then proceed to the next step. Otherwise, acquire and apply the Management Agent software for the required platform using Self Update.

For information on how to acquire and apply the Management Agent software for a platform using Self Update, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

Note: If you want to install a Management Agent on a host that is running on the Oracle Enterprise Linux 4.x **64-bit platform**, Red Hat Enterprise Linux 4.x **64-bit platform**, or the SUSE Linux Enterprise 10 **64-bit platform**, ensure that the **32-bit version of the Management Agent software for the platform** is available in Software Library.

4. Download the Management Agent software from Software Library to a temporary directory on the OMS host:

```
$<OMS_HOME>/bin/emcli get_agentimage -destination=<download_directory>
-platform="<platform>" -version=<version>
```

For example,

```
./emcli get_agentimage -destination=/tmp -platform="Linux x86-64"
-version=12.1.0.3.0
```

Important: If you use the `get_agentimage` EM CLI verb to download the Management Agent software for a platform different from the OMS host platform, then you must set the `ZIP_LOC` environment variable to the location of the ZIP utility.

For example, if the ZIP utility is present in `usr/bin/zip`, set `ZIP_LOC=usr/bin/zip`.

Also, ensure that the ZIP utility is of version 3.0 2008 build or higher.

Note: In the command, note the following:

- `-destination` is a directory on the OMS host where you want the Management Agent software to be downloaded. Ensure that you have write permission on this location.

If the destination directory is titled with two or more words separated by a space, then enclose the directory name with double quotes.

For example, if the destination directory is titled `/tmp/linux agentimage`, then enter the value as `-destination="/tmp/linux agentimage"`

- `-platform` is the platform for which you want to download the software; this must match one of the platforms listed in the previous step for which the software is available in Software Library.
 - `-version` is the version of the Management Agent software that you want to download; this is an optional argument. If you do not pass this argument, then the version is defaulted to the OMS version.
-

The command downloads the core Management Agent software to the destination directory you entered. For example, for Linux x86-64, you will see the file `12.1.0.3.0_AgentCore_226.zip`. For information on the contents of this core software, see [Section 6.4.9](#).

6.4.2.2.2 Transfer the Management Agent Software to the Destination Host

1. Transfer the downloaded ZIP file to a temporary directory (`/tmp`) on the destination host where you want to install the Management Agent. You can use any file transfer utility to transfer the file.

6.4.2.2.3 Install the Management Agent Using the `agentDeploy` Script

Follow the steps mentioned in [Section 6.4.2.1.2](#) to install the Management Agent.

6.4.3 Installing a Management Agent Using the RPM File

To install a Management Agent using a `.rpm` file, follow these steps:

1. [Acquire the Management Agent Software and Download the RPM File onto the OMS Host.](#)
2. [Transfer the RPM File to the Destination Host.](#)
3. [Install the Management Agent Using the RPM File.](#)

6.4.3.1 Acquire the Management Agent Software and Download the RPM File onto the OMS Host

1. On the OMS host, from the OMS home, log in to EM CLI. EM CLI is available by default with every OMS installation, so you need not install the client separately on the OMS host.

```
$<OMS_HOME>/bin/emcli login -username=<username> -password=<password>
```

For example,

```
$<OMS_HOME>/bin/emcli login -username=sysman -password=2benot2be
```

Note: Ensure that the EM CLI log in user has the ADD_TARGET privilege.

2. Synchronize EM CLI:

```
$<OMS_HOME>/bin/emcli sync
```

3. Identify the platforms for which the Management Agent software is available in Software Library:

```
$<OMS_HOME>/bin/emcli get_supported_platforms
```

This command lists all the platforms for which the Management Agent software is available in Software Library. [Example 6-6](#) shows a sample output of the command.

Example 6-6 Output Showing Software Availability for Different Platforms

```
-----
Version = 12.1.0.3.0
Platform Name = Linux x86-64
-----
Version = 12.1.0.3.0
Platform Name = Oracle Solaris on x86-64 (64-bit)
-----
Version = 12.1.0.3.0
Platform Name = HP-UX PA-RISC (64-bit)
-----
```

If the output lists the platform on which you want to install the Management Agent, then proceed to the next step. Otherwise, acquire and apply the Management Agent software for the required platform using Self Update.

For information on how to acquire and apply the Management Agent software for a platform using Self Update, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

Note: If you want to install a Management Agent on a host that is running on the Oracle Enterprise Linux 4.x **64-bit platform**, Red Hat Enterprise Linux 4.x **64-bit platform**, or the SUSE Linux Enterprise 10 **64-bit platform**, ensure that the **32-bit version of the Management Agent software for the platform** is available in Software Library.

4. Download the .rpm file of the Management Agent from Software Library to a temporary directory on the OMS host

```
$<OMS_HOME>/bin/emcli get_agentimage_rpm -destination=<download_directory> -platform="<platform>" -version=<version>
```

For example,

```
./emcli get_agentimage_rpm -destination=/tmp/agentRPM -platform="Linux x86-64" -version=12.1.0.3.0
```

In the command, note the following:

- -destination is a directory on the OMS host where you want the .rpm file to be downloaded. Ensure that you have write permission on this location.

- `-platform` is the platform for which you want to download the `.rpm` file; this must match one of the platforms listed in the previous step for which the software is available on the OMS host.
- `-version` is the version of the Management Agent for which you want to download the `.rpm` file; this is an optional argument. If you do not pass this argument, then the version is defaulted to the OMS version.

The command downloads the `.rpm` file of the core Management Agent to the destination directory you entered. For example,
`oracle-agt-12.1.0.3.0-1.0.i386.rpm`

6.4.3.2 Transfer the RPM File to the Destination Host

1. Transfer the downloaded `.rpm` file to a temporary directory (`/tmp`) on the destination host where you want to install the Management Agent. You can use any file transfer utility to transfer the file.

6.4.3.3 Install the Management Agent Using the RPM File

1. On the destination host, install the `.rpm` file as a `root` user to install the Management Agent:

```
rpm -ivh <download_directory>/<rpm_file>
```

For example,

```
rpm -ivh /tmp/oracle-agt-12.1.0.3.0-1.0.i386.rpm
```

Note: The following is the output of the command:

```
Preparing... ##### [100%]
Running the prereq
1:oracle-agt ##### [100%]
Follow the below steps to complete the agent rpm installation:
1. Edit the properties file: /usr/lib/oracle/agent/agent.properties
with the correct values
2. Execute the command /etc/init.d/oracle-agt RESPONSE_
FILE=<location_to_agent.properties>
```

2. Edit the `agent.properties` file as described in [Table 6–4](#). The file is available in the following location:

```
/usr/lib/oracle/agent/agent.properties
```

3. Run the following command to complete the installation:

```
/etc/init.d/oracle-agt RESPONSE_FILE=<location_to_agent.properties>
```

If the Management Agent install fails, diagnose the problem by viewing the Management Agent install logs. For information on the location of these logs, see [Section B.3](#).

6.4.4 Creating a Response File for Installing Using AgentPull Script

[Table 6–2](#) describes the various parameters you can include in the response file while installing a Management Agent using the `AgentPull` script.

Table 6–2 Creating a Response File for Installing Oracle Management Agent Using AgentPull Script

Parameter	Description
LOGIN_USER	(Mandatory) Enter the Enterprise Manager console login user name. For example, LOGIN_USER=sysman
LOGIN_PASSWORD	(Mandatory) Enter the Enterprise Manager console login password. For example, LOGIN_PASSWORD=welcome1
PLATFORM	(Mandatory) Enter the platform for which you want to download the Management Agent software. For example, PLATFORM="Linux x86-64" Note: The value of this parameter must be in " ".
VERSION	(Optional) Enter the version of the Management Agent software you want to download. For example, VERSION=12.1.0.3.0 If you do not specify this parameter, it is assigned the OMS version.
AGENT_REGISTRATION_PASSWORD	(Mandatory) Enter a password for registering new Management Agents that join the Enterprise Manager system. By default, the communication between the OMS and the Management Agents is secured and locked. Any new Management Agents that join the Enterprise Manager system must be authenticated before they become part of the system. The password you enter here will be used for authenticating those new Management Agents. For example, AGENT_REGISTRATION_PASSWORD=Wel456come
CURL_PATH (For Microsoft Windows hosts only)	(Optional) Enter the absolute path of the installed cURL utility. For example, CURL_PATH=c:\Program Files\curl If you do not include this parameter, it is assigned the value c:\.

6.4.5 Using a Response File for Installing Using agentDeploy Script

Table 6–3 describes the various parameters you must include in the response file while installing a Management Agent using the agentDeploy script.

Table 6–3 Creating a Response File for Installing Oracle Management Agent Using agentDeploy Script

Parameter	Description
OMS_HOST	(Mandatory) Enter the OMS host name. For example, OMS_HOST=example.com
EM_UPLOAD_PORT	(Mandatory) Enter the upload port (HTTP or HTTPS) for communicating with the OMS. For example, EM_UPLOAD_PORT=14511

Table 6–3 (Cont.) Creating a Response File for Installing Oracle Management Agent Using agentDeploy Script

Parameter	Description
AGENT_REGISTRATION_PASSWORD	<p>(Mandatory) Enter a password for registering new Management Agents that join the Enterprise Manager system.</p> <p>By default, the communication between the OMS and the Management Agents is secured and locked. Any new Management Agents that join the Enterprise Manager system must be authenticated before they become part of the system. The password you enter here will be used for authenticating those new Management Agents.</p> <p>For example, AGENT_REGISTRATION_PASSWORD=We1456come</p>
AGENT_INSTANCE_HOME	<p>(Optional) Enter a directory location on the destination host where all Management Agent-related configuration files can be stored. For this parameter, you can do one of the following:</p> <ul style="list-style-type: none"> ■ Leave it blank. In this case, by default, an instance directory titled agent_inst is created in the agent installation base directory. For example, if the installation base directory is /john/oracle/, then the instance directory is defaulted to /john/oracle/agent_inst ■ Enter the absolute path to a custom directory. Although you can enter any location as a custom location, Oracle recommends you to maintain the instance directory inside the installation base directory. For example, AGENT_INSTANCE_HOME=/john/oracle/instance_dir/inst_mydir
AGENT_PORT	<p>(Optional) Enter a free port on which the Management Agent process should be started. The same port is used for both HTTP and HTTPS.</p> <p>For example, AGENT_PORT=1832</p> <p>If you do not enter any value, then either 3872 or any free port between 1830 and 1849 is honored.</p>
b_startAgent	<p>(Optional) Enter TRUE if you want the Management Agent to start automatically once it is installed and configured. Otherwise, enter FALSE.</p> <p>For example, b_startAgent=TRUE</p> <p>If you do not include this parameter, it defaults to TRUE.</p>
ORACLE_HOSTNAME	<p>(Optional) Enter the fully qualified domain name of the host where you want to install the Management Agent.</p> <p>For example, ORACLE_HOSTNAME=example.com</p> <p>If you do not include this parameter, it defaults to the physical host name.</p>

Table 6–3 (Cont.) Creating a Response File for Installing Oracle Management Agent Using agentDeploy Script

Parameter	Description
ALLOW_IPADDRESS	<p>(Optional) Enter TRUE if you want to specify an IP address for ORACLE_HOSTNAME. If ALLOW_IPADDRESS is set to FALSE, a prerequisite check fails when you specify an IP address for ORACLE_HOSTNAME while installing a Management Agent.</p> <p>For example, ALLOW_IPADDRESS=TRUE</p> <p>If you do not include this parameter, it defaults to FALSE.</p>
START_PRIORITY_LEVEL (For Unix based hosts only)	<p>(Optional) Use this parameter to specify the priority level of the Management Agent service when the host is started. This parameter accepts values between 0 and 99. However, Oracle recommends that you provide a value between 91 and 99 for this parameter.</p> <p>For example, START_PRIORITY_LEVEL=95</p> <p>If you do not include this parameter, it defaults to 98.</p>
SHUT_PRIORITY_LEVEL (For Unix based hosts only)	<p>(Optional) Use this parameter to specify the priority level of the Management Agent service when the host is shut down. This parameter accepts values between 0 and 99.</p> <p>For example, SHUT_PRIORITY_LEVEL=25</p> <p>If you do not include this parameter, it defaults to 19.</p>
PROPERTIES_FILE	<p>(Optional) Use this parameter to specify the absolute location of the properties file.</p> <p>For example, PROPERTIES_FILE=/tmp/agent.properties</p> <p>In the properties file, specify the parameters that you want to use for the Management Agent deployment. The list of parameters that you can specify in the properties file is present in \$<AGENT_INSTANCE_HOME>/sysman/config/emd.properties. In the properties file, you must specify the parameters in name value pairs, for example:</p> <p>REPOSITORY_PROXYHOST=abc.example.com</p> <p>REPOSITORY_PROXYPORT=1532</p> <p>The properties file does not support parameter values that have spaces. If the value of a particular parameter contains a space, then run the following command after deploying the Management Agent:</p> <p>\$<AGENT_INSTANCE_HOME>/bin/emctl setproperty agent -name <parameter_name> -value <parameter_value></p>
s_agentHomeName	<p>(Optional) Enter the name of the Oracle home you want to see created for the Management Agent.</p> <p>For example, s_agentHomeName=agent12cR2</p> <p>If you do not include this parameter, it defaults to agent12cn, where n is 1 for the first Management Agent installed on the host, 2 for the second Management Agent installed on the host, and so on.</p> <p>Note: Ensure that the name you enter consists of only alphanumeric characters, and is not more than 128 characters long.</p>

Table 6–3 (Cont.) Creating a Response File for Installing Oracle Management Agent Using agentDeploy Script

Parameter	Description
s_agentSvcName (Only for Microsoft Windows hosts)	<p>(Optional) Enter the customized Management Agent service name.</p> <p>For example, s_agentSvcName=agentsrvcl</p> <p>If you do not include this parameter, it defaults to Oracle+<oracle_home_name>+Agent.</p> <p>Note: (For Microsoft Windows hosts) If you upgrade a 12.1.0.x Management Agent installed on a host and you want to install another Management Agent on the same host, which points to a different OMS, specify the s_agentSvcName parameter while installing the Management Agent.</p>

6.4.6 Creating a Response File for Installing Using an RPM File

Table 6–4 describes the various parameters you can include in the agent.properties response file while installing a Management Agent using a .rpm file.

Table 6–4 Creating a Response File for Installing Oracle Management Agent Using an RPM File

Parameter	Description
OMS_HOST	<p>(Mandatory) Enter the host name of the OMS to which you want to connect.</p> <p>For example, OMS_HOST=example.com</p>
OMS_PORT	<p>(Mandatory) Enter the upload port (HTTP or HTTPS) to communicate with the OMS.</p> <p>For example, OMS_PORT=1835</p>
AGENT_REGISTRATION_PASSWORD	<p>(Mandatory) Enter a password for registering new Management Agents that join the Enterprise Manager system.</p> <p>By default, the communication between the OMS and the Management Agents is secured and locked. Any new Management Agents that join the Enterprise Manager system must be authenticated before they become part of the system. The password you enter here will be used for authenticating those new Management Agents.</p> <p>For example, AGENT_REGISTRATION_PASSWORD=We1456come</p>
AGENT_USERNAME	<p>(Mandatory) Enter the user name with which you want to install the Management Agent.</p> <p>For example, AGENT_USERNAME=oracle</p>
AGENT_GROUP	<p>(Mandatory) Enter the group to which the Management Agent user should belong.</p> <p>For example, AGENT_GROUP=dba</p>
AGENT_PORT	<p>(Optional) Enter the port used for the Management Agent process.</p> <p>For example, AGENT_PORT=1832</p> <p>If you do not enter any value, then either 3872 or any free port between 1830 and 1849 is honored.</p>

Table 6–4 (Cont.) Creating a Response File for Installing Oracle Management Agent Using an RPM File

Parameter	Description
ORACLE_HOSTNAME	(Only for Virtual Hosts) Enter the virtual host name where you want to install the Management Agent. For example, ORACLE_HOSTNAME=example.com

6.4.7 Understanding the Options Supported by the AgentPull Script

Table 6–5 lists the options supported by the AgentPull.sh script. On Microsoft Windows, these options apply to the AgentPull.bat file.

Table 6–5 Understanding the Options Supported by AgentPull.sh/AgentPull.bat

Option	Description
-download_only	Only downloads the Management Agent software. Does not deploy the Management Agent.
-showPlatforms	Displays the platforms for which the Management Agent software is available on the OMS host. Does not install the Management Agent.
-help	Displays command line help and describes the usage of the AgentPull.sh script.

6.4.8 Understanding the Options Supported by the agentDeploy Script

Table 6–6 lists the options supported by the agentDeploy.sh script. On Microsoft Windows, these options apply to the agentDeploy.bat file.

Table 6–6 Understanding the Options Supported by agentDeploy.sh/agentDeploy.bat

Option	Description
-prereqOnly	Runs only the prerequisite checks. Does NOT actually install the Management Agent. This option is useful when you want to verify whether your environment meets all the prerequisites for a successful Management Agent installation.
-ignorePrereqs	Skips running the prerequisite checks. Use this when you have already used the -prereqOnly option and verified the prerequisites, and only want to install the software binaries.
-invPtrLoc	Considers the Oracle Inventory directory for storing inventory details. Enter the absolute path to the oraInst.loc file that contains the location of the OraInventory directory. Important: If you enter a value for this option, do NOT use the INVENTORY_LOCATION option. Also note that this parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.

Table 6–6 (Cont.) Understanding the Options Supported by

Option	Description
INVENTORY_LOCATION	<p>Considers the Oracle Inventory directory for storing inventory details. Enter the absolute path to the OraInventory directory.</p> <p>Important:</p> <ul style="list-style-type: none"> ■ If you enter a value for this option, do NOT use the <code>-invPtrLoc</code> option. ■ Do NOT use this option if you already have the <code>/var/opt/oracle/oraInst.loc</code> on HP and Solaris platforms, and <code>/etc/oraInst.loc</code> file on all other UNIX platforms. ■ This parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
-help	Displays command line help and describes the usage of the deployment script.
-debug	Logs more debug messages useful for debugging and resolving errors.
-ignoreUnzip	Skips extracting the software binaries of the Management Agent software. Use this when you do not want to copy the binaries again, but only want to configure the available binaries.
-softwareOnly	<p>Installs only the software binaries, and does NOT configure the installation. Use this when you want to perform a software-only installation of the Management Agent. For more information, see Chapter 9.</p> <p>Note: This option does not apply if you are cloning using a ZIP file.</p>
-configOnly	<p>Configures the software binaries, and does not install any software binaries. Use this when you have performed a software-only installation using the <code>-softwareOnly</code> option, so that only the configuration is done to the copied software binaries. For more information, see Chapter 9.</p> <p>Note: This option does not apply if you are cloning using a ZIP file.</p>
-forceConfigure	<p>Forcefully configures the Management Agent even when the OMS is unreachable. Use this option only when you are installing the Management Agent before installing the OMS, and when you know for sure that you will install the OMS later on the same host and port mentioned for the parameters <code>OMS_HOST</code> and <code>EM_UPLOAD_PORT</code>, respectively, in the response file you pass.</p> <p>If you pass this option, then do not pass <code>-configOnly</code>, <code>-softwareOnly</code>, and <code>-prereqOnly</code>.</p> <p>Note: When you pass this option, the Management Agent is configured to use HTTP (non-secure) communication. To establish a secure HTTPS communication between the Management Agent and the OMS, you must manually secure the Management Agent after the OMS is available.</p>

6.4.9 Understanding the Contents of the Downloaded Management Agent Software

[Table 6–7](#) describes the contents of the core Management Agent software you download before installing the Management Agent using the `agentDeploy` script.

Table 6–7 Contents of the Downloaded Management Agent Software

Files	Description
12.1.0.3.0_PluginsOneoffs_<platform id>.zip	Plug-in ZIP file containing all the discovering plug-ins, which were installed with the OMS, Oracle Home discovery plug-in, and Oracle Home monitoring plug-in.
agentcoreimage.zip	Archived ZIP file containing the core agent bits and agent set-uid binaries.
agentDeploy.sh/agentDeploy.bat	Script used for deploying the Management Agent.
unzip	Utility used for unarchiving the ZIP files.
agentimage.properties	Properties file used for getting the version, platform ID, and so on.
agent.rsp	Response file to be edited and passed for installing the Management Agent.

6.4.10 Understanding the Contents of the Management Agent RPM File

If you choose to install a Management Agent using the .rpm file, the .rpm file you download contains an agent base directory. [Table 6–8](#) describes the contents of this agent base directory:

Table 6–8 Contents of the Agent Base Directory Present in RPM File

Element	Description
core/12.1.0.3.0	Contains the Management Agent software.
sbin	Contains the Management Agent binaries.
plugins.txt	Response file specifying the plug-ins deployed on the Management Agent.
plugins	Contains the plug-in software.
agentimage.properties	Properties file used for getting the version, platform ID, and so on.
agent.properties	Response file to be edited and passed for installing the Management Agent.
oracle-agt	Management Agent configuration script.

6.5 After You Install

After you install the Management Agent, follow these steps:

1. (Only for UNIX Operating Systems) Manually run the following scripts as a *root* user:

- If this is the first Oracle product you just installed on the host, then run the `oraInstroot.sh` script from the inventory location specified in the `oraInst.loc` file that is available in the Management Agent home. This location is also displayed when you run the `agentDeploy` script with the `-configOnly` option.

For example, if the inventory location specified is `$HOME/oraInventory`, then run the following command:

```
$HOME/oraInventory/oraInstRoot.sh
```

- Run the `root.sh` script from the Management Agent home:

```
$<AGENT_HOME>/root.sh
```

Note: You do not need to run the `oraInstroot.sh` and `root.sh` scripts if you are installing a Management Agent using a `.rpm` file.

2. Verify the installation:

- a. Navigate to the Management Agent home and run the following command to see a message that confirms that the Management Agent is up and running:

```
$<AGENT_INSTANCE_HOME>/bin/emctl status agent
```

- b. Navigate to the Management Agent home and run the following command to see a message that confirms that EMD upload completed successfully:

```
$<AGENT_INSTANCE_HOME>/bin/emctl upload agent
```

3. Verify whether all the plug-ins listed in `$<AGENT_BASE_DIRECTORY>/plugins.txt` were installed successfully. To do so, run the following command:

```
$<AGENT_INSTANCE_HOME>/bin/emctl listplugins agent -type all
```

4. If you had ignored a prerequisite check warning about wrong time zone settings, run the following command and follow the steps it displays:

```
$<AGENT_INSTANCE_HOME>/bin/emctl resetTZ agent
```

5. By default, the host and the Management Agent get automatically added to the Enterprise Manager Cloud Control console for monitoring. None of the targets running on that host get automatically discovered and monitored.

To monitor the other targets, you must add them to Enterprise Manager Cloud Control either using the Auto Discovery Results page, the Add Targets Manually page, or the discovery wizards offered for the targets you want to monitor.

For information about discovering targets in Enterprise Manager Cloud Control, refer to the chapter on adding targets in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

Note:

- If 12c (12.1.0.x) Management Agents hang frequently or do not respond on Solaris 9ux and 10ux operating systems, then refer to document ID 1427773.1 on My Oracle Support.
- You can repoint your existing Management Agents to a new Oracle Management Service (OMS). For information on how to do this, see the Redirecting Oracle Management Agent to Another Oracle Management Service Appendix present in *Oracle Enterprise Manager Cloud Control Advanced Installation Guide*.

When you repoint your existing Management Agents to a new OMS, you cannot move the targets monitored by the Management Agents, the target history, and the Management Agent history. The monitored targets and the history data is lost.

Cloning Oracle Management Agent

This chapter explains how you can clone an existing Oracle Management Agent (Management Agent). In particular, this section covers the following:

- [Overview](#)
- [Before You Begin](#)
- [Prerequisites](#)
- [Cloning Procedure](#)
- [After You Clone](#)

7.1 Overview

Oracle Management Agent (Management Agent) is one of the core components of Enterprise Manager Cloud Control that enables you to convert an unmanaged host to a managed host in the Enterprise Manager system. The Management Agent works in conjunction with the plug-ins to monitor the targets running on that managed host.

Therefore, if you want to monitor a target running on a host, you must first convert that unmanaged host to a managed host by installing an Oracle Management Agent, and then manually discover the targets running on it to start monitoring them.

However, the Management Agent you install using other installation types is always a fresh installation without any customized configuration that you had done or interim one-off patches that you had applied to other running Management Agents.

If you want to install an additional Management Agent that is identical to the existing well-tested, pre-patched, and running Management Agent, then the best option is to clone the existing instance. This saves time and effort in patching a fresh installation all over again and bringing it to the current state.

You can clone an existing Management Agent in graphical or silent mode.

- In graphical mode, you use the Add Host Targets Wizard that is accessible from within the Enterprise Manager Cloud Control console. The wizard enables you to select a source Management Agent, which you want to clone, and identify one or more remote hosts on which you want to clone it.

The wizard first copies the source Management Agent image to the host on which Oracle Management Service (OMS) is running, and then, it transfers that copied image to the destination hosts. Although the wizard can be used for remotely cloning one, single Management Agent, it is best suited for mass-deployment of Management Agents, particularly while mass-deploying Management Agents of different releases on hosts of different platforms.

- In silent mode, you use a compressed file (ZIP), which you transfer. Understandably, this is a much easier method because you compress the Oracle home of an existing Management Agent and transfer it to the destination host without having to specify any parameters or values in an interview screen, but still retaining all its configuration settings and applied one-off patches.

However, in silent mode, you can install only on one destination host at any given time. Once you are done with cloning of a Management Agent on a host, you must redo the procedure to clone on another host. Therefore, you cannot clone on multiple hosts simultaneously, and as a result, this approach is best suited when you want to clone only on a few hosts, one host after the other.

Understandably, as a prerequisite, you need to have at least one Management Agent in your environment, and its software binaries must be accessible from all the hosts where you want to clone an additional Management Agent. Therefore, note that this installation type must be used for installing only additional Management Agents in your environment.

After installing a Management Agent, to monitor a target, add the target to Enterprise Manager Cloud Control either using the Auto Discovery Results page, the Add Targets Manually page, or the discovery wizards offered for the targets you want to monitor.

For information about discovering targets in Enterprise Manager Cloud Control, refer to the chapter on adding targets in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

Once the installation is complete, you will see the following default contents in the agent base directory:

```
<agent_base_directory>
|____core
|    |____12.1.0.3.0
|    |____plugins
|    |____plugins.txt
|    |____agent_inst
|    |____sbin
|    |____agentimage.properties
```

Note: You can repoint your existing Management Agents to a new Oracle Management Service (OMS). For information on how to do this, see the Redirecting Oracle Management Agent to Another Oracle Management Service Appendix present in *Oracle Enterprise Manager Cloud Control Advanced Installation Guide*.

When you repoint your existing Management Agents to a new OMS, you cannot move the targets monitored by the Management Agents, the target history, and the Management Agent history. The monitored targets and the history data is lost.

7.2 Before You Begin

Before you begin installing an Oracle Management Agent, keep these points in mind:

- *(Only for Graphical Mode)* The Add Host Targets Wizard converts an unmanaged host to a managed host in the Enterprise Manager system by cloning an existing Oracle Management Agent.

- Oracle Management Agent 12c communicates only with Oracle Management Service 12c and not with any earlier release of Enterprise Manager.
- *(Only for Graphical Mode)* Using the Add Host Targets Wizard, you can clone only when the source host (from where you are cloning the Management Agent) and the destination host are running on the same operating system. Therefore, if you have hosts running on different platforms, then you must have one deployment session per platform.
- While cloning, the source Management Agent is not shut down.
- If the source Management Agent was installed using the Add Host Targets Wizard, or EM CLI, it is recommended that you clone this Management Agent in graphical mode.

If the source Management Agent that you want to clone was installed in silent mode, you can clone this Management Agent in either graphical mode or silent mode.

- *(Only for Graphical Mode)* If you have multiple hosts, sharing a common mounted drive, then install the Management Agents in two different phases:
 1. First, clone the Management Agent to the host where the drive is shared by selecting the deployment type **Clone Existing Agent** in the Add Host Targets Wizard. Follow the instructions outlined in this chapter.
 2. Then, install a Management Agent on all other hosts that access the shared, mounted drive by selecting the deployment type **Add Host to Shared Agent** in the Add Host Targets Wizard. (Here, you will select the Management Agent you installed in the previous step.) For more information, follow the instructions outlined in [Chapter 8](#).
- Cloning on shared clusters is NOT supported. If you have an Oracle RAC Cluster with multiple nodes, then you must clone the Management Agent on each of the nodes separately. In other words, in the Add Host Targets Wizard, you must add each node explicitly as a destination host.
- *(Only for Graphical Mode)* The Add Host Targets Wizard uses SSH to establish connectivity between Oracle Management Service (OMS) and the remote hosts where you want to install the Management Agents
- *(Only for Graphical Mode)* Only SSH1 (SSH version 1) and SSH2 (SSH version 2) protocols offered by OpenSSH are supported for deploying a Management Agent.
- *(Only for Graphical Mode)* The Add Host Targets Wizard supports Named Credentials that enable you to use a set of credentials registered with a particular name specifically for this operation, by your administrator. This ensures an additional layer of security for your passwords because as an operator, you can only select the named credential, which is saved and stored by an administrator, and not know the actual user name and password associated with it.

In case the named credential you select does not have the privileges to clone, then you can set the named credential to run as another user (locked user account). In this case, the wizard logs in to the hosts using the named credential you select, but clones using the locked user account you set.

For example, you can create a named credential titled User_A (the user account that has remote login access), and set it to run as User_X (the Management Agent install user account for which no direct login is set) that has the required privileges. In this case, the wizard logs in to the hosts as User_A, but installs as User_X, using the privilege delegation setting (sudo or PowerBroker) specified in the named credential.

- (Only for Graphical Mode) Named credentials support SSH public key authentication and password based authentication. So you can use an existing SSH public key authentication without exposing your passwords.

To set up SSH public key authentication for a named credential, follow these steps:

Note: If you have already set up SSH public key authentication for a named credential and the SSH keys are already created, upload the SSH keys to Enterprise Manager, as mentioned in Step 3 of the following procedure.

1. Navigate to the following location in the OMS home:

```
$<OMS_HOME>/oui/prov/resources/scripts
```

For example,

```
/home/software/em/middleware/oms/oui/prov/resources/scripts
```

2. If the OMS host runs on a Unix based operating system, run the following script on the OMS host as the OMS user, and pass the Management Agent install user name and the fully qualified name of the target hosts:

```
sshUserSetup.sh -setup -user <agent_install_user_name> -hosts  
<target_hosts>
```

The following SSH keys are created:

```
$HOME/.ssh/id_rsa  
$HOME/.ssh/id_rsa_pub
```

Here, \$HOME refers to the home directory of the OMS install user.

If the OMS host runs on Microsoft Windows, install Cygwin on the OMS host (described in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*), then run the following script on the OMS host as the OMS user, and pass the Management Agent install user name and the fully qualified name of the target hosts:

```
sshUserSetupNT.sh -setup -user <agent_install_user_name> -hosts  
<target_hosts>
```

3. Upload the SSH keys to Enterprise Manager.

From the **Setup** menu, select **Security**, then select **Named Credentials**. Click **Create**. For **Credential Name**, specify the credential name. For **Credential Type**, select **SSH Key Credentials**.

To upload one of the private SSH keys created in Step 2, in the Credential Properties section, specify the location of the private SSH key as a value for the **Upload Private Key** field. Click **Save**.

To upload one of the public SSH keys created in Step 2, in the Credential Properties section, specify the location of the public SSH key as a value for the **Upload Public Key** field. Click **Save**.

[Figure 7–1](#) describes how to upload SSH keys to Enterprise Manager.

Figure 7–1 Uploading SSH Keys to Enterprise Manager

The screenshot shows the 'Create Credential' window. Under 'General Properties', the 'Credential name' is 'oracle_ssh', 'Authenticating Target Type' is 'Host', and 'Credential type' is 'SSH Key Credentials'. Under 'Credential Properties', the 'UserName' is 'oracle', the 'SSH Private Key' is a long string of characters, and the 'SSH Public Key' is another long string. There are 'Upload Private Key' and 'Upload Public Key' buttons, each with a 'Browse...' link.

If you have already set up SSH public key authentication for a named credential, you can use the named credential while installing Management Agents using the Add Host Targets Wizard.

- By default, the Add Host Targets Wizard configures all the plug-ins that were configured with the Management Agent you are cloning.
- You must have *read* privileges on the Oracle WebLogic Server's alert log directories for the Support Workbench (Incident) metrics to work properly. You must also ensure that the Management Agent that is monitoring this Oracle WebLogic Server target is running on the same host as the Oracle WebLogic Server.

7.3 Prerequisites

Before cloning the Management Agent, ensure that you meet the following prerequisites.

Table 7–1 Prerequisites for Cloning Oracle Management Agent

Requirement	Description
Hardware Requirements	Ensure that you meet the hard disk space and physical memory requirements. For more information, see the chapter on hardware requirements in the <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i> .
Software Requirements (Only for Graphical Mode)	<p>(For Microsoft Windows) Ensure that you have installed Cygwin 1.7 on the destination host. For more information, see the chapter on installing Cygwin in the <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>.</p> <p>Note: While running <code>cygwin.bat</code> in Microsoft Windows Server 2008 and Microsoft Windows Vista, ensure that you invoke it in administrator mode. To do this, right-click the <code>cygwin.bat</code> file and select Run as administrator.</p>

Table 7–1 (Cont.) Prerequisites for Cloning Oracle Management Agent

Requirement	Description
Operating System Requirements	<p>Ensure that you install the Management Agent only on certified operating systems as mentioned in the Enterprise Manager certification matrix available on <i>My Oracle Support</i>.</p> <p>To access the Enterprise Manager certification matrix, follow the steps outlined in <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>.</p> <p>For information about platforms receiving future support, refer to <i>My Oracle Support</i> note 793512.1.</p> <p>Note: If you use Oracle Solaris 10, then ensure that you have update 9 or higher installed. To verify whether it is installed, run the following command:</p> <pre>cat /etc/release</pre> <p>You should see the output similar to the following. Here, <code>s10s_u6</code> indicates that update 6, which is not a supported update level for installation, is installed.</p> <pre>Solaris 10 10/08 s10s_u6wos_07b SPARC</pre>
Package Requirements	<p>Ensure that you install all the operating system-specific packages. For more information, see the chapter on package requirements in the <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>.</p>
User and Operating System Group Requirement	<p>Ensure that the destination host where you want to install the Management Agent has the appropriate users and operating system groups created.</p> <p>For more information, see the chapter on creating operating system groups and users in the <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>.</p>
/etc/hosts File Requirements	<p>Ensure that the <code>/etc/hosts</code> file on the host has the IP address, the fully qualified name, and the short name in the following format:</p> <pre>172.16.0.0 example.com mypc</pre>
Destination Host Requirements	<p>Ensure that the destination hosts are accessible from the host where the OMS is running.</p> <p>If the destination host and the host on which OMS is running belong to different network domains, then ensure that you update the <code>/etc/hosts</code> file on the destination host to add a line with the IP address of that host, the fully qualified name of that host, and the short name of the host.</p> <p>For example, if the fully-qualified host name is <code>example.com</code> and the short name is <code>mypc</code>, then add the following line in the <code>/etc/hosts</code> file:</p> <pre>172.16.0.0 example.com mypc</pre>
Destination Host Credential Requirements (Only for Graphical Mode)	<p>Ensure that all the destination hosts running on the same operating system have the same set of credentials. For example, all the destination hosts running on Linux operating system must have the same set of credentials.</p> <p>The wizard installs the Management Agent using the same user account. If you have hosts running on the same operating system but with different credentials, then have two different deployment sessions.</p>

Table 7–1 (Cont.) Prerequisites for Cloning Oracle Management Agent

Requirement	Description
Destination Host Time Zone Requirements (Only for Graphical Mode)	<p>Ensure that the time zones of the destination hosts have been set correctly. To verify the time zone of a destination host, log in to the OMS host, and run the following command:</p> <pre>ssh -l <install_user> <destination_host_name> /bin/sh -c 'echo \$TZ'</pre> <p>If the time zone displayed is incorrect, log in to the destination host, and follow these steps:</p> <ol style="list-style-type: none"> Run the following commands to set the time zone on the destination host: <ul style="list-style-type: none"> For Korn shell: <pre>TZ=<value> export TZ</pre> For Bourne shell or Bash shell: <pre>export TZ=<value></pre> For C shell: <pre>setenv TZ <value></pre> <p>For example, in the Bash shell, run the following command to set the time zone to America/New_York:</p> <pre>export TZ='America/New_York'</pre> <p>To set the time zone on a destination host that runs on Microsoft Windows, from the Start menu, select Control Panel. Click Date and Time, then select the Time Zone tab. Select your time zone from the displayed drop down list.</p> <p>To view a list of the time zones you can use, access the <code>supportedtzs.lst</code> file present in the <code><AGENT_HOME>/sysman/admin</code> directory of the central agent (that is, the Management Agent installed on the OMS host).</p> <ol style="list-style-type: none"> Restart the SSH daemon. <p>If the destination host runs on a UNIX based operating system, run the following command:</p> <pre>sudo /etc/init.d/sshd restart</pre> <p>If the destination host runs on a Microsoft Windows operating system, run the following commands:</p> <pre>cygrunsrv -E sshd cygrunsrv -S sshd</pre> Verify whether the SSH server can access the TZ environment variable by logging in to the OMS host, and running the following command: <pre>ssh -l <install_user> <destination_host_name> /bin/sh -c 'echo \$TZ'</pre> <p>Note: If you had ignored a prerequisite check warning about wrong time zone settings during the cloning procedure, you must set the correct time zone on the destination hosts after cloning the Management Agent. For information on setting time zones post cloning, see Section 7.5.</p>

Table 7–1 (Cont.) Prerequisites for Cloning Oracle Management Agent

Requirement	Description
Time Zone Requirements (Only for Silent Mode)	<p>Ensure that the host time zone has been set correctly. To verify the host time zone, run the following command:</p> <pre>echo \$TZ</pre> <p>If the time zone displayed is incorrect, run the following commands, before running the <code>agentDeploy.sh</code> or <code>agentDeploy.bat</code> scripts, to set the correct time zone:</p> <ul style="list-style-type: none"> For Korn shell: <pre>TZ=<value> export TZ</pre> For Bourne shell or Bash shell: <pre>export TZ=<value></pre> For C shell: <pre>setenv TZ <value></pre> <p>For example, in the Bash shell, run the following command to set the time zone to America/New_York:</p> <pre>export TZ='America/New_York'</pre> <p>To set the time zone on a destination host that runs on Microsoft Windows, from the Start menu, select Control Panel. Click Date and Time, then select the Time Zone tab. Select your time zone from the displayed drop down list.</p> <p>To view a list of the time zones you can use, access the <code>supportedtzs.lst</code> file present in the <code><AGENT_HOME>/sysman/admin</code> directory of the central agent (that is, the Management Agent installed on the OMS host).</p> <p>Note:</p> <ul style="list-style-type: none"> If you are installing a Management Agent on a host that runs on Microsoft Windows Server 2003, and you encounter an error when you use the Asia/Kolkata time zone, see the My Oracle Support note 1530571.1. If you had ignored a prerequisite check warning about wrong time zone settings during the cloning procedure, you must set the correct time zone on the host after cloning the Management Agent. For information on setting time zones post cloning, see Section 7.5. <p>Note: If you had ignored a prerequisite check warning about wrong time zone settings during the cloning procedure, you must set the correct time zone on the host after cloning the Management Agent. For information on setting time zones post cloning, see Section 7.5.</p>

Table 7–1 (Cont.) Prerequisites for Cloning Oracle Management Agent

Requirement	Description
sudo/pbrun/sesu/su SSH Requirements (Only for Graphical Mode)	<p>(Only for UNIX)</p> <p>Ensure that you set the <code>oracle.sysman.prov.agentpush.enablePty</code> property to true in the <code>\$(OMS_HOME)/sysman/prov/agentpush/agentpush.properties</code> file, if the privilege delegation tool you are using requires a pseudo terminal for remote command execution via SSH. Most privilege delegation tools such as <code>pbrun</code>, <code>sesu</code>, and <code>su</code> require a pseudo terminal for remote command execution, by default.</p> <p>Note: If you are using <code>sudo</code> as your privilege delegation tool, and you do not want to set the <code>oracle.sysman.prov.agentpush.enablePty</code> property to true, do one of the following:</p> <ul style="list-style-type: none"> ■ Include Defaults <code>visiblepw</code> in the <code>/etc/sudoers</code> file, or enter the <code>sudo</code> command with the <code>-S</code> option for Privileged Delegation Setting on the Installation Details page. For information on how to access the Installation Details page, see Section 7.4.1. ■ Comment out Defaults <code>requiretty</code> in the <code>/etc/sudoers</code> file.
sudo/pbrun/sesu/su Requirements (for Root User) (Only for Graphical Mode)	<p>(Only for UNIX)</p> <ul style="list-style-type: none"> ■ Ensure that the installing user has the privileges to invoke the <code>id</code> command and the <code>agentdeployroot.sh</code> script as <code>root</code>. Grant the privileges in the configuration file of your privilege delegation tool. For example, if you are using <code>sudo</code> as your privilege delegation tool, include the following in the <code>/etc/sudoers</code> file to grant the required privileges: <pre><install_user> ALL=(root) /usr/bin/id, <agent_home> /*/agentdeployroot.sh</pre> For example, <code>oracle</code> <code>ALL=(root) /usr/bin/id, /home/oracle/agentibd/*/*agentdeployroot.sh</code> Here, <code>oracle</code> is the installing user, and <code>/home/oracle/agentibd</code> is the Management Agent home, that is, the agent base directory. ■ You do not require the following entry in the <code>/etc/sudoers</code> file for installing a Management Agent. However, the entry is required for performing provisioning and patching operations in Enterprise Manager. Therefore, if you are removing this entry before installing a Management Agent, then ensure that you bring back the entry after installing the Management Agent. In Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2) or Release 3 (12.1.0.3): <pre>(root) /<AGENT_BASE_DIRECTORY>/sbin/nmosudo</pre> In Enterprise Manager Cloud Control 12c Release 1 (12.1.0.1) [with Bundle Patch 1]: <pre>(root) /<AGENT_INSTANCE_DIRECTORY>/bin/nmosudo</pre>

Table 7–1 (Cont.) Prerequisites for Cloning Oracle Management Agent

Requirement	Description
sudo/pbrun/sesu/su Requirements (for Locked Account User) <i>(Only for Graphical Mode)</i>	<p><i>(Only for UNIX)</i></p> <p>Ensure that the installing user has the privileges to invoke <code>/bin/sh</code> as the locked account user. Grant the privileges in the configuration file of your privilege delegation tool.</p> <p>For example, if you are using <code>sudo</code> as your privilege delegation tool, include the following in the <code>/etc/sudoers</code> file to grant the required privileges:</p> <pre>login_user1 ALL=(oracle) /bin/sh</pre> <p>Here, <code>login_user1</code> is the SSH log in user, and <code>oracle</code> is the locked account and install user.</p> <p>If you do not want to grant privileges to the installing user to invoke <code>/bin/sh</code> as the locked account user, set the <code>oracle.sysman.prov.agentpush.pdpShellOutEnabled</code> property to <code>false</code>, and ensure that the installing user has the privileges to invoke <code>id</code>, <code>chmod</code>, <code>cp</code>, <code>mkdir</code>, <code>rm</code>, <code>tar</code>, <code>emctl</code>, <code>agentDeploy.sh</code>, <code>runInstaller</code>, and <code>unzip</code> as the locked account user. Grant the privileges in the configuration file of your privilege delegation tool.</p> <p>For example, if you are using <code>sudo</code> as your privilege delegation tool, include the following in the <code>/etc/sudoers</code> file to grant the required privileges:</p> <pre>login_user1 ALL=(oracle) /usr/bin/id, /bin/chmod, /bin/cp, /bin/mkdir, /bin/rm, /bin/tar, /home/oracle/agentibd/agent_inst/bin/emctl, /home/oracle/agentibd/*/agentDeploy.sh, /home/oracle/agentibd/*/prereq_stage/core/12.1.0.3.0/oui/bin/runInstaller, /home/oracle/agentibd/*/unzip, /home/oracle/agentibd/*/unzipTmp/unzip</pre> <p>Here, <code>login_user1</code> is the SSH log in user, <code>oracle</code> is the locked account and install user, and <code>/home/oracle/agentibd</code> is the agent base directory.</p>
Permission Requirements	<ul style="list-style-type: none"> ■ Ensure that the agent base directory you specify is empty and has <i>write</i> permission. ■ Ensure that the instance directory is empty and has <i>write</i> permission.
PATH Environment Variable Requirements <i>(Only for Graphical Mode)</i>	<p>On the destination host, ensure the following:</p> <ul style="list-style-type: none"> ■ <i>(For Microsoft Windows)</i> Ensure that the Cygwin software location appears before other software locations in the <code>PATH</code> environment variable. After making it the first entry, restart the SSH daemon (<code>sshd</code>). ■ <i>(For UNIX)</i> On the destination host, ensure that the SCP binaries (for example, <code>/usr/bin/scp</code>) are in the <code>PATH</code> environment variable:
Path Validation Requirements	<p>Validate the path to all command locations. For more information, see the appendix on validating command locations in the <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>.</p>
CLASSPATH Environment Variable Requirements	<p>Unset the <code>CLASSPATH</code> environment variable. You can always reset the variable to the original value after the installation is complete.</p>

Table 7–1 (Cont.) Prerequisites for Cloning Oracle Management Agent

Requirement	Description
Temporary Directory Space Requirements	<p>Ensure that you allocate 400 MB of space for a temporary directory where the executables can be copied.</p> <p>By default, the temporary directory location set to the environment variable <code>TMP</code> or <code>TEMP</code> is honored. If both are set, then <code>TEMP</code> is honored. If none of them are set, then the following default values are honored: <code>/tmp</code> on UNIX hosts and <code>c:\Temp</code> on Microsoft Windows hosts.</p>
Agent Base Directory Requirements	<p>Ensure that the agent base directory is empty and has at least 1 GB of free space.</p> <p>Ensure that the directory name does not contain any spaces.</p> <p>Ensure that the installing user owns the agent base directory. Ensure that the installer user or the root user owns all the parent directories. Ensure that the root user owns the root directory.</p> <p>For example, if the agent base directory is <code>/scratch/OracleHomes/agent</code>, and <code>oracle</code> is the installing user, then the <code>/scratch/OracleHomes/agent</code> directory must be owned by <code>oracle</code>, directories <code>scratch</code> and <code>OracleHomes</code> must be owned by either <code>oracle</code> or <code>root</code> user, and the root directory (<code>/</code>) must be owned by <code>root</code> user.</p> <p>If the agent base directory is mounted, then ensure that it is mounted with the <code>setuid</code> turned on.</p>
Default SSH Port Requirements (Only for Graphical Mode)	<p>Ensure that the SSH daemon is running on the default port (that is, 22) on all the destination hosts. To verify the SSH port on a Unix host, run the following command:</p> <pre>netstat -anp grep -i sshd</pre> <p>For example, the output of this command may be the following:</p> <pre>tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 3188/sshd</pre> <p>The above output indicates that the SSH daemon is running on port 22.</p> <p>Also, on a Unix host, you can run the following command to verify the SSH port:</p> <pre>cat /etc/ssh/sshd_config</pre> <p>For a Microsoft Windows host, the SSH port value is mentioned in the <code>C:\cygwin\etc\sshd_config</code> file.</p> <p>If the SSH port is a non-default port, that is, any port other than 22, then update the <code>SSH_PORT</code> property in the following file:</p> <pre>\$<OMS_HOME>/oui/prov/resources/Paths.properties</pre>
Software Availability Requirements (Only for Graphical Mode)	<p>For Cloning an Existing Management Agent</p> <p>Ensure that you already have Oracle Management Agent 12c running in your environment. Ensure that the platform on which it is running is the same as the platform of the destination hosts on which you want to clone.</p> <p>For Installing a Management Agent Using Shared Oracle Home</p> <p>Ensure that you already have Oracle Management Agent 12c installed as a <i>Master Agent</i> in a shared, mounted location.</p>
Installation Base Directory Requirements (Only for Graphical Mode)	<p>Ensure that the agent base directory you specify in the Installation Base Directory field is empty and has <i>write</i> permission.</p>

Table 7–1 (Cont.) Prerequisites for Cloning Oracle Management Agent

Requirement	Description
Job System Requirements	Ensure that the job system is enabled on the source Management Agent you want to clone.
Installing User Requirements	<p>If the central inventory owner and the user installing the Management Agent are different, then ensure that they are part of the same group.</p> <p>Also ensure that the inventory owner and the group to which the owner belongs have <i>read</i> and <i>write</i> permissions on the inventory directory.</p> <p>For example, if the inventory owner is <i>abc</i> and the user installing the Management Agent is <i>xyz</i>, then ensure that <i>abc</i> and <i>xyz</i> belong to the same group, and they have read and write access to the inventory.</p>
Central Inventory (oraInventory) Requirements	<ul style="list-style-type: none"> ■ Ensure that you allocate 100 MB of space for the Central Inventory. ■ Ensure that the central inventory directory is not in a shared file system. If it is already in a shared file system, then create a new inventory in a non-shared file system. You can optionally migrate the products that were previously installed in the shared file system to this new inventory in the non-shared file system. ■ Ensure that you have <i>read</i>, <i>write</i>, and <i>execute</i> permissions on oraInventory on all remote hosts. If you do not have these permissions on the default inventory (typically at <code>/etc/oraInst.loc</code>) on any remote host, then ensure that you specify the path to an alternative inventory location by using one of the following options in the Additional Parameters field of the Add Host Targets Wizard. However, these parameters are supported only on UNIX platforms, and not on Microsoft Windows platforms. <pre>INVENTORY_LOCATION=<absolute_path_to_inventory_directory> -invPtrLoc <absolute_path_to_oraInst.loc></pre>
Port Requirements	Ensure that the default ports described in Section 2.1.9.1 are free.
Agent User Account Permissions and Rights (Only for Microsoft Windows)	<p>(For Microsoft Windows) If you are installing the Management Agent on a Microsoft Windows-based operating system, then ensure that the agent user account has permissions and rights to perform the following:</p> <ul style="list-style-type: none"> ■ Act as part of the operating system. ■ Adjust memory quotas for a process. ■ Replace process level token. ■ Log in as a batch job. <p>To verify whether the agent user has these rights, follow these steps:</p> <ol style="list-style-type: none"> 1. Launch the Local Security Policy. From the Start menu, click Settings and then select Control Panel. From the Control Panel window, select Administrative Tools, and from the Administrative Tools window, select Local Security Policy. 2. In the Local Security Policy window, from the tree structure, expand Local Policies, and then expand User Rights Assignment.

Table 7–1 (Cont.) Prerequisites for Cloning Oracle Management Agent

Requirement	Description
Permissions for cmd.exe	<p>(For Microsoft Windows) If you are installing the Management Agent on a Microsoft Windows-based operating system, then ensure that you grant the <code>cmd.exe</code> program <i>Read</i> and <i>Execute</i> permissions for the user account that the batch job runs under. This is a restriction from Microsoft.</p> <p>For more information on this restriction and to understand how you can grant these permissions, access the following URL to Microsoft Web site:</p> <p>http://support.microsoft.com/kb/867466/en-us</p>
Preinstallation/Postinstallation Scripts Requirements (Only for Graphical Mode)	<p>Ensure that the preinstallation and postinstallation scripts that you want to run along with the installation are available either on the OMS host, destination hosts, or on a shared location accessible to the destination hosts.</p>
Browser Requirements (Only for Graphical Mode)	<ul style="list-style-type: none"> ■ Ensure that you use a certified browser as mentioned in the Enterprise Manager certification matrix available on <i>My Oracle Support</i>. <p>To access the Enterprise Manager certification matrix, follow the steps outlined in <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>.</p> <ul style="list-style-type: none"> ■ If you use Microsoft Internet Explorer 8 or 9, do the following: <ul style="list-style-type: none"> ■ Turn off the compatibility view mode. To do so, in Microsoft Internet Explorer, from the Tools menu, click Compatibility View to disable it if it is enabled. Also, click Compatibility View Settings and deregister the Enterprise Manager Cloud Control console URL. ■ Enable XMLHTTP. To do so, from the Tools menu, click Internet Options. Click the Advanced tab, and under the Security heading, select Enable native XMLHTTP support to enable it.

7.4 Cloning Procedure

This section describes the following:

- [Cloning in Graphical Mode](#)
- [Cloning in Silent Mode](#)

7.4.1 Cloning in Graphical Mode

To clone a Management Agent in graphical mode, follow these steps:

1. In Cloud Control, do one of the following:
 - From the **Setup** menu, select **Add Target**, and then, click **Auto Discovery Results**. On the Auto Discovery Results page, select a host you want to monitor in Enterprise Manager Cloud Control, and click **Promote**.

Enterprise Manager Cloud Control displays the Add Host Wizard, where you can select the option to clone an existing Management Agent.

- From the **Setup** menu, select **Add Target**, and then, click **Add Targets Manually**. On the Add Targets Manually page, select **Add Host Targets** and click **Add Host**.

Enterprise Manager Cloud Control displays the Add Host Wizard, where you can select the option to clone an existing Management Agent.

2. On the Host and Platform page, do the following:
 - a. Accept the default name assigned for this session or enter a unique name of your choice. The custom name you enter can be any intuitive name, and need not necessarily be in the same format as the default name. For example, `add_host_operation_1`

A unique deployment activity name enables you to save the cloning details specified in this deployment session and reuse them in the future without having to enter all the details all over again in the new session.
 - b. Click **Add** to enter the fully qualified name and select the platform of the host on which you want to clone the Management Agent.

Note:

- Oracle recommends you to enter the fully qualified domain name of the host. For monitoring purpose, Enterprise Manager Cloud Control adds that host and the Management Agent with the exact name you enter here.
 - You must enter only one host name per row. Entering multiple host names separated by a comma is not supported.
 - You must ensure that the host name you enter does not have underscores.
-

Alternatively, you can click either **Load from File** to add host names stored in a file, or **Add Discovered Hosts** to add host names from a list of hosts discovered by Enterprise Manager. For information on how the host name entries must appear in the host file, see [Section 7.4.1.2](#).

Note: When you click **Add Discovered Hosts** and add hosts from a list of discovered hosts, the host's platform is automatically detected and displayed. The platform name is detected using a combination of factors, including hints received from automated discovery and the platform of the OMS host. This default platform name is a suggestion, so Oracle strongly recommends you to verify the platform details before proceeding to the next step.

As you can clone only if the source host and destination host are running on the same platform, set the platform for the first host in the first row of the table and from the **Platform** list, select **Same for All Hosts**. This will ensure that the platform name you selected for the first host is also set for the rest of the hosts in the table.

Note: If you are cloning a Management Agent on a platform that is different from the platform on which the OMS host is running, then ensure that the Management Agent software for that platform is available in Oracle Software Library (Software Library). If the Management Agent software for the required platform is not available in Software Library, acquire and apply the software using the Self Update console.

To access the Self Update Console, from the **Setup** menu, select **Extensibility**, then select **Self Update**. To acquire the latest Management Agent software, click **Agent Software**, select the required software, then click **Download**.

For more information on how to acquire and apply the Management Agent software for a platform using the Self Update console, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

- c. Click **Next**.
3. On the Installation Details page, do the following:
 - a. In the Deployment Type section, select **Clone Existing Agent**. Then, for **Select Target**, click the torch icon and select the Management Agent you want to clone.

Note: If you have multiple hosts sharing a common mounted drive, then install the Management Agents in two different phases:

1. In the Add Host Targets Wizard, select the deployment type **Clone Existing Agent**, and clone the Management Agent to the host where the drive is shared.
 2. In the Add Host Targets Wizard, select the deployment type **Add Host to Shared Agent**, and install a Management Agent on all other hosts that access the shared, mounted drive. (Here, you will select the Management Agent you cloned in the previous step as the master agent or shared agent.)
-

Figure 7–2 describes this step.

Figure 7–2 Cloning a Management Agent

Add Target

Host and Platform Installation Details Review

Add Host Targets : Installation Details

On this screen, select each row from the following table and provide the installation details in the Installation Details section.

☒ **Deployment Type**
Select the type of deployment you want to perform.

☐ Fresh Agent Install

☒ Clone Existing Agent

Select Target

☐ Add Host to Shared Agent

Platform	Agent Software Version	Hosts
----------	------------------------	-------

- b. From the table, select the first row that indicates the hosts grouped by their common platform name.

- c. In the Installation Details section, provide the installation details common to the hosts selected in Step 3 (b). For **Installation Base Directory**, enter the absolute path to the agent base directory where you want the software binaries, security files, and inventory files of the Management Agent to be copied.

For example, `/usr/home/software/oracle/agentHome`

If the path you enter does not exist, the application creates a directory at the specified path, and copies the Management Agent software binaries, security files, and inventory files there.

Note: The Installation Base Directory is essentially the agent base directory. Ensure that the directory you provide is empty. If a previously run deployment session had failed for some reason, then you might see an `ADATMP_<timestamp>` subdirectory in the installation base directory. In this case, either delete the subdirectory and start a new deployment session, or retry the failed session from the Add Host Status page.

- d. For **Instance Directory**, accept the default instance directory location or enter the absolute path to a directory of your choice where all Management Agent-related configuration files can be stored.

For example, `/usr/home/software/oracle/agentHome/agent_inst`

If you are entering a custom location, then ensure that the directory has write permission. Oracle recommends you to maintain the instance directory inside the installation base directory.

If the path you enter does not exist, the application creates a directory at the specified path, and stores all the Management Agent-related configuration files there.

- e. From **Named Credential** list, select an appropriate profile whose credentials can be used for setting up the SSH connectivity between the OMS and the remote hosts, and for installing a Management Agent on each of the remote hosts.

Note:

- If you do not have a credential profile, or if you have one but do not see it in the **Named Credential** list, then click the plus icon against this list. In the Create New Named Credential window, enter the credentials and store them with an appropriate profile name so that it can be selected and used for installing the Management Agents. Also set the run privilege if you want to switch over from the Named Credential you are creating, to another user who has the privileges to perform the installation.
 - If the plus icon is disabled against this list, then you do not have the privileges to create a profile with credentials. In this case, contact your administrator and either request him/her to grant you the privileges to create a new profile or request him/her to create a profile and grant you the access to view it in the **Named Credential** list.
 - If you have manually set up SSH public key authentication between the OMS and the remote hosts, then you may not have a password for your user account. In this case, create a named credential with a dummy password. Do NOT leave the password field blank.
-

- f. For **Privileged Delegation Setting**, validate the Privilege Delegation setting to be used for running the root scripts. By default, it is set to the Privilege Delegation setting configured in Enterprise Manager Cloud Control.

For example, you can specify one of the following for the **Privileged Delegation Setting** field:

```
/usr/bin/sudo -u %RUNAS% %COMMAND%
/usr/bin/sesu - %RUNAS% -c "%COMMAND%"
/usr/bin/pbrun %PROFILE% -u %RUNAS% %COMMAND%
/usr/bin/su - %RUNAS% -c "%COMMAND%"
```

If you leave the **Privileged Delegation Setting** field blank, the root scripts will not be run by the wizard; you will have to run them manually after the installation. For information about running them manually, see [Section 7.5](#).

This setting will also be used for performing the installation as the user set in the Run As attribute of the selected Named Credential if you had set the user while creating that Named Credential.

Note: In the Privilege Delegation setting, the %RUNAS% is honored as the root user for running the root scripts and as the user set in the Run As attribute of the Named Credential for performing the installation.

- g. For **Port**, accept the default port (3872) that is assigned for the Management Agent to communicate, or enter a port of your choice.

The custom port you enter must not be busy. If you are not sure, you can leave this field blank. Enterprise Manager Cloud Control automatically assigns the first available free port within the range of 1830 - 1849.

- h. (Optional) In the Optional Details section, enter the absolute path to an accessible location where the preinstallation and postinstallation scripts you

want to run are available. Note that only one preinstallation or one postinstallation script can be specified.

If you want to run the script as **root**, then select **Run as Root**. If the script is on the host where OMS is running and is not on the host where you want to install the Management Agent, then select **Script on OMS**. In this case, the script will be copied from the OMS host to the destination hosts, and then run on the destination hosts.

- i. (Optional) For **Additional Parameters**, enter a whitespace-separate list of additional parameters that you want to pass during the installation. For a complete list of supported additional parameters, see [Table 7-2](#).

For example, if you want to provide the inventory pointer location file, then enter `-invPtrLoc` followed by the absolute path to the file location. Note that this parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.

- j. Repeat Step 3 (b) to Step 3 (i) for every other row you have in the table.
- k. Click **Next**.

4. On the Review page, review the details you have provided and if you are satisfied with the details, then click **Deploy Agent** to clone the Management Agent.

If you want to modify the details, then click **Back** repeatedly to reach the page where you want to make the changes.

When you click **Deploy Agent** and submit the deployment session, you are automatically taken to the Add Host Status page that enables you to monitor the progress of the deployment session.

Note: On the Add Host Status page, if you see the error message *Copying Source Agent Image Failed*, then refer to the following log file in the OMS home:

```
$<OMS_
HOME>/sysman/prov/agentpush/<timestampdir>/applogs/deployfwk
.log
```

This error usually occurs when the job system is not enabled on the source Management Agent you are cloning. Ensure that the job system is enabled.

7.4.1.1 Supported Additional Parameters

[Table 7-2](#) lists the additional parameters supported for cloning a Management Agent in graphical mode.

Table 7-2 Supported Additional Parameters

Parameter	Description
INVENTORY_LOCATION	<p>Enter the absolute path to the Central Inventory (oraInventory). For example, <code>INVENTORY_LOCATION=\$HOME/oraInventory</code></p> <p>Note: This parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.</p> <p>This parameter will be used only when the Central Inventory pointer <code>/etc/oraInst.loc</code> (or <code>/var/opt/oracle/oraInst.loc</code>) does not exist.</p>

Table 7–2 (Cont.) Supported Additional Parameters

Parameter	Description
-invPtrLoc	<p>Enter the absolute path to the inventory file that has the location of the Central Inventory (oraInventory).</p> <p>For example, <code>-invPtrLoc /tmp/oraInst.loc</code></p> <p>Note: This parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.</p>
s_agentSrvcName	<p><i>(Only for Microsoft Windows)</i> Enter a custom name for the Management Agent service.</p> <p>Every Management Agent appears as a service in Microsoft Windows, and every Management Agent has a default service name. If you want to assign a custom name to identify it, then use this parameter.</p> <p>For example, <code>s_agentSrvcName=agentsrvcl</code></p> <p>Note: If you upgrade a 12c Release 1 (12.1.0.1) or Release 2 (12.1.0.2) Management Agent installed on a Microsoft Windows host to 12c Release 3 (12.1.0.3), and you want to install another Management Agent on the same host, reporting to a different OMS, ensure that you specify the <code>s_agentSrvcName</code> parameter.</p>
EM_STAGE_DIR	<p>Enter the absolute path to a custom location that can be created as a temporary Provisioning Advisor Framework (PAF) staging directory.</p> <p>By default, every time you install a Management Agent, a PAF staging directory is created for copying the Software Library entities related to the deployment procedures. By default, this location is the scratch path location (<code>/tmp</code>). The location is used only for provisioning activities—entities are copied for a deployment procedure, and then, deleted once the deployment procedure ends.</p> <p>If you want to override this location with a custom location, you can pass this option and enter a custom location.</p> <p>For example,</p> <p><code>EM_STAGE_DIR=/home/john/software/oracle/pafdir</code></p>
b_startAgent=false	<p>Specify this parameter if you do not want the Management Agent to start automatically once it is installed and configured.</p> <p>If you do not specify this parameter, the Management Agent starts automatically once it is installed and configured.</p>
b_secureAgent=false	<p>Specify this parameter if you do not want the Management Agent to be secured after the install.</p> <p>If you specify this parameter, ensure that you also specify the OMS HTTP port, using the <code>EM_UPLOAD_PORT</code> parameter.</p> <p>For example, <code>b_secureAgent=false EM_UPLOAD_PORT=4899</code></p> <p>If you do not specify this parameter, the Management Agent is secured automatically after the install.</p>

7.4.1.2 Format of Host List File

In the Add Host Targets Wizard, you can click **Load from File** to add the hosts listed in a file. However, ensure that the file you select has one of the following formats:

- Only the host name.

For Example,

`host1.example.com`

`host2.example.com`

- The host name followed by the platform name.

For Example,

```
host1.example.com linux_x64
```

```
host2.example.com aix
```

The supported platform names are linux_x64, linux, solaris, hpunix, hpi, linux64_zseries, aix, linux_ppc64, windows_x64, solaris_x64, win32.

7.4.2 Cloning in Silent Mode

To clone a Management Agent manually, follow these steps:

Note: If the source Management Agent that you want to clone was installed using the Add Host Targets Wizard, or EM CLI, it is recommended that you clone this Management Agent in graphical mode. For information on how to do this, see [Section 7.4.1](#).

1. Set the environment variables described in [Table 7–3](#).
2. Navigate to the agent base directory:

```
cd $AGENT_BASE_DIR
```
3. Run the `create_plugin_list.pl` script from the Management Agent Oracle home:

```
$AGENT_HOME/perl/bin/perl $AGENT_HOME/sysman/install/create_plugin_list.pl -instancehome <AGENT_INSTANCE_HOME>
```
4. Compress the directories and files present in the agent base directory, and create a ZIP file in the temporary directory:

```
zip -r $T_WORK/agentcoreimage.zip core sbin plugins plugins.txt agentimage.properties
```
5. Navigate to the temporary directory:

```
cd $T_WORK
```
6. Copy the `agentDeploy.sh` to the temporary directory:

```
cp $AGENT_HOME/sysman/install/agentDeploy.sh .
```
7. Copy the UNZIP utility to the temporary directory:

```
cp $AGENT_HOME/bin/unzip .
```
8. Copy the `agentimage.properties` to the temporary directory:

```
cp $AGENT_BASE_DIR/agentimage.properties .
```
9. Create the final ZIP file with all the contents to be transferred, in the temporary directory:

```
zip -r agent.zip $T_WORK/*
```
10. Transfer the ZIP file to the installation base directory of the destination host using a file transfer utility (for example, FTP).
11. Extract the contents of the ZIP file to a temporary directory on the destination host (the temporary directory is referred to as `<extracted_location>` in the steps that follow).

12. Create a response file titled `agent.rsp` (in the same directory) as described in [Table 6–3](#).

Note: The response file you create can have any name, and not necessarily `agent.rsp`. For easy understanding, this chapter uses the name `agent.rsp`. Also, instead of creating a response file, you can choose to pass the values in separate arguments while invoking the deployment script. However, Oracle recommends that you create a response file and capture the information there.

13. Invoke the deployment script and pass the response file:

```
<extracted_location>/agentDeploy.sh AGENT_BASE_DIR=<absolute_path_to_
clone_agentbasedir> RESPONSE_FILE=<absolute_path_to_responsefile>
```

Note:

- Instead of creating a response file, if you choose to pass the values in separate arguments, then invoke the deployment script with some mandatory arguments in the following way:

```
<extracted_location>/agentDeploy.sh AGENT_BASE_
DIR=<absolute_path_to_agentbasedir> OMS_HOST=<oms_
hostname> EM_UPLOAD_PORT=<em_upload_port> AGENT_
REGISTRATION_PASSWORD=<password>
```

- In addition to passing the agent base directory and a response file (or individual mandatory arguments with installation details), you can also pass other options that are supported by the deployment script. For more information, see [Section 6.4.8](#).
 - If the source Management Agent was installed using the Add Host Targets Wizard, ensure that you specify the `b_startAgent=true` and the `b_secureAgent=true` parameters while invoking the deployment script.
-

7.4.2.1 Setting Environment Variables for Cloning Agent Using ZIP File

[Table 7–3](#) lists the environment variables you need to set and describes how you can set them.

Table 7–3 Setting Environment Variables for Cloning Agent Using ZIP File

AGENT_BASE_DIR	Set it to the installation base directory of the Management Agent you want to clone.	<ul style="list-style-type: none"> ■ In bash terminal, run the following command: <code>export AGENT_BASE_DIR=<absolute_path_to_agent_install_base_dir></code> For example, <code>export AGENT_BASE_DIR=/u01/app/Oracle/software/agent</code> ■ In other terminals, run the following command: <code>setenv AGENT_BASE_DIR <absolute_path_to_agent_install_base_dir></code> For example, <code>setenv AGENT_BASE_DIR /u01/app/Oracle/software/agent</code>
AGENT_HOME	Set it to the Oracle home of the Management Agent. For example, <u>/u01/app/Oracle/software/agent/core/12.1.0.3.0</u>	<ul style="list-style-type: none"> ■ In bash terminal, run the following command: <code>export AGENT_HOME=<absolute_path_to_agent_home></code> For example, <code>export AGENT_HOME=/u01/app/Oracle/software/agent/core/12.1.0.3.0</code> ■ In other terminals, run the following command: <code>setenv AGENT_HOME <absolute_path_to_agent_home></code> For example, <code>setenv AGENT_HOME /u01/app/Oracle/software/agent/core/12.1.0.3.0</code>
T_WORK	Set it to /tmp/clone_work.	<ul style="list-style-type: none"> ■ In bash terminal, run the following command: <code>export T_WORK=/tmp/clone_work</code> ■ In other terminals, run the following command: <code>setenv T_WORK /tmp/clone_work</code>

7.5 After You Clone

After you clone the Management Agent, follow these steps:

1. *(Only for Graphical Mode)* Verify the installation on the Add Host Status page. Review the progress made on each of the phases of the deployment operation — **Initialization, Remote Prerequisite Check, and Agent Deployment.**

Note: In the Add Host Targets Wizard, after you click **Deploy Agent** to install one or more Management Agents, you are automatically taken to the Add Host Status page.

If you want to view the details or track the progress of all the deployment sessions, then from the **Setup** menu, select **Add Target**, and then, click **Add Targets Manually**. On the Add Targets Manually page, select **Add Host Targets** and click **Add Host Results**.

If a particular phase fails or ends up with a warning, then review the details provided for each phase in the Agent Deployment Details section, and do one of the following:

- Ignore the warning or failure, and continue with the session if you prefer.
 - You can choose to proceed with the deployment of Management Agents only on those remote hosts that have successfully cleared the checks, and you can ignore the ones that have Warning or Failed status. To do so, click **Continue** and select **Continue, Ignoring Failed Hosts**.
 - You can choose to proceed with the deployment of Management Agents on all the hosts, including the ones that have Warning or Failed status. To do so, click **Continue** and select **Continue, All Hosts**.
- Fix the problem by reviewing the error description carefully, understanding its cause, and taking action as recommended by Oracle.
 - You can choose to retry the deployment of Management Agents with the same installation details. To do so, click **Retry** and select **Retry Using Same Inputs**.
 - You can retry the deployment of Management Agents with modified installation details. To do so, click **Retry** and select **Update Inputs and Retry**.

Note: If you see the error message *Copying Source Agent Image Failed*, then refer to the following log file in the OMS home:

```
$<OMS_
HOME>/sysman/prov/agentpush/<timestampdir>/applogs/deployfwk
.log
```

This error usually occurs when the job system is not enabled on the source Management Agent you are cloning. Ensure that the job system is enabled.

2. Perform the post installation steps as described in [Section 6.5](#).

Note:

- If Oracle Management Agents 12c (12.1.0.x) hang frequently or do not respond on Solaris 9ux and 10ux operating systems, then refer to document ID 1427773.1 on My Oracle Support.
- You can repoint your existing Management Agents to a new Oracle Management Service (OMS). For information on how to do this, see the Redirecting Oracle Management Agent to Another Oracle Management Service Appendix present in *Oracle Enterprise Manager Cloud Control Advanced Installation Guide*.

When you repoint your existing Management Agents to a new OMS, you cannot move the targets monitored by the Management Agents, the target history, and the Management Agent history. The monitored targets and the history data is lost.

Installing Shared Agent

This chapter describes how you can install a *Shared Agent* with the help of a central, shared Oracle home location of an existing Oracle Management Agent (Management Agent) that is installed on an NFS-mounted drive.

- [Overview](#)
- [Before You Begin](#)
- [Prerequisites](#)
- [Installation Procedure](#)
- [After You Install](#)

8.1 Overview

Shared Agent is a Management Agent that is installed on a remote host, using the binaries of an existing Management Agent. The Management Agent that shares its software binaries, in this context, is called the *Master Agent*, and the one that is configured with an instance directory on the remote host is called a *Shared Agent* or an *NFS Agent*.

This feature facilitates the installation of multiple Management Agents by making use of very limited resources, and helps you carry out lifecycle operations with ease. For example, patching the *Master Agent* updates all its *Shared Agents*.

You can take advantage of this operation by installing additional Management Agents on hosts that share a mounted drive where a Management Agent is already installed. Such an operation makes use of the software binaries of the shared Oracle home present on the mounted drive, and configures the remote hosts such that they are managed by that Management Agent, thereby capitalizing on the NFS visibility and saving hard disk space on the remote hosts.

You can install a *Shared Agent* in graphical or silent mode. In graphical mode, you use the Add Host Targets Wizard that is accessible from within the Enterprise Manager Cloud Control console. In silent mode, you use the `AgentNFS.pl` script.

The wizard and the script use the software binaries from the shared Oracle home and configure an instance directory on each of the destination hosts for storing configuration files such as `emd.properties`, `targets.xml`, log files, and so on.

Note:

- Installing a *Shared Agent* on a host running on Microsoft Windows is not supported.
 - Unlike the Add Host Target Wizard, the `AgentNFS.pl` script must be run only from a destination host, and at a given time, only one Management Agent can be installed. Therefore, if you want to install only a few Management Agents, then use the `AgentNFS.pl` script.
-

8.2 Before You Begin

Before you begin, keep these points in mind:

- When you install a *Shared Agent*, you only configure an instance directory on the destination host to store configuration files; you do not actually install a Management Agent. However, a *Shared Agent* installed on a host behaves exactly like a Management Agent, and has all the features and capabilities of a Management Agent.
- Only the destination host and the *Shared Agent* installed on it get automatically discovered and monitored in the Enterprise Manager system. The targets running on that destination host do not get automatically discovered and added to the Enterprise Manager system.
- The source host (*where the Master Agent is running*) and the destination host must be running on the same operating system.
- The *Master Agent* and the *Shared Agent* must be installed with the same user account.
- (*Only for Graphical Mode*) The Add Host Targets Wizard uses SSH to establish connectivity between Oracle Management Service (OMS) and the remote hosts where you want to install the Management Agents.
- (*Only for Graphical Mode*) Only SSH1 (SSH version 1) and SSH2 (SSH version 2) protocols offered by OpenSSH are supported for deploying a Management Agent.
- (*Only for Graphical Mode*) The Add Host Targets Wizard supports Named Credentials that enable you to use a set of credentials registered with a particular name specifically for this operation, by your administrator. This ensures an additional layer of security for your passwords because as an operator, you can only select the named credential, which is saved and stored by an administrator, and not know the actual user name and password associated with it.

In case the named credential you select does not have the privileges to perform the installation, then you can set the named credential to run as another user (locked user account). In this case, the wizard logs in to the hosts using the named credential you select, but performs the installation using the locked user account you set.

For example, you can create a named credential titled `User_A` (the user account that has remote login access), and set it to run as `User_X` (the Management Agent install user account for which no `direct login` is set) that has the required privileges. In this case, the wizard logs in to the hosts as `User_A`, but installs as `User_X`, using the privilege delegation setting (`sudo` or `PowerBroker`) specified in the named credential.

- (Only for Graphical Mode) Named credentials support SSH public key authentication and password based authentication. So you can use an existing SSH public key authentication without exposing your passwords.

To set up SSH public key authentication for a named credential, follow these steps:

Note: If you have already set up SSH public key authentication for a named credential and the SSH keys are already created, upload the SSH keys to Enterprise Manager, as mentioned in Step 3 of the following procedure.

1. Navigate to the following location in the OMS home:

```
$<OMS_HOME>/oui/prov/resources/scripts
```

For example,

```
/home/software/em/middleware/oms/oui/prov/resources/scripts
```

2. If the OMS host runs on a Unix based operating system, run the following script on the OMS host as the OMS user, and pass the Management Agent install user name and the fully qualified name of the target hosts:

```
sshUserSetup.sh -setup -user <agent_install_user_name> -hosts  
<target_hosts>
```

The following SSH keys are created:

```
$HOME/.ssh/id_rsa  
$HOME/.ssh/id_rsa_pub
```

Here, \$HOME refers to the home directory of the OMS install user.

If the OMS host runs on Microsoft Windows, install Cygwin on the OMS host (described in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*), then run the following script on the OMS host as the OMS user, and pass the Management Agent install user name and the fully qualified name of the target hosts:

```
sshUserSetupNT.sh -setup -user <agent_install_user_name> -hosts  
<target_hosts>
```

3. Upload the SSH keys to Enterprise Manager.

From the **Setup** menu, select **Security**, then select **Named Credentials**. Click **Create**. For **Credential Name**, specify the credential name. For **Credential Type**, select **SSH Key Credentials**.

To upload one of the private SSH keys created in Step 2, in the Credential Properties section, specify the location of the private SSH key as a value for the **Upload Private Key** field. Click **Save**.

To upload one of the public SSH keys created in Step 2, in the Credential Properties section, specify the location of the public SSH key as a value for the **Upload Public Key** field. Click **Save**.

[Figure 8–1](#) describes how to upload SSH keys to Enterprise Manager.

Figure 8–1 Uploading SSH Keys to Enterprise Manager

The screenshot shows the 'Create Credential' wizard. In the 'General Properties' section, the 'Credential name' is 'oracle_ssh', 'Authenticating Target Type' is 'Host', and 'Credential type' is 'SSH Key Credentials'. In the 'Credential Properties' section, the 'Username' is 'oracle', 'SSH Private Key' is a long alphanumeric string, and 'SSH Public Key' is a long alphanumeric string. There are 'Upload Private Key' and 'Upload Public Key' buttons with 'Browse...' links.

If you have already set up SSH public key authentication for a named credential, you can use the named credential while installing Management Agents using the Add Host Targets Wizard.

- By default, the following types of plug-ins are configured on the *Shared Agent*:
 - All discovery plug-ins that were configured with the OMS from where the Management Agent software is being deployed.
 - Oracle Home discovery plug-in
 - Oracle Home monitoring plug-in
 - All the additional plug-ins deployed on the *Master Agent*

8.3 Prerequisites

Before installing a *Shared Agent*, ensure that you meet the following prerequisites:

Table 8–1 Prerequisites for Installing Shared Agent

Requirement	Description
Hardware Requirements	Ensure that you meet the hard disk space and physical memory requirements. For more information, see the chapter on hardware requirements in the <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i> .
Destination Host Disk Space Requirements	Ensure that the <i>Master Agent</i> host has a minimum of 1 GB free hard disk space, and the <i>Shared Agent</i> host has a minimum of 2 MB free hard disk space.

Table 8–1 (Cont.) Prerequisites for Installing Shared Agent

Requirement	Description
Operating System Requirements	<p>Ensure that you install the Management Agent only on certified operating systems as mentioned in the Enterprise Manager certification matrix available on <i>My Oracle Support</i>.</p> <p>You cannot install a <i>Shared Agent</i> using a <i>Master Agent</i> that runs on a Microsoft Windows platform. <i>Shared Agents</i> are not supported on Microsoft Windows platforms.</p> <p>To access the Enterprise Manager certification matrix, follow the steps outlined in <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>.</p> <p>For information about platforms receiving future support, refer to <i>My Oracle Support</i> note 793512.1.</p> <p>Note: If you use Oracle Solaris 10, then ensure that you have update 9 or higher installed. To verify whether it is installed, run the following command:</p> <pre>cat /etc/release</pre> <p>You should see the output similar to the following. Here, s10s_u6 indicates that update 6, which is not a supported update level for installation, is installed.</p> <pre>Solaris 10 10/08 s10s_u6wos_07b SPARC</pre>
Package Requirements	<p>Ensure that you install all the operating system-specific packages. For more information, see the chapter on package requirements in the <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>.</p>
User and Operating System Group Requirement	<p>Ensure that the destination host where you want to install the Management Agent has the appropriate users and operating system groups created.</p> <p>For more information, see the chapter on creating operating system groups and users in the <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>.</p>
Software Availability Requirements	<p>Ensure that you already have Oracle Management Agent 12c installed as a <i>Master Agent</i> in a shared, mounted location.</p> <p>For information on how to install a Management Agent, see <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>.</p>

Table 8–1 (Cont.) Prerequisites for Installing Shared Agent

Requirement	Description
Software Mount Requirements	<p>Ensure that at least one <i>Shared Agent</i> host has read write permissions on the mount location. To mount the Management Agent software on the <i>Shared Agent</i> host with read write permissions, run the following command:</p> <pre>mount -t nfs -o rw <master_agent_host_name>:<agent_base_dir_of_master_agent> <agent_base_dir_of_shared_agent></pre> <p>For example, run the following command:</p> <pre>mount -t nfs -o rw abc.oracle.com:/scratch/agent /scratch/agent</pre> <p>To mount the Management Agent software on the <i>Shared Agent</i> host with read only permissions, run the following command:</p> <pre>mount -t nfs -o ro <master_agent_host_name>:<agent_base_dir_of_master_agent> <agent_base_dir_of_shared_agent></pre> <p>For example, run the following command:</p> <pre>mount -t nfs -o ro abc.oracle.com:/scratch/agent /scratch/agent</pre> <p>Note: Before mounting the Management Agent software on the <i>Shared Agent</i> host, ensure that you have created the agent base directory on the <i>Shared Agent</i> host, such that the directory has the same path as the agent base directory on the <i>Master Agent</i> host.</p>
/etc/hosts File Requirements	<p>Ensure that the /etc/hosts file on the host has the IP address, the fully qualified name, and the short name in the following format:</p> <pre>172.16.0.0 example.com mypc</pre>
Destination Host Access Requirements	<p>Ensure that the destination hosts are accessible from the host where the OMS is running.</p> <p>If the destination host and the host on which OMS is running belong to different network domains, then ensure that you update the /etc/hosts file on the destination host to add a line with the IP address of that host, the fully qualified name of that host, and the short name of the host.</p> <p>For example, if the fully-qualified host name is example.com and the short name is mypc, then add the following line in the /etc/hosts file:</p> <pre>172.16.0.0 example.com mypc</pre>
Destination Host Credential Requirements (Only for Graphical Mode)	<p>Ensure that all the destination hosts running on the same operating system have the same set of credentials. For example, all the destination hosts running on Linux operating system must have the same set of credentials.</p> <p>The wizard installs the Management Agent using the same user account. If you have hosts running on the same operating system but with different credentials, then have two different deployment sessions.</p>

Table 8–1 (Cont.) Prerequisites for Installing Shared Agent

Requirement	Description
Destination Host Time Zone Requirements (Only for Graphical Mode)	<p>Ensure that the time zones of the destination hosts have been set correctly. To verify the time zone of a destination host, log in to the OMS host, and run the following command:</p> <pre>ssh -l <install_user> <destination_host_name> /bin/sh -c 'echo \$TZ'</pre> <p>If the time zone displayed is incorrect, log in to the destination host, and follow these steps:</p> <ol style="list-style-type: none"> Run the following commands to set the time zone on the destination host: <ul style="list-style-type: none"> For Korn shell: <pre>TZ=<value> export TZ</pre> For Bourne shell or Bash shell: <pre>export TZ=<value></pre> For C shell: <pre>setenv TZ <value></pre> <p>For example, in the Bash shell, run the following command to set the time zone to America/New_York:</p> <pre>export TZ='America/New_York'</pre> <p>To view a list of the time zones you can use, access the supportedtzs.lst file present in the <AGENT_HOME>/sysman/admin directory of the central agent (that is, the Management Agent installed on the OMS host).</p> <ol style="list-style-type: none"> Restart the SSH daemon. <p>If the destination host runs on a UNIX based operating system, run the following command:</p> <pre>sudo /etc/init.d/sshd restart</pre> <p>If the destination host runs on a Microsoft Windows operating system, run the following commands:</p> <pre>cygrunsrv -E sshd cygrunsrv -S sshd</pre> Verify whether the SSH server can access the TZ environment variable by logging in to the OMS host, and running the following command: <pre>ssh -l <install_user> <destination_host_name> /bin/sh -c 'echo \$TZ'</pre> <p>Note: If you had ignored a prerequisite check warning about wrong time zone settings during the Management Agent install, you must set the correct time zone on the destination hosts after installing the Management Agents. For information on setting time zones post install, refer Section 8.5.</p>

Table 8–1 (Cont.) Prerequisites for Installing Shared Agent

Requirement	Description
Time Zone Requirements <i>(Only for Silent Mode)</i>	<p>Ensure that the host time zone has been set correctly. To verify the host time zone, run the following command:</p> <pre>echo \$TZ</pre> <p>If the time zone displayed is incorrect, run the following commands, before running the <code>agentDeploy.sh</code> or <code>agentDeploy.bat</code> scripts, to set the correct time zone:</p> <ul style="list-style-type: none"> For Korn shell: <pre>TZ=<value> export TZ</pre> For Bourne shell or Bash shell: <pre>export TZ=<value></pre> For C shell: <pre>setenv TZ <value></pre> <p>For example, in the Bash shell, run the following command to set the time zone to America/New_York:</p> <pre>export TZ='America/New_York'</pre> <p>To view a list of the time zones you can use, access the <code>supportedtzs.lst</code> file present in the <code><AGENT_HOME>/sysman/admin</code> directory of the central agent (that is, the Management Agent installed on the OMS host).</p> <p>Note: If you had ignored a prerequisite check warning about wrong time zone settings during the Management Agent install, you must set the correct time zone on the host after installing the Management Agent. For information on setting time zones post install, refer Section 8.5.</p>
sudo/pbrun/sesu/su SSH Requirements <i>(Only for Graphical Mode)</i>	<p>Ensure that you set the <code>oracle.sysman.prov.agentpush.enablePty</code> property to true in the <code>\$(OMS_HOME)/sysman/prov/agentpush/agentpush.properties</code> file, if the privilege delegation tool you are using requires a pseudo terminal for remote command execution via SSH. Most privilege delegation tools such as pbrun, sesu, and su require a pseudo terminal for remote command execution, by default.</p> <p>Note: If you are using sudo as your privilege delegation tool, and you do not want to set the <code>oracle.sysman.prov.agentpush.enablePty</code> property to true, do one of the following:</p> <ul style="list-style-type: none"> Include Defaults <code>visiblepw</code> in the <code>/etc/sudoers</code> file, or enter the sudo command with the <code>-S</code> option for Privileged Delegation Setting on the Installation Details page. For information on how to access the Installation Details page, see Section 8.4.1. Comment out Defaults <code>requiretty</code> in the <code>/etc/sudoers</code> file.

Table 8–1 (Cont.) Prerequisites for Installing Shared Agent

Requirement	Description
<p>sudo/pbrun/sesu/su Requirements (for Root User)</p> <p>(Only for Graphical Mode)</p>	<ul style="list-style-type: none"> <p>Ensure that the installing user has the privileges to invoke the <code>id</code> command and the <code>agentdeployroot.sh</code> script as <i>root</i>. Grant the privileges in the configuration file of your privilege delegation tool.</p> <p>For example, if you are using <code>sudo</code> as your privilege delegation tool, include the following in the <code>/etc/sudoers</code> file to grant the required privileges:</p> <pre><install_user> ALL=(root) /usr/bin/id, <agent_home> /*/agentdeployroot.sh</pre> <p>For example, <code>oracle</code> <code>ALL=(root) /usr/bin/id, /u01/app/oracle/admin/shared/agent_home /*/agentdeployroot.sh</code></p> <p>Here, <code>oracle</code> is the installing user, and <code>/u01/app/oracle/admin/shared/agent_home</code> is the <i>Shared Agent</i> home.</p> <p>You do not require the following entry in the <code>/etc/sudoers</code> file for installing a Management Agent. However, the entry is required for performing provisioning and patching operations in Enterprise Manager. Therefore, if you are removing this entry before installing a Management Agent, then ensure that you bring back the entry after installing the Management Agent.</p> <p>In Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2) or Release 3 (12.1.0.3):</p> <pre>(root) /<AGENT_BASE_DIRECTORY>/sbin/nmosudo</pre> <p>In Enterprise Manager Cloud Control 12c Release 1 (12.1.0.1) [with Bundle Patch 1]:</p> <pre>(root) /<AGENT_INSTANCE_DIRECTORY>/bin/nmosudo</pre>

Table 8–1 (Cont.) Prerequisites for Installing Shared Agent

Requirement	Description
<p>sudo/pbrun/sesu/su Requirements (for Locked Account User)</p> <p>(Only for Graphical Mode)</p>	<p>Ensure that the installing user has the privileges to invoke <code>/bin/sh</code> as the locked account user. Grant the privileges in the configuration file of your privilege delegation tool.</p> <p>For example, if you are using <code>sudo</code> as your privilege delegation tool, include the following in the <code>/etc/sudoers</code> file to grant the required privileges:</p> <pre>login_user1 ALL=(oracle) /bin/sh</pre> <p>Here, <code>login_user1</code> is the SSH log in user, and <code>oracle</code> is the locked account and install user.</p> <p>If you do not want to grant privileges to the installing user to invoke <code>/bin/sh</code> as the locked account user, set the <code>oracle.sysman.prov.agentpush.pdpShellOutEnabled</code> property to <code>false</code>, and ensure that the installing user has the privileges to invoke <code>id</code>, <code>chmod</code>, <code>cp</code>, <code>mkdir</code>, <code>rm</code>, <code>tar</code>, <code>emctl</code>, <code>perl</code>, <code>runInstaller</code>, and <code>unzip</code> as the locked account user. Grant the privileges in the configuration file of your privilege delegation tool.</p> <p>For example, if you are using <code>sudo</code> as your privilege delegation tool, include the following in the <code>/etc/sudoers</code> file to grant the required privileges:</p> <pre>login_user1 ALL=(oracle) /usr/bin/id, /bin/chmod, /bin/cp, /bin/mkdir, /bin/rm, /bin/tar, /home/oracle/agentinst/bin/emctl, /home/oracle/agentibd/core/12.1.0.3.0/perl/bin/perl, /home/oracle/agentibd/core/12.1.0.3.0/oui/bin/runInstaller, /home/oracle/agentibd/core/12.1.0.3.0/bin/unzip</pre> <p>Here, <code>login_user1</code> is the SSH log in user, <code>oracle</code> is the locked account and install user, <code>/home/oracle/agentinst</code> is the agent instance directory of the <i>Shared Agent</i>, and <code>/home/oracle/agentibd</code> is the agent base directory.</p>
Temporary Directory Space Requirements	<p>Ensure that you allocate 400 MB of space for a temporary directory where the executables can be copied.</p> <p>By default, the temporary directory location set to the environment variable <code>TMP</code> or <code>TEMP</code> is honored. If both are set, then <code>TEMP</code> is honored. If none of them are set, then the following default values are honored: <code>/tmp</code> on UNIX hosts and <code>c:\Temp</code> on Microsoft Windows hosts.</p>
Instance Directory Requirements	Ensure that the <i>Shared Agent</i> instance directory (the directory where you want to save the <i>Shared Agent</i> configuration files) you specify is empty and has write permissions for the install user. Also, ensure that the parent directory has write permissions for the install user.
Shared Oracle Home Requirements	Ensure that the <i>Master Agent</i> home is accessible from the destination host where you want to install the <i>Shared Agent</i> . Ensure that the <i>Master Agent</i> home is mounted with the <code>setuid</code> turned on.
Path Validation Requirements (Only for Graphical Mode)	Validate the path to all command locations. For more information, see the appendix on validating command locations in the <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i> .
CLASSPATH Environment Variable Requirements	If the value assigned to the <code>CLASSPATH</code> environment variable has white spaces in it, then ensure that you unset it. You can always reset the environment variable to the original value after the installation is complete.

Table 8–1 (Cont.) Prerequisites for Installing Shared Agent

Requirement	Description
Default SSH Port Requirements (Only for Graphical Mode)	<p>Ensure that the SSH daemon is running on the default port (that is, 22) on all the destination hosts. To verify the SSH port on a Unix host, run the following command:</p> <pre>netstat -anp grep -i sshd</pre> <p>For example, the output of this command may be the following:</p> <pre>tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 3188/sshd</pre> <p>The above output indicates that the SSH daemon is running on port 22.</p> <p>Also, on a Unix host, you can run the following command to verify the SSH port:</p> <pre>cat /etc/ssh/sshd_config</pre> <p>For a Microsoft Windows host, the SSH port value is mentioned in the C:\cygwin\etc\sshd_config file.</p> <p>If the SSH port is a non-default port, that is, any port other than 22, then update the SSH_PORT property in the following file:</p> <pre>\$<OMS_HOME>/oui/prov/resources/Paths.properties</pre>
Port Requirements	Ensure that the default ports described in Section 2.1.9.1 are free.
Installing User Requirements	<ul style="list-style-type: none"> ■ The <i>Master Agent</i> and the <i>Shared Agent</i> must be installed with the same user account. ■ If the central inventory owner and the user installing the Management Agent are different, then ensure that they are part of the same group. ■ Ensure that the inventory owner and the group to which the owner belongs have <i>read</i> and <i>write</i> permissions on the inventory directory. <p>For example, if the inventory owner is <i>abc</i> and the user installing the Management Agent is <i>xyz</i>, then ensure that <i>abc</i> and <i>xyz</i> belong to the same group, and they have read and write access to the inventory.</p>
Central Inventory (oraInventory) Requirements	<ul style="list-style-type: none"> ■ Ensure that you allocate 100 MB of space for the Central Inventory. ■ Ensure that the inventory directory is not in a shared file system. ■ The <i>Shared Agent</i> uses the inventory location mentioned in the oraInst.loc file, which is present in the <MASTER_AGENT_BASE DIR>/core/12.1.0.3.0/ directory. Ensure that the <i>Shared Agent</i> user has read and write permissions on this directory.
Preinstallation/Postinstallation Scripts Requirements (Only for Graphical Mode)	Ensure that the preinstallation and postinstallation scripts that you want to run along with the installation are available either on the OMS host, destination hosts, or on a shared location accessible to the destination hosts.

Table 8–1 (Cont.) Prerequisites for Installing Shared Agent

Requirement	Description
Browser Requirements (Only for Graphical Mode)	<ul style="list-style-type: none"> Ensure that you use a certified browser as mentioned in the Enterprise Manager certification matrix available on <i>My Oracle Support</i>. To access the Enterprise Manager certification matrix, follow the steps outlined in <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>. If you use Microsoft Internet Explorer 8 or 9, do the following: <ul style="list-style-type: none"> Turn off the compatibility view mode. To do so, in Microsoft Internet Explorer, from the Tools menu, click Compatibility View to disable it if it is enabled. Also, click Compatibility View Settings and deregister the Enterprise Manager Cloud Control console URL. Enable XMLHTTP. To do so, from the Tools menu, click Internet Options. Click the Advanced tab, and under the Security heading, select Enable native XMLHTTP support to enable it.

8.4 Installation Procedure

This section describes the following:

- [Installing in Graphical Mode](#)
- [Installing in Silent Mode](#)

8.4.1 Installing in Graphical Mode

To install a *Shared Agent* in graphical mode, follow these steps:

- In Cloud Control, do one of the following:
 - From the **Setup** menu, select **Add Targets**, and then, click **Auto Discovery Results**. On the Auto Discovery Results page, select a host you want to monitor in Enterprise Manager Cloud Control, and click **Promote**.
 - From the **Setup** menu, select **Add Target**, and then, click **Add Targets Manually**. On the Add Targets Manually page, select **Add Host Targets** and click **Add Host**.
- On the Host and Platform page, do the following:
 - Accept the default name assigned for this session or enter a unique name of your choice. The custom name you enter can be any intuitive name, and need not necessarily be in the same format as the default name. For example, add_host_operation_1

A unique deployment activity name enables you to save the installation details specified in this deployment session and reuse them in the future without having to enter all the details all over again in the new session.

- b. Click **Add** to enter the fully qualified name and select the platform of the host on which you want to install the Management Agent.

Note:

- Oracle recommends you to enter the fully qualified domain name of the host. For monitoring purpose, Enterprise Manager Cloud Control adds that host and the Management Agent with the exact name you enter here.
 - You must enter only one host name per row. Entering multiple host names separated by a comma is not supported.
 - You must ensure that the host name you enter does not have underscores.
-

Alternatively, you can click either **Load from File** to add host names stored in a file, or **Add Discovered Hosts** to add host names from a list of hosts discovered by Enterprise Manager. For information on how the host name entries must appear in the host file, see [Section 7.4.1.2](#)

Note: When you click **Add Discovered Hosts** and add hosts from a list of discovered hosts, the host's platform is automatically detected and displayed. The platform name is detected using a combination of factors, including hints received from automated discovery and the platform of the OMS host. This default platform name is a suggestion, so Oracle strongly recommends you to verify the platform details before proceeding to the next step.

As the *Shared Agent* can be installed only if the source host and the destination host are running on the same platform, set the platform for the first host in the first row of the table and from the **Platform** list, select **Same for All Hosts**. This will ensure that the platform name you selected for the first host is also set for the rest of the hosts in the table.

Note: If you are installing a Management Agent on a host that is running on a platform different from the OMS host platform, then ensure that the Management Agent software for that platform is available in Oracle Software Library (Software Library). If the Management Agent software for the required platform is not available in Software Library, acquire and apply the software using the Self Update console.

To access the Self Update Console, from the **Setup** menu, select **Extensibility**, then select **Self Update**. To acquire the latest Management Agent software, click **Agent Software**, select the required software, then click **Download**.

For more information on how to acquire and apply the Management Agent software for a platform using the Self Update console, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

- c. Click **Next**.

3. On the Installation Details page, do the following:
 - a. In the Deployment Type section, select **Add Host to Shared Agent**. Then, for **Select Target**, click the torch icon and select the Management Agent that is shared and mounted. This location must be visible on all remote hosts.

Figure 8–2 describes this step.

Figure 8–2 Installing a Shared Agent

- b. From the table, select the first row that indicates the hosts grouped by their common platform name.
- c. In the Installation Details section, provide the installation details common to the hosts selected in Step 3 (b). For **Oracle Home**, validate or enter the location of the shared Management Agent home. Ensure that the Management Agent home is on a shared location, and is accessible from all the destination hosts.
- d. For **Instance Directory**, enter the absolute path to a directory, on the *Shared Agent* host, where all Management Agent-related configuration files can be stored. Ensure that the directory has write permission.

For example, `/usr/home/software/oracle/agentHome/agent_inst`

If the path you enter does not exist, the application creates a directory at the specified path, and stores all the Management Agent-related configuration files there.

- e. From **Named Credential** list, select an appropriate profile whose credentials can be used for setting up the SSH connectivity between the OMS and the remote hosts, and for installing a Management Agent on each of the remote hosts.

Note:

- If you do not have a credential profile, or if you have one but do not see it in the **Named Credential** list, then click the plus icon against this list. In the Create New Named Credential window, enter the credentials and store them with an appropriate profile name so that it can be selected and used for installing the Management Agents. Also set the run privilege if you want to switch over from the Named Credential you are creating, to another user who has the privileges to perform the installation.
 - If the plus icon is disabled against this list, then you do not have the privileges to create a profile with credentials. In this case, contact your administrator and either request him/her to grant you the privileges to create a new profile or request him/her to create a profile and grant you the access to view it in the **Named Credential** list.
 - If you have manually set up SSH public key authentication between the OMS and the remote hosts, then you may not have a password for your user account. In this case, create a named credential with a dummy password. Do NOT leave the password field blank.
-

- f. For **Privileged Delegation Setting**, validate the Privilege Delegation setting to be used for running the root scripts. By default, it is set to the Privilege Delegation setting configured in Enterprise Manager Cloud Control.

For example, you can specify one of the following for the **Privileged Delegation Setting** field:

```
/usr/bin/sudo -u %RUNAS% %COMMAND%
/usr/bin/sesu - %RUNAS% -c "%COMMAND%"
/usr/bin/pbrun %PROFILE% -u %RUNAS% %COMMAND%
/usr/bin/su - %RUNAS% -c "%COMMAND%"
```

If you leave the **Privileged Delegation Setting** field blank, the root scripts will not be run by the wizard; you will have to run them manually after the installation. For information about running them manually, see [Section 8.5](#).

This setting will also be used for performing the installation as the user set in the Run As attribute of the selected Named Credential if you had set the user while creating that Named Credential.

Note: In the Privilege Delegation setting, the %RUNAS% is honored as the root user for running the root scripts and as the user set in the Run As attribute of the Named Credential for performing the installation.

- g. For **Port**, accept the default port (3872) that is assigned for the Management Agent to communicate, or enter a port of your choice.

The custom port you enter must not be busy. If you are not sure, you can leave it blank. Enterprise Manager Cloud Control automatically assigns the first available free port within the range of 1830 - 1849.

- h. (Optional) In the Optional Details section, enter the absolute path to an accessible location where the preinstallation and postinstallation scripts you

want to run are available. Note that only one preinstallation or one postinstallation script can be specified.

If you want to run the script as **root**, then select **Run as Root**. If the script is on the host where OMS is running and is not on the host where you want to install the Management Agent, then select **Script on OMS**. In this case, the script will be copied from the OMS host to the destination hosts, and then run on the destination hosts.

- i. (Optional) For **Additional Parameters**, enter a whitespace-separate list of additional parameters that you want to pass during the installation. For a complete list of supported additional parameters, see [Table 8-2](#).

For example, if you want to provide the inventory pointer location file, then enter `-invPtrLoc` followed by the absolute path to the file location. However, this parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.

- j. Repeat Step 3 (b) to Step 3 (h) for every other row you have in the table.
- k. Click **Next**.

- 4. On the Review page, review the details you have provided and if you are satisfied with the details, then click **Deploy Agent** to install the Management Agent.

If you want to modify the details, then click **Back** repeatedly to reach the page where you want to make the changes.

When you click **Deploy Agent** and submit the deployment session, you are automatically taken to the Add Host Status page that enables you to monitor the progress of the deployment session.

Note: If you restart the destination host after installing a *Shared Agent*, and the *Shared Agent* does not start up automatically, restore the mount with the original permissions, then start the *Shared Agent* manually.

8.4.1.1 Supported Additional Parameters

[Table 8-2](#) lists the additional parameters supported for installing a *Shared Agent* in graphical mode.

Table 8-2 Supported Additional Parameters

Parameter	Description
EM_STAGE_DIR	<p>Enter the absolute path to a custom location that can be created as a temporary Provisioning Advisor Framework (PAF) staging directory.</p> <p>By default, every time you install a Management Agent, a PAF staging directory is created for copying the Software Library entities related to the deployment procedures. By default, this location is the scratch path location (<code>/tmp</code>). The location is used only for provisioning activities—entities are copied for a deployment procedure, and then, deleted once the deployment procedure ends.</p> <p>If you want to override this location with a custom location, you can pass this option and enter a custom location.</p> <p>For example,</p> <pre>EM_STAGE_DIR=/home/john/software/oracle/pafdir</pre>

Table 8–2 (Cont.) Supported Additional Parameters

Parameter	Description
b_startAgent=false	Specify this parameter if you do not want the Management Agent to start automatically once it is installed and configured. If you do not specify this parameter, the Management Agent starts automatically once it is installed and configured.
b_secureAgent=false	Specify this parameter if you do not want the Management Agent to be secured after the install. If you specify this parameter, ensure that you also specify the OMS HTTP port, using the EM_UPLOAD_PORT parameter. For example, b_secureAgent=false EM_UPLOAD_PORT=4899 If you do not specify this parameter, the Management Agent is secured automatically after the install.

8.4.2 Installing in Silent Mode

To install a *Shared Agent* in silent mode, follow these steps:

On the Master Agent Host:

1. Run the create_plugin_list.pl script from the *Master Agent* host:

```
$AGENT_HOME/perl/bin/perl $AGENT_HOME/sysman/install/create_plugin_list.pl -instancehome <AGENT_INSTANCE_HOME>
```

On the Shared Agent Host:

1. Create a response file titled AgentNFS.rsp as described in [Table 8–3](#).

Note: The response file you create can have any name, and not necessarily AgentNFS.rsp. For easy understanding, this chapter uses the name AgentNFS.rsp. Also, instead of creating a response file, you can choose to pass the arguments explicitly while invoking the script. However, Oracle recommends that you create a response file and capture the information there.

2. Invoke the script from the *Shared Agent* host, and pass the response file.

```
$<AGENT_HOME>/perl/bin/perl <AGENT_HOME>/sysman/install/AgentNFS.pl -responseFile <absolute_path_to_response_file>
```

For example,

```
/scratch/agent_base_dir/core/12.1.0.3.0/perl/bin/perl /scratch/agent_base_dir/core/12.1.0.3.0/sysman/install/AgentNFS.pl -responseFile /home/john/AgentNFS.rsp
```

Ensure that <AGENT_HOME> is a shared location, and is accessible from all the destination hosts.

Note:

- Instead of creating a response file, you can choose to pass all the arguments explicitly while invoking the script. In this case, invoke the script in the following way:

```
<AGENT_HOME>/perl/bin/perl <AGENT_
HOME>/sysman/install/AgentNFS.pl AGENT_INSTANCE_
HOME=<absolute_path_to_instance_dir> ORACLE_
HOME=<absolute_path_to_master_agent_oracle_home>
<parameter1>=<value1> <parameter2>=<value2>
<parameter3>=<value3>...
```

For example,

```
/scratch/agent_base_dir/core/12.1.0.3.0/perl/bin/perl
/scratch/agent_base_
dir/core/12.1.0.3.0/sysman/install/AgentNFS.pl AGENT_
INSTANCE_HOME=/home/john/agent_inst ORACLE_
HOME=/scratch/agent_base_dir/core/12.1.0.3.0 AGENT_
PORT=1832 AGENT_REGISTRATION_PASSWORD=welcome b_
startAgent=TRUE
```

- If the *Master Agent* was installed using the Add Host Targets Wizard, then ensure that you pass the following arguments with these values:

```
AGENT_REGISTRATION_PASSWORD=<password>
b_startAgent=TRUE
```

- Do NOT pass the `-invPtrLoc` argument because, by default, the location `<AGENT_HOME>/oraInst.loc` is honored, where `<AGENT_HOME>` is the *Master Agent*. Also ensure that the Oracle Inventory directory, to which the inventory file points, is not in a shared location.
- If you restart the destination host after installing a *Shared Agent*, and the *Shared Agent* does not start up automatically, restore the mount with the original permissions, then start the *Shared Agent* manually.

3. When prompted to run the `root.sh` script, run it from the instance directory of the *Shared Agent*:

```
<AGENT_INSTANCE_HOME>/root.sh
```

If you are not a *root* user, then use SUDO to change to a *root* user. For example, run the following command:

```
/usr/local/bin/sudo /scratch/OracleHomes/agent_inst/root.sh
```

4. Repeat Step (2) to Step (4) on the remaining hosts where you want to install the *Shared Agent*.

8.4.2.1 Creating a Response File

For silently installing a *Shared Agent*, you must invoke the `AgentNFS.pl` script and pass a response file that captures all the required information. [Table 8–3](#) describes the various parameters you must include in the response file.

Table 8–3 Creating a Response File for Installing Oracle Management Agent Using the AgentNFS.pl Script

Parameter	Description
ORACLE_HOME	Specify the absolute path to the <i>Master Agent</i> home, which is shared and visible on the destination host. For example, /scratch/agent_base_dir/core/12.1.0.3.0
AGENT_PORT	(Optional) Enter the port on which the <i>Shared Agent</i> process should be started. You can enter any free port between 1830 and 1849. The same port is used for both HTTP and HTTPS. For example, 1832
AGENT_INSTANCE_HOME	Specify the absolute path to a location on the destination host where you want to store all Management Agent-related configuration files. For example, /home/john/agent_inst
AGENT_REGISTRATION_PASSWORD	Enter a password for registering new Management Agents that join the Enterprise Manager system. By default, the communication between the OMS and the Management Agents is secured and locked. Any new Management Agents that join the Enterprise Manager system must be authenticated before they become part of the system. The password you enter here will be used for authenticating those new Management Agents. For example, Wel456come Note: If the <i>Master Agent</i> was installed using the Add Host Targets Wizard, then you must pass this parameter.
b_startAgent	Set it to TRUE so that the <i>Shared Agent</i> is started automatically once it is installed and configured. Note: If the <i>Master Agent</i> was installed using the Add Host Targets Wizard, then you must pass this parameter.
ORACLE_HOSTNAME	(Optional) (Only for Installation on Virtual Hosts) Specify the virtual host name where you are installing the <i>Shared Agent</i> .
ALLOW_IPADDRESS	(Optional) Enter TRUE if you want to specify an IP address for ORACLE_HOSTNAME. If ALLOW_IPADDRESS is set to FALSE, a prerequisite check fails when you specify an IP address for ORACLE_HOSTNAME while installing a Management Agent. For example, ALLOW_IPADDRESS=TRUE If you do not include this parameter, it defaults to FALSE.
START_PRIORITY_LEVEL (For Unix based hosts only)	(Optional) Use this parameter to specify the priority level of the Management Agent service when the host is started. This parameter accepts values between 0 and 99. However, Oracle recommends that you provide a value between 91 and 99 for this parameter. For example, START_PRIORITY_LEVEL=95 If you do not include this parameter, it defaults to 98.
SHUT_PRIORITY_LEVEL (For Unix based hosts only)	(Optional) Use this parameter to specify the priority level of the Management Agent service when the host is shut down. This parameter accepts values between 0 and 99. For example, SHUT_PRIORITY_LEVEL=25 If you do not include this parameter, it defaults to 19.

Table 8–3 (Cont.) Creating a Response File for Installing Oracle Management Agent Using the AgentNFS.pl Script

Parameter	Description
PROPERTIES_FILE	<p>(Optional) Use this parameter to specify the absolute location of the properties file.</p> <p>For example, PROPERTIES_FILE=/tmp/agent.properties</p> <p>In the properties file, specify the parameters that you want to use for the Management Agent deployment. The list of parameters that you can specify in the properties file is present in \$<AGENT_INSTANCE_HOME>/sysman/config/emd.properties. In the properties file, you must specify the parameters in name value pairs, for example:</p> <pre>REPOSITORY_PROXYHOST=abc.example.com REPOSITORY_PROXYPORT=1532</pre> <p>The properties file does not support parameter values that have spaces. If the value of a particular parameter contains a space, then run the following command after deploying the Management Agent:</p> <pre>\$<AGENT_INSTANCE_HOME>/bin/emctl setproperty agent -name <parameter_name> -value <parameter_value></pre>

8.5 After You Install

After you install a *Shared Agent*, follow these steps:

1. (Only for Graphical Mode) Verify the installation on the Add Host Status page. Review the progress made on each of the phases of the deployment operation — **Initialization**, **Remote Prerequisite Check**, and **Agent Deployment**.

Note: In the Add Host Targets Wizard, after you click **Deploy Agent** to install one or more Management Agents, you are automatically taken to the Add Host Status page.

If you want to view the details or track the progress of all the deployment sessions, then from the **Setup** menu, select **Add Target**, and then, click **Add Targets Manually**. On the Add Targets Manually page, select **Add Host Targets** and click **Add Host Results**.

If a particular phase fails or ends up with a warning, then review the details provided for each phase in the Agent Deployment Details section, and do one of the following:

- Ignore the warning or failure, and continue with the session if you prefer.
 - You can choose to proceed with the deployment of Management Agents only on those remote hosts that have successfully cleared the checks, and you can ignore the ones that have Warning or Failed status. To do so, click **Continue** and select **Continue, Ignoring Failed Hosts**.
 - You can choose to proceed with the deployment of Management Agents on all the hosts, including the ones that have Warning or Failed status. To do so, click **Continue** and select **Continue, All Hosts**.
- Fix the problem by reviewing the error description carefully, understanding its cause, and taking action as recommended by Oracle.

- You can choose to retry the deployment of Management Agents with the same installation details. To do so, click **Retry** and select **Retry Using Same Inputs**.
- You can retry the deployment of Management Agents with modified installation details. To do so, click **Retry** and select **Update Inputs and Retry**.

2. Verify the installation:

- a. Navigate to the *Shared Agent* instance home and run the following command to see a message that confirms that the Management Agent is up and running:

```
$<AGENT_INSTANCE_HOME>/bin/emctl status agent
```

- b. Navigate to the *Shared Agent* home and run the following command to see a message that confirms that EMD upload completed successfully:

```
$<AGENT_INSTANCE_HOME>/bin/emctl upload agent
```

3. (Only for Graphical Mode) If you have restrictive Privilege Delegation Provider (PDP) configuration settings, enter the location of `nmosudo` in your PDP configuration file.

Enterprise Manager supports PDPs such as SUDO and PowerBroker that enable administrators to restrict certain users from running certain commands.

In Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2) or Release 3 (12.1.0.3), `nmosudo` is located in the `sbin` directory, which is in the agent base directory. For example, `<AGENT_BASE_DIRECTORY>/sbin/nmosudo`. In Enterprise Manager Cloud Control 12c Release 1 (12.1.0.1) [with or without Bundle Patch 1], `nmosudo` is located in the agent instance directory. For example, `<AGENT_INSTANCE_DIRECTORY>/bin/nmosudo`.

Therefore, when you install a 12.1.0.3 Management Agent, you must modify your PDP configuration file to update the new location of `nmosudo`.

For example, if you use SUDO as your PDP, the configuration file for SUDO is typically `/etc/sudoers`. In this file, update the following entry with the new location to `nmosudo`.

```
sudouser ALL : oracle /eminstall/basedir/sbin/nmosudo *
```

4. (Only for UNIX Operating Systems) Manually run the following scripts as a *root* user:

- If this is the first Oracle product you installed on the host, then run the `oraInstroot.sh` script from the inventory location specified in the `oraInst.loc` file that is available in the *Shared Agent* home.

For example, if the inventory location specified in the `oraInst.loc` file is `$HOME/oraInventory`, then run the following command:

```
$HOME/oraInventory/oraInstRoot.sh
```

- Run the `root.sh` script from the *Shared Agent* home:

```
$<AGENT_HOME>/root.sh
```

5. If you had ignored a prerequisite check warning about wrong time zone settings, run the following command and follow the steps it displays:

```
$<AGENT_INSTANCE_HOME>/bin/emctl resetTZ agent
```

6. By default, the host and the *Shared Agent* get automatically added to the Enterprise Manager Cloud Control console for monitoring. None of the targets running on that host get automatically discovered and monitored.

To monitor the other targets, you need to add them to Enterprise Manager Cloud Control either using the Auto Discovery Results page, the Add Targets Manually page, or the discovery wizards offered for the targets you want to monitor.

To add the host targets and the `oracle_emd` targets to the *Shared Agent*, run the following command:

```
$<SHARED_AGENT_HOME>/bin/emctl config agent addinternaltargets
```

For information about discovering targets in Enterprise Manager Cloud Control, refer to the chapter on adding targets in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

Note: If Oracle Management Agents 12c (12.1.0.x) hang frequently or do not respond on Solaris 9ux and 10ux operating systems, then refer to document ID 1427773.1 on My Oracle Support.

Installing Oracle Management Agent Software Now and Configuring Later

This chapter explains how you can install only the software binaries of Oracle Management Agent (Management Agent) at one point and configure the installation at a later stage. In particular, this chapter covers the following:

- [Overview](#)
- [Before You Begin](#)
- [Prerequisites](#)
- [Installation Procedure](#)
- [Configuration Procedure](#)
- [After You Install](#)

9.1 Overview

You can choose to install only the software binaries of the Management Agent at one point and configure it at a later stage to work with the associated Oracle Management Service (OMS). This approach enables you to divide the installation process into two phases, mainly the installation phase and the configuration phase.

During the installation phase, you invoke the `agentDeploy.sh` script passing the `-softwareOnly` argument to copy the software binaries and create an Oracle home for the Management Agent. During the configuration phase, you invoke the same script passing `-configOnly` to configure the software binaries.

Understandably, the installation phase takes much lesser time compared to the configuration phase because the installation phase involves only copying of binaries. This helps you plan your installation according to the time and priorities you have.

Note: This installation type is available only in silent mode.

Note: If you want to repoint your existing Management Agents to a new Oracle Management Service (OMS), then you must first deinstall those Management Agents and plug-ins, and then redeploy those Management Agents and plug-ins using the new OMS. This is typically done when you want to move from an Enterprise Manager Cloud Control system in a test environment to an Enterprise Manager Cloud Control system in a production environment.

When you repoint your existing Management Agents to a new OMS, you cannot move the targets monitored by the Management Agents, the target history, and the Management Agent history. The monitored targets and the history data is lost.

9.2 Before You Begin

Before you begin installing a Management Agent, review the points outlined in [Section 6.2](#).

9.3 Prerequisites

Before installing the Management Agent, ensure that you meet the prerequisites described in [Section 6.3](#).

9.4 Installation Procedure

To install only the software binaries of a Management Agent in silent mode, follow one of the procedures mentioned in [Section 6.4.2](#). While invoking the deployment script, ensure that you pass the `-softwareOnly` option:

```
<Software_Extracted_Location>/agentDeploy.sh AGENT_BASE_DIR=<absolute_path_to_agentbasedir> RESPONSE_FILE=<absolute_path_to_responsefile> -softwareOnly
```

For example, `/tmp/agtImg/agentDeploy.sh AGENT_BASE_DIR=/scratch/agent12c RESPONSE_FILE=/tmp/agtImg/agent.rsp -softwareOnly`

If the Management Agent is installed successfully, a message mentioning so is displayed on the command line.

Note: Do not pass the option `-forceConfigure`.

9.5 Configuration Procedure

To configure the software binaries of a Management Agent in silent mode, invoke the deployment script with the following options from the Management Agent home:

```
$<AGENT_HOME>/sysman/install/agentDeploy.sh AGENT_BASE_DIR=<absolute_path_to_agentbasedir> RESPONSE_FILE=<absolute_path_to_responsefile> -configOnly
```

For example, `/tmp/agtImg/agentDeploy.sh AGENT_BASE_DIR=/scratch/agent12c RESPONSE_FILE=/tmp/agtImg/agent.rsp -configOnly`

If the Management Agent is installed successfully, a message mentioning so is displayed on the command line.

Note:

- The response file you pass here is the same response file you passed in [Section 9.4](#).
 - Do not pass the option `-forceConfigure`.
-

9.6 After You Install

After you install the Management Agent, follow the steps outlined in [Section 6.5](#).

Part V

Advanced Installation and Configuration

This part describes the advanced installation and configuration tasks you can perform after you have installed Enterprise Manager Cloud Control and have started using the product.

In particular, this part contains the following chapters:

- [Chapter 11, "Configuring Enterprise Manager for Firewalls"](#)
- [Chapter 12, "Sizing Your Enterprise Manager Deployment"](#)
- [Chapter 13, "Installing ADP with Advanced Installation Options"](#)
- [Chapter 14, "Installing JVMD with Advanced Install Options"](#)
- [Chapter 15, "Integrating BI Publisher with Enterprise Manager"](#)

Performing Additional Configuration Tasks

This chapter contains the following sections:

- [Understanding Default and Custom Data Collections](#)
- [Enabling Multi-Inventory Support for Configuration Management](#)
- [Manually Configuring a Database Target for Complete Monitoring](#)
- [Modifying the Default Login Timeout Value](#)
- [Configuring Clusters and Cluster Databases in Cloud Control](#)
- [Collecting Client Configurations](#)
- [Configuring Privilege Delegation Providers](#)

10.1 Understanding Default and Custom Data Collections

When you install the Oracle Management Agent on a host computer, Enterprise Manager automatically begins gathering a default set of metrics that you can use to monitor the performance and availability of each targets on that host. For some of these target metrics, Enterprise Manager provides default threshold settings that determine when you will be notified that there is a problem with the metric.

See Also: *About Alerts* in the Enterprise Manager online help

For selected metrics, you can customize the default thresholds. When you make these types of customizations, Enterprise Manager saves the new settings in a file on the local disk. The following section provides more information about how these settings are saved.

10.1.1 How Enterprise Manager Stores Default Collection Information

Enterprise Manager stores the default collection criteria for each target in the following location on each Oracle Management Agent host:

`AGENT_HOME/sysman/admin/default_collection/`

The path is different with the plugin homes having the default_collection and metadata info for the targets. The agent home contains the collection/metadata details only for the other targets such as host, and oracle_emd.

For some targets, you can use the Oracle Enterprise Manager 10g Grid Control Console to modify the default metric collection settings. For example, you can modify the default thresholds for your host targets. When you make these types of

modifications, Enterprise Manager creates a new instance collection file in the following directory:

```
AGENT_HOME/sysman/emd/collection/
```

This collection file overrides the default collection information stored in the `sysman/admin/default_collection` directory.

10.2 Enabling Multi-Inventory Support for Configuration Management

Every time you install an Oracle software product on a host computer, Oracle Universal Installer saves information about the software installation on your hard disk. The directories and files that contain this software configuration information are referred to as the Oracle Universal Installer inventory.

See Also: *Oracle Universal Installer and OPatch User's Guide*

When you use Enterprise Manager to monitor your Oracle software installations, Enterprise Manager takes advantage of information saved in the Universal Installer inventory.

As it gathers information about the configuration of your host computer, by default, Enterprise Manager assumes that you have one Oracle Universal Installer inventory on the host. Specifically, Enterprise Manager recognizes the inventory that Oracle Universal Installer uses when you run the Universal Installer on the host.

However, in some cases, you may have more than one inventory. For example, you may have worked with Oracle Support to clone your Oracle software installations. For those cases, you can use the following procedure to be sure that Enterprise Manager can track and manage the software information in multiple inventories on the same host.

Caution: Enabling support for multiple inventories is optional and available only for advanced users who are familiar with the Oracle Universal Installer inventory architecture and who have previously worked with multiple inventories on a managed host. This procedure is not required for hosts where normal installations have been performed.

To set up Enterprise Manager so it can read multiple inventories on a host, follow these steps:

1. Locate the *OUIinventories.add* file in the following directory:

```
<agent_inst>/sysman/config
```

The Management Agent state listed in this example represents an installation for Database Control. For more information about the Management Agent state to use for other installations, see [Section 10.2.1, "AGENT_HOME Versus AGENT_STATE Directories"](#) on page 10-3.

2. Open *OUIinventories.add* using a text editor.

Instructions within the file describe the format to use when identifying multiple inventories, as well other techniques for mapping Oracle Homes.

3. Carefully review the instructions within the file.
4. Add entries to the file for each additional inventory on the managed host.

5. Save your changes and close the file.

During its next collection of host configuration information, Enterprise Manager will start gathering software configuration information from the inventories that you identified in the *OUIinventories.add* file, in addition to the default inventory that Enterprise Manager normally collects.

Alternatively, to see the data gathered from the additional inventories before the next regularly-scheduled collection, navigate to the Host home page in the Grid Control console, click the **Configuration** tab, and click the Refresh Data icon next to the page timestamp.

Note: If there are any irrecoverable problems during the collection of the default inventory (for example, if the inventory file or directory protections prevent Enterprise Manager from reading the inventory), inventories listed in *OUIinventories.add* file are also not collected.

If the Enterprise Manager is able to read the default inventory, but there is a problem reading an additional inventory listed in the *OUIinventories.add* file, Enterprise Manager issues a collection warning for those inventories. However, Enterprise Manager does collect the configuration information for the other inventories.

10.2.1 AGENT_HOME Versus AGENT_STATE Directories

The Management Agent recognizes two main directory structures; its installation directory where software binaries and all unchanging metadata are stored, and its configuration/state directory where all customizations and output/log content are stored and/or generated. In a normal Management Agent installation, these two directories are the same. However, they can be different in the following cases:

- Database Control installation (`$ORACLE_HOME` versus `$ORACLE_HOME/<nodename>_<sid>`)
- State-only Management Agent deployment (using the `emctl deploy agent` command -- `$ORACLE_HOME` versus `$EMSTATE`)

In each of the above cases, there will be multiple instances of the Management Agent running off the same binaries installation. The different instances have different locations to maintain separate configurations but use the same set of binaries. The command `emctl status agent` provides the values of the Management Agent's binaries and state locations.

The `AGENT_BASE` or `ORACLE_BASE` directories contain the Management Agent Binaries. This section of the directory is read-only. The new Management Agent creates multiple Oracle Homes under a single parent directory called `AGENT_BASE` or `ORACLE_BASE`.

The Agent State directory is usually placed under `AGENT_BASE`; however, by design the Agent State directory could be located in any location. For example, in the case of an NFS installation, the Agent State Directory is not placed under `AGENT_BASE`. This is the only directory into which non-deployment agent code should be written.

The default name set by the installer for the state home (or instance home) is `agent_inst`. The state home must have world read and execute permission.

10.3 Manually Configuring a Database Target for Complete Monitoring

When you first discover an Oracle Database target, you should check the monitoring credentials to be sure the password for the DBSNMP database user account is set correctly in the database target properties.

Besides setting the monitoring credentials, no other configuration tasks are required to monitor an Oracle Database target.

However, when you monitor an Oracle9i database, there is some additional configuration required if you want to monitor certain types of database performance metrics using the Grid Control console.

To monitor these additional performance metrics Enterprise Manager requires that Oracle Statspack and some additional Enterprise Manager packages be installed and configured in the database you are monitoring.

See Also: "Using Statspack" in *Oracle Database Performance Tuning Guide and Reference* in the Oracle9i Documentation Library

If these additional objects are not available and configured in the database, Enterprise Manager will not be able to gather the data for the complete set of performance metrics. In addition, Enterprise Manager will not be able to gather information that otherwise could be readily available from the Database home page, such as Bad SQL and the Top SQL Report.

You can use the Configure Database wizard in the Grid Control console to install the required packages into the database, or you can use the following manual procedure.

See Also: "Modifying Target Properties" in the Enterprise Manager online help for information on configuring managed targets, including database targets

To manually install Statspack and the other required database objects into an Oracle9i database that you are managing with Enterprise Manager, you can use SQL*Plus and the following procedure:

1. Log in to the database host using an account with privileges that allow you to write to the database home directory and to the Management Agent home directory.

For each of the commands in this procedure, replace AGENT_HOME with the actual path to the Oracle Management Agent home directory and replace ORACLE_HOME with the path to the database home directory.

2. Start SQL*Plus and connect to the database using the SYS account with SYSDBA privileges.

For example:

```
$PROMPT> ./sqlplus "connect / as sysdba"
```

3. Enter the following command to run the database dbmon script:

```
SQL> @AGENT_HOME/sysman/admin/scripts/db/config/dbmon
```

The script will display the following prompt:

```
Enter value for dbm_password:
```

4. When prompted, enter the password for the DBSNMP account.

The script performs several configuration changes and returns you to the SQL*Plus prompt.

5. Connect as the DBSNMP user.

For example:

```
SQL> connect DBSNMP
```

6. Enter the following command:

```
SQL> @AGENT_HOME/sysman/admin/scripts/db/config/response.plb
SQL> grant EXECUTE on dbsnmp.mgmt_response to OEM_MONITOR;
```

Note: The above script should not be run on an Oracle database of version 8.1.7 or prior. Oracle does not support SQL Response Time for 8.1.7 databases or prior.

7. Connect as SYS and enter the following command to create the PERFSTAT user:

```
SQL> @ORACLE_HOME/rdbms/admin/spcreate
```

Note: The spcreate script will prompt you for a default tablespace and default temporary tablespace for the PERFSTAT user. Do not specify the SYSTEM tablespace as the default tablespace for the PERFSTAT user. For more information, see "Using Statspack" in the *Oracle Database Performance Tuning Guide*

8. Connect as the PERFSTAT user.

For example:

```
SQL> connect PERFSTAT;
```

9. Enter the following commands from the PERFSTAT user account:

```
SQL> define snap_level='6';
SQL> define cinterval='1';
SQL> define cjobno='-1';
SQL> @AGENT_HOME/sysman/admin/scripts/db/config/spset
```

10. Connect as the SYS user and enter the following command:

```
SQL> grant OEM_MONITOR to dbsnmp;
```

11. If the database you are modifying is an Oracle8i database, also enter the following commands as the SYS user:

```
grant select on sys.ts$ to OEM_MONITOR;
grant select on sys.seg$ to OEM_MONITOR;
grant select on sys.user$ to OEM_MONITOR;
grant select on sys.obj$ to OEM_MONITOR;
grant select on sys.sys_objects to OEM_MONITOR;
grant select on sys.file$ to OEM_MONITOR;
grant select on sys.attrcol$ to OEM_MONITOR;
grant select on sys.clu$ to OEM_MONITOR;
grant select on sys.col$ to OEM_MONITOR;
grant select on sys.ind$ to OEM_MONITOR;
grant select on sys.indpart$ to OEM_MONITOR;
grant select on sys.indsubpart$ to OEM_MONITOR;
```

```
grant select on sys.lob$ to OEM_MONITOR;
grant select on sys.lobfrag$ to OEM_MONITOR;
grant select on sys.partobj$ to OEM_MONITOR;
grant select on sys.tab$ to OEM_MONITOR;
grant select on sys.tabpart$ to OEM_MONITOR;
grant select on sys.tabsubpart$ to OEM_MONITOR;
grant select on sys.undo$ to OEM_MONITOR;
```

12. For any supported database version, enter the following command from the SYS account:

```
SQL> show parameter job_queue_processes
```

If the output from the *show parameter* command is zero, then perform the following steps to modify the *job_queue_processes* initialization parameter:

If you start the database using an spfile, enter the following command:

```
SQL> alter system set job_queue_processes = 2 SCOPE=BOTH;
```

Otherwise, do the following:

- a. Enter the following command:

```
SQL> alter system set job_queue_processes = 2;
```

- b. Exit SQL*PLUS and update the *init.ora* database configuration file with the following entry so the parameter will be applied whenever the database is restarted:

```
job_queue_processes=2
```

13. Exit SQL*Plus and change directory to the following directory in the home directory of the Management Agent that is monitoring the database:

```
AGENT_HOME/bin
```

14. Reload the Management Agent by entering the following command:

```
$PROMPT> ./emctl agent reload
```

15. Using the Cloud Control console, return to the Database home page and verify that the Bad SQL and Top SQL Report metrics are now being gathered.

10.4 Modifying the Default Login Timeout Value

To prevent unauthorized access to the Grid Control console, Enterprise Manager will automatically log you out of the Grid Control console when there is no activity for a predefined period of time. For example, if you leave your browser open and leave your office, this default behavior prevents unauthorized users from using your Enterprise Manager administrator account.

By default, if the system is inactive for 45 minutes or more, and then you attempt to perform an Enterprise Manager action, you will be asked to log in to the Grid Control console again.

Caution: As stated in the previous paragraphs, the timeout value for logging in to the Grid Control console is defined in order to protect your system from unauthorized logins. If you make changes to the login timeout value, be sure to consider the security implications of leaving your session open for other than the default timeout period.

To increase or decrease the default timeout period:

1. Set the value for the OMS ORACLE_HOME environment variable. For example:

```
export ORACLE_HOME=/u01/app/oracle/product/Middleware/oms
```

2. Navigate to the following directory:

```
OMS $ORACLE_HOME/bin
```

3. Issue the following command to increase the timeout. In this example, you can increase the timeout to 60 minutes.

```
./emctl set property -name oracle.sysman.eml.maxInactiveTime  
-value 60 -sysman_pwd oracle12
```

4. Stop and restart the OMS to reflect the new property value:

```
./emctl stop oms
```

```
./emctl start oms
```

Note: The default timeout value does not apply when you restart the Web server or the Oracle Management Service. In both of those cases, you will be asked to log in to the Grid Control console, regardless of the default timeout value.

10.5 Configuring Clusters and Cluster Databases in Cloud Control

This section describes how to configure cluster databases and discover instances.

10.5.1 Configuring Cluster Databases

After you have added the cluster target, you can add a cluster database target either from the Databases page or from the All Targets page.

To add a cluster database target, perform the following steps:

1. In the Enterprise Manager Cloud Control console, select one of the following entry locations:
 - From the Databases page, click **Add**. The Add Database Instance Target: Specify Host page appears.
 - From the All Targets page, select **Database Instance** from the Add drop-down menu, then click **Go**. The Add Database Instance Target: Specify Host page appears.
2. Specify any host member of the cluster target where the cluster databases reside, then click **Continue**. The Add Database: Specify Source page appears.
3. Keep the default option (on all hosts in the cluster) selected and click **Continue**. This option sends requests to all Management Agents in the cluster to perform discovery.

After target discovery completes, the newly discovered RAC databases appear in the *Targets Discovered on Cluster* page. If the databases do not appear, see the *Troubleshooting* section below.

4. If the desired targets do not appear in the Cluster Databases table, or if the discovered targets are not configured appropriately, click **Manually Add**. The Properties page of the Configure Cluster Database wizard appears.
5. Provide the required values for the Properties table.
6. You must specify at least one instance in the Instances table. If no instances appear in the table, click **Add**. The Properties: Add Instance page appears. Provide the required values, then click **OK**. The Properties page of the Configure Cluster Database wizard reappears.
7. Click **Next**. For database versions 10.1 and higher, Enterprise Manager bypasses the Install Packages, Credentials, and Parameters steps, and goes directly to the Review page.
8. Click **OK**. The Targets Discovered on Cluster page reappears, and displays the newly added cluster database and instances.

See Also: The Enterprise Manager online help for more information about configuring cluster databases

10.5.2 Discovering Instances Added to the Cluster Database

If you need to configure additional instances, follow these steps:

1. In Enterprise Manager, select **Databases** on the Targets page, then navigate to the desired **Cluster Database Home** page.
2. Click **Monitoring Configuration** in the Related Links section. The Properties page of the Configure Cluster Database wizard appears.
3. Provide the required information in the Properties table at the top of the page.
4. Examine the Instances table. One or more additional instances may exist, but may not appear in the Instances table. If this is the case, click **Add** to discover the instance in the cluster database. The Properties: Add Instance page appears.
5. Provide the required information, then click **OK**. The wizard Properties page reappears, and displays the added instance view.
6. Click **Check Connection** to ensure that the connection is working.

See Also: The Enterprise Manager online help for more information about discovering instances added to the cluster database

10.5.2.1 Troubleshooting

If you encounter configuration issues, check the following required conditions to ensure that automatic discovery is able to function correctly:

- The host user running the Management Agent is able to run the SRVCTL utility in the Oracle home and retrieve the database configuration.
- The host user running the Management Agent is able to connect to the database through SQLPLUS using OS authentication.
- The Oratab (UNIX) or Registry (Windows) contains information about the database.

If automatic discovery still does not resolve your configuration issues after you have ensured the conditions previously listed, you can manually configure cluster databases (see [Section 10.5.1, "Configuring Cluster Databases"](#)).

10.6 Collecting Client Configurations

A client is comprised of a host and operating system user. Client configuration data that is collected includes:

- Hardware for the client.
- Operating system (includes information such as operating system properties, file systems, and patches) for the client.
- Operating system-registered software.
- Network data, which includes:
 - Latency to the Web server
 - Bandwidth to the Web server
- Client-specific data items that describe the configuration of the browser used to access the client configuration collection applet, which includes:
 - Browser type (vendor)
 - Browser version
 - JVM vendor (of the JVM used to run the client configuration collection applet)
 - JVM version (of the JVM used to run the client configuration collection applet)
 - Proxy server (if specified)
 - Proxy server exceptions
 - Browser cache size (MB)
 - Browser cache update frequency
 - Supported HTTP version
- Other client-oriented data items, including:
 - Client configuration collection applet identifier (version, defined in the applet code)
 - Application URL (from which the client configuration collection applet was accessed)
 - Boot drive serial number (not available from diskless systems)
 - Collection timestamp (from the client configuration collection applet JSP)
 - Collection durations, in milliseconds
 - Client IP address
 - Effective client IP address - if a network proxy server is being used between the client and the Web server providing the client configuration collection applet, the effective client IP address will be the IP address of the proxy server.

10.6.1 Configuring the Client System Analyzer

The Client System Analyzer (CSA) allows Web server administrators to collect and analyze end-user client data. The client data is collected by an applet, diagnosed and sent back to the CSA application. The Oracle Management Agent uploads this data to the Enterprise Manager Management Repository. After the client configuration data has been collected by the client configuration collection applet and written to the Web server directory specified by the CSA applet, the client configuration data is uploaded to the Oracle Management Repository.

You can either use the Client System Analyzer in the Cloud Control application pre-installed with Enterprise Manager or you can deploy CSA independently to your Web server.

10.6.1.1 Client System Analyzer in Oracle Cloud Control

Client System Analyzer in Cloud Control - An instance of CSA is pre-installed with Enterprise Manager. If you use this option, you can collect client data without setting up a separate Web server. To activate the pre-installed CSA application in Enterprise Manager, click **Configuration**, then click **Client System Analyzer in Cloud Control** and use the button provided to activate the application. Once CSA is activated, end-users can use the URL provided to run the CSA applet. The CSA applet can collect base client configuration information from client systems and Oracle Collaboration Suite client information from Oracle Collaboration Suite client systems.

- To download the CSA applet and have it collect base client configuration information, a client should use the Client System Analyzer URL in this format:
http[s]://management-service-host:port/em/public/ecm/csa/CSA
- To download the CSA applet and have it collect Oracle Collaboration Suite client configuration information, a client should use the Client System Analyzer URL in this format:
http[s]://management-service-host:port/em/public/ecm/csa/CSA?application=OCS

10.6.1.2 Deploying Client System Analyzer Independently

The Client System Analyzer Application can be deployed independently to any J2EE-capable Web server. Click the **Deployments** tab. Then click **Getting Started with Client System Analyzer** and click **Deploy Client System Analyzer Application**. Follow these steps to deploy the CSA applet and collect the client configuration data.

1. Download the CSA Application:

The CSA application includes the CSA directory along with the necessary JSP applet files. The application is packaged as an EAR file. To download this default EAR file, click **Download Client System Analyzer Application**. You can customize the default CSA EAR file by modifying the following:

- Rules - This file contains a default set of rules against which the client data is evaluated. You can customize and add rules before deploying CSA.
- Context parameters - You can customize the context parameters in the *web.xml* file.
- Custom classes - You can provide customized applet classes that can be used to perform tasks like collecting additional data, changing the behavior of the applet, and performing certain operations on the client.

2. Deploy CSA to any J2EE Web server.

The CSA application is deployed on an Application Server as a regular J2EE application. Once the CSA application is deployed, context parameters can be changed similar to other web applications.

3. Direct users to the CSA.

In order for the client data to be collected, the user must access the CSA application. Users can access the CSA JSP page directly or by using a link from another application. Users can be automatically redirected to CSA using the following methods:

- HTTP Server (Apache's *mod_rewrite*) - This option does not require changes in the Web application.
- Servlet Filter - A servlet filter is a program that filters requests to and from the server. The *CSA_filter.jar* file contains the servlet filter classes. The servlet filter and the filter mapping need to be added to the Web application.
- CSA Redirection JSP - The CSA Redirection JSP (*CSARedirect.jsp*) page can be included into the Web application.

4. Configure Enterprise Manager.

Collected client data is recorded in the Receive File Directory on the Web server. To upload the collected client data into Enterprise Manager, you need to do the following:

- Add a CSA Collector Target to the Enterprise Manager Management Agent. To do so, click **Add Collector** and choose a target from the list.
- Specify the absolute path to the Receive File Directory. The path specified must be the same as the path specified in the *outputDir* parameter of the CSA application. By default, the client data is stored in the Receive File Directory *csa_results* under the context root of the Client System Analyzer Web application, but this can be configured by changing the applications's *outputDir* context parameter.

5. Test the CSA Deployment.

To verify the CSA deployment, click the URL of the CSA page and check if the client data is collected.

10.6.2 Configuration Parameters

The Client System Analyzer (CSA) can be further configured by modifying the context parameters in the CSA application's WAR file.

Table 10–1 Configuration Parameters

Parameter	Description	Default Value
alertWhenDone	If set to true, a message indicating that the applet has been executed is displayed.	false
appletJAR	The name of the JAR file.	CSA.jar
application	The name of the application associated with this CSA instance. If the application parameter value is not specified, then the Collection Tag has a value of Default.	none
autoRedir	If set to "true", this causes the CSA JSP page to automatically use the Sun JVM if JVM was set to JInitiator and the client does not have the appropriate version of JInitiator installed.	false

Table 10–1 (Cont.) Configuration Parameters

Parameter	Description	Default Value
bwTestFile	The name of the file that is downloaded from the server during the bandwidth test.	CSA.mb (included with CSA)
bwTestMsec	The amount of time the applet should spend on the bandwidth test. The applet computes bandwidth by counting the number of bytes it can download in this interval.	200 ms
classid	The "classid" field for the OBJECT tag. Applicable only if JVM is set to "JInitiator." The classid for Sun is "clsid:8AD9C840-044E-11D1-B3E9-00805F499D93" codebase - the "codebase" field for the OBJECT tag. Applicable only if JVM is set to "JInitiator."	None – this field MUST be set if JVM is set to "JInitiator," and is ignored otherwise
codebase	The codebase field for the OBJECT tag. Applicable only if the JVM is set to "JInitiator".	The default for Sun is http://java.sun.com/products/plugin/autodl/jinstall-1_4_2-windows-i586.cab#Version=1,4,0,0
collectCookie	The list of the names of cookies to be collected. This parameter is a comma-separated list of cookie names. Only cookies for the current OS user in the current browser will be collected. The Administrator can specify asterisk (*) to collect all of the current user's cookies for the current browser.	If this field is not present, no cookies will be collected.
cookieDomain	The domain of the CSA cookie.	If either the domain or path of the cookie is not set, cookies are disabled
cookieMaxAge	The maximum duration, in seconds, of the cookie on the client machine.	1 year
cookiePath	The path of the CSA cookie	If either the domain or path is not specified, cookies are disabled.
customClass	The name of the class used to collect custom data.	none – the default behavior is for no custom code to be executed
customKey1 customKey2 customKey3	The values of the three custom keys. All client collections done by a CSA JSP page that uses this deployment descriptor will have these values for the custom keys. These values can be overridden by custom code.	If no custom key values are specified, none will be collected (unless they are collected by custom code)
descriptionFile	The full path of a text file containing the description that will be displayed on the deployment page. The contents of the file should be HTML-formatted text.	None

Table 10–1 (Cont.) Configuration Parameters

Parameter	Description	Default Value
destURL	Specifies the destination URL. This is the URL to which the "Proceed" button on the CSA JSP page is linked.	If no destURL is specified, the "Proceed" button will take the user to the referring page; if there is no referring page, the "Proceed" button will not be displayed.
destURLResultsParam	Specifies the name of the URL parameter that will be added to the "destination URL" to indicate the client's compliance level. For example, if the value was "compliance", and the client's overall compliance level was critical, then the parameter "compliance=critical" would be added to the destination URL.	Sun
JVM	This determines the type of JVM that is to be used. If the value is ""Sun," the JSP page will direct the browser to use the Sun JVM. If the value is "Oracle," the page will direct the browser to use Oracle Jinitiator. If the value is "any," the JSP will write out the standard "applet" tag, which causes the client to use whichever JVM is plugged into the browser.	Sun
maxExecInterval	Parameter that is added to CSA cookie payload. When the redirection logic reads the cookie, if the timestamp of the cookie differs from the current time by more than this value, the applet is deployed again. This parameter can be overridden by the "csa execInterval" context parameter in the redirection JSP filter.	90 days
maxFileSize	Maximum amount of data, in KB, that can be posted back to the receiver in a single request. If the size of the posted data exceeds this limit, the request is rejected and any data already written to the hard drive is deleted.	100
maxOutputFiles	Maximum number of output files that can be present in XML OutputDir.	100
outputDir	Directory to which CSA configuration xml files will be written. Both the applet page and the receiver page must read this parameter, and this parameter must be identical for both pages.	By default, the output files are written into the "csa_results" subdirectory of the application root directory (if the application root directory exists, and if the subdirectory exists or can be created). Using the default value for this parameter is not recommended.
outputEnabled	Enables or disables creation of output XML files. Applicable to both applet and receiver pages.	By default, the XML files are created and stored in the XMLOutputDir.

Table 10–1 (Cont.) Configuration Parameters

Parameter	Description	Default Value
pluginspage	Used to direct the user to the JVM installer under Netscape, since Netscape does not support automatic installation. Applicable only if JVM is JInitiator. Default for Sun is http://java.sun.com/products/plugin/index.html#download	none - This field must be set if JVM is set to "JInitiator" and is ignored otherwise.
receiver	The URL to which the applet should post the collected data. Note: When setting this parameter, the administrator must ensure that the version of the receiver is the same as the version of the applet.	Default is to look for "CSAr.jsp" in the same path as the CSA JSP page
ruleFile	Specifies the path on the server, relative to the web application root, of the file that contains the rules to be evaluated.	rules.xml
script	Specifies a script, provided by the administrator, which can be run on the CSA XML file before it is marked for upload by the Management Agent.	none - If no script is specified, no script will be run.
type	The type field for the OBJECT tag rendered by the CSA JSP page to deploy the applet. This is only applicable if the JVM is set to JInitiator. If the JVM is set to Sun, the type is application/x-java-applet.	none - this field must be set if JVM is set to "JInitiator," and is ignored otherwise
viewData	If set to true, this parameters allows the end-user to view the collected data after it is posted to the server.	false

In addition to these parameters, the CSA redirection parameters can also be configured. Redirection can be enabled either by using a servlet filter or by including a CSA redirection JSP file in some other page. The following context parameters must be available for the redirection to work.

Table 10–2 Configuration Parameters

Parameter Name	Description	Default Value
csaURL	The URL of the CSA JSP page to which the user should be redirected.	No default: This value must be set or redirection cannot work.
execInterval	The interval, in seconds, between executions of CSA. If the difference between the cookie's age and the current server time is greater than execInterval, the user is redirected.	None. If the execInterval is not set, then the user is only redirected if there is a CSA cookie.
redirectURL	The URL to which the user should be directed after CSA has executed	None. If this parameter is not set, the user is directed back to the originally requested page
UIMode	0 - synchronous (in the current browser window) 1 - asynchronous visible 2 - asynchronous invisible	synchronous

10.6.2.1 Associating the Parameters with an Application

In certain cases, different sets of parameters may be required for different applications. For example, two different applications may have different rule sets and custom code, and the administrator may want to associate them with different CSA Collector Targets. In this scenario, the administrator can specify the *ruleFile*, *appletJar*, *script*, and *outputDir* parameters for a particular application by using the context parameters

`<application name> ruleFile`, `<application name> appletJar`, and so on. If an application is specified, either as a context parameter or through the URL, then CSA is executed using the parameter values specific to the application. If no application is specified, or if one of the parameters for an application is not overridden, the default parameters are used.

10.6.3 Rules

Custom rules can be supplied to the CSA application so that the users receive immediate feedback as to whether their systems satisfy certain constraints. A sample RULES file is shown in [Example 10-1](#) followed by a description of each tag contained in the file.

Example 10-1 Sample RULES

```
<RULES>
<RULE>
<NAME>Client has sufficient memory</NAME>
<DESCRIPTION>Checks to see if the client has enough memory to run the
application</DESCRIPTION>
<VIOLATION> //ROWSET[@TABLE='MGMT_ECM_HW']/ROW/AVAIL_MEMORY_SIZE_IN_MB[number()
< < $arg=SIZE$] </VIOLATION>
<SEVERITY level="CRITICAL">
<PARAM id='SIZE'>100</PARAM>
<MOREINFO>
<TEXT>Application cannot run with less than 100 MB. </TEXT>
</MOREINFO>
</SEVERITY>
<SEVERITY level="WARNING">
<PARAM id='SIZE'>150</PARAM>
<MOREINFO>
<TEXT>Approaching minimum memory level</TEXT>
</MOREINFO>
</SEVERITY>
</RULE>
</RULES>
```

[Example 10-1](#) demonstrates a rule that can be used to check whether or not the client has sufficient memory to run the application. The `<VIOLATION>` is an XPATH expression that the applet will evaluate against an XML file that contains all of the data it has collected. Since the violation is an XPATH expression embedded in an XML file, certain characters in the XPATH, such as '`<`', '`>`', and '`&`', must be replaced with entities. If the XPATH expression returns a non-null node set, the rule has failed. In this case, the rule will fail if the client's available memory is less than a certain amount. The actual amount that triggers a violation can be configured by using different severity levels.

In [Table 10-3](#), the applet will first replace the substring "`$arg=SIZE$`" in the VIOLATION expression with "100" and then evaluate the expression. If the client's available memory is less than 100 MB, then the rule will fail with critical status. The applet will indicate the status along with the message *Application cannot run with less than 100 MB of memory*. If the rule passes through successfully, the applet will then replace `$arg=SIZE$` with 150 and try again; if the rule fails, the applet will display the message *Approaching minimum memory level*. If the applet goes through all specified severity levels and does not find a violation, the rule is successful.

Table 10–3 Tags in the RULES File

Tag Name	Description
RULES	This is the top-level tag for the XML file
BUNDLE	This tag specifies the resource bundles used for translation. The value of the tag is either the name of a file or a Java class name. The rule engine reads this string and first attempts to find a file in the applet JAR that has this name. This file is expected to contain a mapping of resource IDs to strings in various languages. If such a file does not exist, then the string is treated as the name of a Java resource bundle class. Strings in a resource bundle are referenced using the syntax <code><resource id>@<bundle id></code> .
PRECONDITION	This tag is used to specify an XPATH expression that must return a non-null node set in order for a rule to be evaluated. The "id" attribute specified the ID of the precondition. A rule can specify a list of preconditions that should be evaluated by listing their IDs.
RULE	This tag represents an individual node that is to be evaluated. The rule's severity is specified using a <code><SEVERITY></code> tag. At least one severity tag must be specified for a rule. The tag has an optional "precondition" attribute, which is used to specify a list of precondition IDs separated by commas. Before the rule is evaluated, all of the preconditions must be met. If the pre-conditions are not met, the rule has a status of "Not Applicable" and is not displayed in the client UI at all. The children of a RULE tag are NAME, DESCRIPTION, VIOLATION, SEVERITY, and MOREINFO.
NAME	This tag specifies the name of the rule and identifies the tag in the repository. Note: This tag must contain a value and cannot be blank.
DESCRIPTION	This is the description of the rule.
VIOLATION	This tag lists the violations that are to be checked for a given rule. The violation is specified in the CSA Condition Language.
SEVERITY	A rule can have three severity levels: INFO, WARNING, and CRITICAL. The SEVERITY node must contain a number of ARG children equal to the number of arguments that can be accepted by the expression in the VIOLATION node. When the rule engine evaluates a rule, it evaluates the condition in VIOLATION for each of the sets of arguments specified in the severity levels, starting with CRITICAL and moving down in order of severity. As soon as the engine encounters a condition that fails, the rule is declared a failure, with a severity level equal to the severity level of the argument that caused the failure. If the conditions for all specified levels are met, the rule passes.
PARAM	This tag specifies the value of an argument that should be substituted into an expression. The 'id' attribute of the tag must match the name of one of the arguments in the expression.
MOREINFO	This tag specifies the information that is displayed if the user clicks the "more information" button that is displayed next to a failed rule. The children of MOREINFO are TEXT and ARG. Note: The MOREINFO node can be a child either of the severity node (in the case where multiple severities are specified) or of the rule itself.

Table 10–3 (Cont.) Tags in the RULES File

Tag Name	Description
TEXT	This tag specifies the text to be displayed when the "More Info" button is clicked. The "resource" attribute specifies a string in a resource bundle – if this string is not present, the value of the node is displayed instead. The text (either in the resource bundle or in the node itself) can specify a location for arguments to be inserted by using "{0}", "{1}", and so on. In this case, the expressions in the ARG nodes are evaluated and inserted into the text in the order in which they are specified. If there are more ARG nodes specified than there are slots in the string, the extra nodes are ignored.
ARG	This tag specifies an expression in the CSA Condition Language that can be evaluated and inserted into the MOREINFO text.

See Also: Enterprise Manager online help associated with the Getting Started with CSA page

10.6.4 Customization

In addition to writing custom classes to collect custom properties, the administrator can also specify custom properties in the deployment descriptor. Custom property names are specified by including a context parameter of the form *csa value_<name>*. The <name> field of the context parameter name is treated by the Client System Analyzer (CSA) as the custom property name, and the value of the parameter is treated as the custom property value. Similarly, administrators can specify the type, *type_ui*, *name_ui*, *display_ui*, and *history_tracking* fields for a custom property by using *csa_type_<name>*, *csa_type_ui_<name>*, *csa_name_ui_<name>*, *csa_display_ui_<name>*, and *csa_history_tracking_<name>* parameters, respectively. Custom properties can also be specified on the CSA Applet URL, using the same naming convention.

10.6.5 CSA Deployment Examples

The following sections outline sample use cases for client configurations.

10.6.5.1 Using Multiple Collection Tags

An administrator can check the compatibility of users with two distinct Web applications. The first is an online teaching website that delivers content using a number of various plug-ins, allowing an administrator to be sure that all users have the required installed plug-ins. The second is a software distribution portal that allows an administrator to ensure that all users downloading software from the portal have the required hardware and operating system. In this case, though both applications require their own set of rules, the administrator can use a single CSA instance for both applications through the use of collection tags displayed in the following list:

1. Choose a collection tag for each application, such as "teaching" and "distribution".
2. Create two separate rule files, one for each application.
3. Use context parameters to map each rule file to the corresponding application, as shown in [Example 10–2](#).
4. Create the appropriate links from each application to CSA. The links from the teaching and distribution applications should have *application=teaching* and *application=distribution*, respectively, in the query string. This ensures that users of each application have the correct collection tags when running CSA.

Example 10–2 Using Collection Tags for Selecting a Rule File

```
<context-param>
  <param-name>csa teaching ruleFile</param-name>
  <param-value>teaching_rules.xml</param-value>
</context-param>

<context-param>
  <param-name>csa distribution ruleFile</param-name>
  <param-value>distribution_rules.xml</param-value>
</context-param>
```

[Example 10–2](#) shows only the use of collection tags for selecting a rule file. However, collection tags can be used for any of the CSA context parameters.

Collection tags also affect how client configurations are stored in the Enterprise Manager Management Repository. If the user comes to CSA using the link from the teaching application in [Example 10–2](#), then in addition to running the rules for the *teaching* collection tag, CSA also causes this tag to be stored with the client configuration data in the Management Repository. The collection tag forms part of the unique identifier for the client configuration, which makes it possible for a single client to have multiple configurations in the Management Repository, each with its own tag. Collection tags can be associated with Enterprise Manager targets in order to restrict access to client data; an Enterprise Manager user can only view a client configuration if he or she has view privileges on a target that is associated with the collection tag for that client configuration.

In [Example 10–2](#), suppose that host H1, application server A1, and database D1 are used to host the teaching application, while host H2, application server A2, and database D2 are used for the distribution application. All 6 targets are monitored by Enterprise Manager, with user X having access to A1, H1, and D1 and user Y having access to A2, H2, and D2. Since each of the two Enterprise Manager users is monitoring the resources used for one of the applications, it may also make sense to have each user also monitor the application's clients. In that case, an Enterprise Manager super user would associate the *teaching* tag with A1, D1, or H1 and associate the *distribution* tag with A2, D2, or H2. This allows user X to see all client configurations with the *teaching* tag and user Y to see all configurations with the *distribution* tag.

10.6.5.2 Privilege Model for Viewing Client Configurations

Collection Tags are used to restrict access to client data in Enterprise Manager. A client configuration is visible to the user only if the Collection Tag for that configuration is associated with a target on which the user has View privileges. For example, if collection tag C is associated with target T1, then only those users that can view target T1 will be able to see client configurations that have tag X. In [Example 10–2](#), user X will be able to see client configurations with the *teaching* tag because user X has view privileges on targets that are associated with the *teaching* tag. However, user X will not be able to see any client configurations with the *distribution* tag because that tag is not associated with any targets that user X can see. Super users can associate collection tags with targets by using the Collection Tag Associations page, which can be accessed from the Deployments tab or from the Client System Analyzer in Cloud Control link on the Setup page. Super users can view all client configurations regardless of any collection tag associations.

10.6.5.3 Using the Customization API Example

If the administrator is interested in the user's settings for an e-mail client in addition to the normal CSA data, the administrator can add this information to the other data collected by CSA through the use of the customization API, as shown in [Example 10-3](#).

1. Create the Java classes required to gather the information. The administrator can create as many classes as necessary, but there must be at least one class that implements `oracle.sysman.eml.ecm.csa.CSAResultInterface` and one that implements `oracle.sysman.eml.ecm.csa.CSACustomInterface`, both of which are shown in [Example 10-3](#). Assume that the former is `acme.csa.custom` and the latter is `acme.csa.result`.
2. Set the value of the "customClass" parameter in CSA to "acme.csa.custom"

Example 10-3 Customization API

```
public interface CSACustomInterface {

    /**
     * requires: none
     * effects: returns a CSAResultInterface object that may contain custom
     * properties. Other effects are determined by the customActions method
     * in the implementing class
     * modifies: unknown - dependent on implementing class.
     * @param inputData contains client config data collected by default, plus
     * applet parameters, etc. None of the data in the inputData is guaranteed
     * to be there as there could have been collection errors.
     * @return a data structure that may contain custom properties
     */
    CSAResultInterface customActions(CSAInputInterface inputData);
}

public interface CSAResultInterface {

    /**
     * requires: none
     * effects: returns an array of custom properties
     * modifies: none
     * @return String[][7] where ...
     *
     * String[i][0] is a name
     * String[i][1] is a value of the i-th row. (Type and name must be unique.)
     * String[i][2] is a type/category of data (could be null),
     * String[i][3] is the displayed value of the name of the property
     * String[i][4] is the displayed value of the type of the property
     * String[i][5] indicates data item (ie "Y") whose history should be computed
     * String[i][6] indicates data item (ie "Y") should be displayed in default UI
     */
    String[][] getResultsData();
}

public interface CSAInputInterface {

    /**
     * Get data value for given name
     * requires: name is not null
     * effects: returns the data value associated with the name
     * modifies: none
     * @param name the name of the key whose value is to be returned
     * @return the value associated with name
     */
}
```

```
*
*/
String getDataValue(String name);

/**
 * Get table-formatted data.
 * requires: name is not null
 * effects: returns the table with this name
 * modifies: none
 * @param name the name of the table
 * @return the rows of the child tables
 */
CSAInputInterface[] getDataTable(String name);
}
```

The additional data collected by the custom code will be stored in the table `MGMT_ECM_CSA_CUSTOM`. To add data to this table, the custom code returns it in an object that implements *CSAResultInterface*. The custom code can also manipulate the normal data collected by CSA by modifying the *CSAInputInterface* object passed to the `customActions` method by the applet.

Since the custom code is executed before rules are evaluated, the administrator can also write rules based on the custom data. For example, if the administrator wants to write a rule that raises a critical error if the user does not have the correct IMAP server set up his or her e-mail client, the administrator would write custom code that retrieves the IMAP server settings and stores them in the `MGMT_ECM_CSA_CUSTOM` table and then writes a rule that checks these values.

10.6.5.4 Using the CSA Servlet Filter Example

Since CSA does not involve the use of a Management Agent on the user's machine, there is no way to keep the data in the Management Repository up to date unless end users run CSA periodically. One way to ensure that they do is to check whether or not users have run CSA recently, and if they have not, to inform them to run CSA again. This check can be accomplished using the CSA servlet filter provided by Oracle.

The CSA servlet filter works by checking the cookie that CSA sets in the user's browser whenever it runs. The payload of this cookie indicates the time at which CSA was last run. To use the filter, the administrator places it in front of some frequently accessed application, such as an employee portal. The administrator then sets the interval at which he or she wants users to run CSA. Whenever a user tries to connect to the portal application, the filter intercepts the request and checks the CSA cookie. If the cookie is not present or if it is older than the execution interval specified by the administrator, the user is directed to the CSA page; if not, the user is allowed to proceed to the application.

Assume that Acme Corporation has a CSA instance deployed at *www.acme.com/csa/CSA.jsp*. Assume also that the company has a portal at *www.acme.com/portal* that can be used by employees to check e-mail, access their personal information, or display news about the company. Because the portal is accessed frequently by employees, the administrator at Acme decides that the portal can be used to keep CSA data up to date. The administrator would take the following steps:

1. Download the CSA servlet filter classes. These classes are contained in a JAR file, *CSA_filter.jar*, which can be downloaded from the *Deploy Client System Analyzer* page in the Enterprise Manager Cloud Control console.

2. Place the JAR file in the *WEB-INF/lib* directory of the application to which the filter will be applied.
3. Specify context parameters for the filter. In this case, the administrator wants users to run CSA every 30 days and return to the portal homepage after CSA has finished.

```
<context-param>
  <param-name>csa csaURL</param-name>
  <param-value>www.acme.com/csa/CSA.jsp</param-value>
</context-param>

<context-param>
  <param-name>csa execInterval</param-name>
  <param-value>2592000</param-value>
</context-param>
```

An alternative is to have CSA run in a separate browser window in the background. This can be set up by using the *csa_uiMode* parameter. If the parameter is set to 1, the filter will open a new browser window that is the same size as the original window and go to the CSA page. If the parameter is set to 2, CSA will run in *invisible* mode; in this case, the filter will open a new browser window and immediately minimize it, and it will close the window as soon as CSA has completed.

10.6.5.5 Sample Deployments

In the following sample deployment examples, there are three primary actors. The first is the CSA administrator, who is responsible for setting up CSA. The second is the Enterprise Manager user, who will be viewing the client data in Enterprise Manager. The third is the end user, whose data is being collected by CSA.

10.6.5.5.1 Example 1: Helpdesk

In this example, the CSA administrator is using CSA to support the operations of a helpdesk. End users who have problems running a particular application can call customer support, and the customer support technician can, if necessary, instruct the user to go to a particular URL and run CSA. The Enterprise Manager users are the support personnel who will use the data collected by CSA to assist the end user. To speed up the process of diagnosing the customer's problem, the CSA administrator creates some rules in a file called *rules.xml* so that the helpdesk personnel can quickly identify potential problems. In the simplest case, suppose that the helpdesk is being set up to provide support for a single application. The application is running on an application server on host *application.acme.com*, which has an Enterprise Manager Management Agent installed on it that sends data back to the Management Service at *oms.acme.com/em*. The helpdesk personnel who will be looking at client data can log into Enterprise Manager as the user *helpdesk*, which does not have super user privileges.

1. The CSA administrator adds *rules.xml* to the *CSA.war* file contained in *CSA.ear*.
2. Deploy the EAR file to the application server using the Application Services Control console.
3. Use the Application Services Control console to set the necessary context parameters, such as *ruleFile* and *outputDir*.
4. Optionally, the administrator can choose a collection tag for the CSA data by specifying a value for the *application* context parameter. If no tag is chosen, the tag *Default* will be used.

5. An Enterprise Manager user with super user privileges adds a CSA Collector Target to the Management Agent on *application.acme.com* and sets its receive file directory to the directory specified in the *outputDir* parameter of CSA.
6. An Enterprise Manager superuser creates the collection tag associations needed to allow the helpdesk users to look at the data. For example, the superuser could associate the tag *Default* with host *application.acme.com* and then give the *helpdesk* Enterprise Manager user view privileges on the host.

With the setup previously described, when a user calls the helpdesk to ask for support with the application, the helpdesk technician can instruct the user to run CSA from the appropriate URL on *application.acme.com*. The Management Agent collects the data after a certain interval and loads it into the Management Repository. The helpdesk technician can then log into Enterprise Manager as *helpdesk* and find the customer's information by searching for an identifying field such as the customer's operating system user name or host name. By default, the Management Agent will check the output directory for new data every two minutes, but this interval can be shortened by editing the file

\$ORACLE_HOME/sysman/admin/default_collection/oracle_csa_collector.xml.

10.6.5.5.2 Example 2: Inventory

In [Example 10–4](#), a system administrator is in charge of keeping track of the hardware and software used by employees in two different departments, Human Resources (HR) and Sales. This administrator serves as both the Enterprise Manager user and the CSA administrator. The setup for this case is similar to the one described in the example on using servlet filters, but in this case, each department has its own portal application, at *hr.acme.com/portal* and *sales.acme.com/portal*, respectively. The administrator sets up an application server on host *server1.acme.com* and deploys CSA with the URL *http://server1.acme.com/csa/CSA.jsp*. A Management Agent on *server1.acme.com* collects data and sends to an Oracle Management Service at *oms.acme.com/em*. The administrator would like to collect data once every 30 days and to have CSA run in invisible mode. The administrator would also like to distinguish data from the two different departments by using two separate collection tags, *hr* and *sales*. The administrator can log into Enterprise Manager as *sysman* and will thus be able to see clients with both tags.

The administrator arranges to have users directed to CSA by deploying the CSA servlet filter on both applications. Most of the filter context parameters for the two applications will be identical. However, because each application corresponds to a different tag, the values of the *csa csaURL* parameter will be slightly different. For the HR portal, the value would be *http://server1.acme.com/csa/CSA.jsp?application=hr*, and for the sales portal, the value would be *http://server1.acme.com/csa/CSA.jsp?application=sales*.

Example 10–4 Inventory Code

```
<context-param>
  <param-name>csa csaURL</param-name>
  <param-value>www.acme.com/csa/CSA.jsp?application=sales</param-value>
</context-param>

<context-param>
  <param-name>csa execInterval</param-name>
  <param-value>2592000</param-value>
</context-param>

<context-param>
  <param-name>csa uiMode</param-name>
```



```
<param-value>2</param-value>
</context-param>
```

Under this setup, users in the HR department who are directed to CSA from the HR portal will have the tag *hr*, and users from the sales department will have the tag *sales*. Thus, if the administrator wants to see information about only hardware on machines in the HR department, he or she can simply use the *Collection Tag* filter on the Client Configurations page in Enterprise Manager and set it to *hr*.

10.6.5.5.3 Example 3: Problem Detection

In this example, the goal is to use CSA to inform end users of potential problems they may experience while running an application. The setup is similar to the one used in Example 2. In this example, however, the CSA administrator creates rules for each application. In addition, the administrator wants CSA to run in the original browser window to ensure that end users are aware of any potential problems.

[Example 10-5](#) displays the context parameter values for the CSA servlet filter on the sales portal.

Example 10-5 Context Parameter Values for CSA Servlet Filter

```
<context-param>
  <param-name>csa csaURL</param-name>
  <param-value>www.acme.com/csa/CSA.jsp?application=sales</param-value>
</context-param>

<context-param>
  <param-name>csa execInterval</param-name>
  <param-value>2592000</param-value>
</context-param>

<context-param>
  <param-name>csa uiMode</param-name>
  <param-value>0</param-value>
</context-param>
```

[Example 10-6](#) represents the context parameter definitions to map rules to collection tags.

Example 10-6 Context Parameter Definitions Mapping Rules to Collection Tags

```
<context-param>
  <param-name>csa sales ruleFile</param-name>
  <param-value>sales_rules.xml</param-value>
</context-param>

<context-param>
  <param-name>csa distribution ruleFile</param-name>
  <param-value>hr_rules.xml</param-value>
</context-param>
```

10.7 Configuring Privilege Delegation Providers

A privilege delegation provider is defined as a program that allows a logged in user to perform an activity with the privileges of another user. Typically, the privileges that are granted to a specific user are administered centrally.

Enterprise Manager preferred credentials allow you to use two types of privilege delegation providers:

- **Sudo**

Sudo allows a permitted user to execute a command as the super user or another user, as specified in the sudo user administration file (*sudoers*). If the invoking user is root or if the target user is the same as the invoking user, no password is required. Otherwise, sudo requires that users authenticate themselves with a password by default.

Note: (In the default configuration, this is the user's password, not the root password).

Sudo determines who is an authorized user by consulting the file */etc/sudoers* file. Once a user has been authenticated, a timestamp is updated and the user may then use sudo without a password for a short period of time (5 minutes unless overridden in the *sudoers* file).

- **PowerBroker**

Symark PowerBroker enables UNIX system administrators to specify the circumstances under which other users may run certain programs such as root (or other important accounts). The result is that responsibility for such actions as adding user accounts, fixing line printer queues, and so on, can be safely assigned to the appropriate people, without disclosing the root password. The full power of root is thus protected from potential misuse or abuse. For example, modifying databases or file permissions, or erasing disks.

Symark PowerBroker can access existing programs as well as its own set of utilities that execute common system administration tasks. Utilities being developed to run on top of Symark PowerBroker can manage passwords, accounts, backups, line printers, file ownership or removal, rebooting, logging people out, killing their programs, deciding who can log in to where from where, and so on. They can also provide TCP/IP, Load Balancer, cron, NIS, NFS, FTP, rlogin, and accounting subsystem management. Users can work from within a restricted shell or editor to access certain programs or files as root.

For additional information about Sudo or PowerBroker, see their respective product documentation.

Using Enterprise Manager's command line interface (EM CLI), you can set/edit privilege delegation provider properties for a host. See the *Oracle Enterprise Manager Command Line Interface* guide for more information. See your privilege delegation provider documentation for detailed setup and configuration information.

10.7.1 Creating a Privilege Delegation Setting

A privilege delegation setting can be created using the Enterprise Manager CLI command line interface's *create_privilege_delegation_setting* verb.

You can also configure a host with a Privilege Delegation setting, apply a Privilege Delegation setting template or unconfigure the Privilege Delegation setting by choosing **Setup**, then **Security** on the Enterprise Manager home page, then selecting *Privilege Delegation* from the left menu panel.

10.7.1.1 Creating a Sudo Setting Using EM CLI

Use the *create_privilege_delegation_setting* EM CLI verb to create a sudo privilege delegation setting. For explicit syntax and examples, see EM CLI command line help or the *Oracle Enterprise Manager Command Line Interface* guide.

Variables

You can use the following variables when using EM CLI to set the privilege delegation settings. Variables are case-sensitive.

Variable	Definition
%RUNAS%	Run the command as this user.
%USERNAME%	Name of the user running the command.
%COMMAND%	Sudo Command

Syntax

```
emcli create_privilege_delegation_setting -setting_name=sudo_
setting_1 -setting_type=SUDO -settings="SETTINGS:<command to be
used with all the options>"
```

The following example illustrates using EM CLI to create a sudo setting. Here, sudo is installed in */opt/sudo/bin*.

Example 10-7 Using EM CLI to Create a Sudo Setting

```
>emcli create_privilege_delegation_setting -setting_name=sudo_setting_1 -setting_
type=SUDO -settings="SETTINGS:/opt/sudo/bin/sudo -S -u %RUNAS% %command%"
```

10.7.1.2 Creating a PowerBroker Setting Using EM CLI

Use the *create_privilege_delegation_setting* EM CLI verb to create a PowerBroker privilege delegation setting.

Variables

You can use the following variables when using EM CLI to set the privilege delegation settings. Variables are case-sensitive.

Variable	Definition
%RUNAS%	Run the command as this user.
%USERNAME%	Name of the user running the command.
%COMMAND%	Sudo Command
%PROFILE%	Use this profile to run the command

Syntax

```
>emcli create_privilege_delegation_setting -setting_
name=powerbroker_setting_1 -setting_type=POWERBROKER
-settings="SETTINGS:<command to be used with all the
```

```
options>;[PASSWORD_PROMPT_STRING,<password prompt for  
PowerBroker>] "
```

Example 10–8 Using EM CLI to Create a Sudo Setting

```
./emcli create_privilege_delegation_setting -setting_name=sudo_setting_1 -setting_  
type=SUDO -settings="SETTINGS: /opt/powerbroker/bin/pbrun -u %RUNAS% %command%"
```

Note: In this example, PowerBroker is installed in */opt/powerbroker* directory and its password prompt is "Password:".

10.7.2 Applying Privilege Delegation Settings

Once you have created a privilege delegation setting, you must apply this setting to selected targets. As with the setting creation process, you use EM CLI to apply the privilege delegation setting to specified targets. The setting can be applied to one or more hosts or to a composite (Group) target (the group must contain at least one host target).

You can also apply a Privilege Delegation setting using the Cloud Control console by selecting **Setup** on the Enterprise Manager Home page, then choosing *Manage Privilege Delegation Settings* from the left menu panel.

10.7.2.1 Applying Settings to Host Targets Using EM CLI

Use the *apply_privilege_delegation_setting* EM CLI verb to apply privilege delegation settings to a host target.

Syntax

```
emcli apply_privilege_delegation_setting -setting_name=<setting  
name> -target_type=host -target_names="host1;host2;..." -input_  
file="FILE:hosts.txt" -force="yes/no"
```

To apply privilege delegation properties to a large number of hosts, you can specify a file containing all hosts by using the *-input_file* option in place of the *-target_names* option, as shown in the following example.

Example 10–9 Using EM CLI to Apply Privilege Delegation Settings to a Host Target

```
./emcli apply_privilege_delegation_setting -setting_name=<setting name> -target_  
type=host -input_file="FILE: /mydirectory/file.txt" -force=yes
```

10.7.2.2 Applying Settings to a Composite Target

Use the *apply_privilege_delegation_setting* EM CLI verb to apply privilege delegation settings to a composite (group) target.

Syntax

```
emcli apply_privilege_delegation_setting -setting_name=<setting  
name> -target_type=composite -target_names="group"  
-force="yes/no"
```

Example 10–10 Using EM CLI to Apply Privilege Delegation Settings to a Composite Target

```
./emcli apply_privilege_delegation_setting -setting_name=<setting name> -target_  
type=composite -input_file="FILE: /mydirectory/file.txt" -force=yes
```

Once the setting has been applied successfully to host targets, you can set their preferred credentials using EM CLI or through the Cloud Control console.

10.7.3 Disabling Host Privilege Delegation Provider Settings Using EM CLI

To disable a privilege delegation setting, an administrator can create a new setting with disabled status and can apply it to the targets. This *disabled setting* can be applied to any privilege delegation provider (Sudo/PowerBroker). It will remove the setting from the host.

1. Create a new privilege delegation setting.

```
./emcli create_privilege_delegation_setting -setting_name= disabled_setting
-setting_type=SUDO -disabled=yes
```

2. Apply the new setting to one or more targets.

```
./emcli apply_privilege_delegation_setting -setting_name= disabled_setting
-target_type=host -target_names="host1;host2;..." -force=yes
```

10.7.4 Sudo Configuration: Sudoers File

Enterprise Manager uses a trust-based model that permits specification of responsibilities with a high degree of granularity. Administrators can set up **sudo** or **pbrun** configuration entries to assign specific Enterprise Manager functional privileges to their OS users. A new executable has been introduced in the Management Agent called **nmosudo**. Administrators will be able to configure **sudo**/**pbrun** such that a less privileged user can run **nmosudo** as a more privileged user.

In the following example, if an administrator wants user 'joe' to run any Enterprise Manager job as user 'oracle', the corresponding entry in the */etc/sudoers* file would be:

```
(JOB_USERS) ALL : (RUNAS_USERS) AGENT_HOME /bin/nmosudo *
```

Where 'joe' would be in the JOB_BACKUP_USERS list and 'oracle' would be in the RUNAS_USERS list.

Enterprise Manager will guarantee that the **nmosudo** executable will only honor requests to run remote operation requests from the OMS via the Management Agent. **nmosudo** will not run the remote operation if it cannot validate that the request came from the Management Agent. Thus, as shown in the example above, it will not be possible for user 'joe' to invoke **nmosudo** directly from the command line and run a Perl script as user 'oracle'.

Note: To ensure system security, the administrator must provide the full path to the **nmosudo** executable.

10.7.5 Configuring Privilege Delegation Providers Using Cloud Control Console

Enterprise Manager Cloud Control allows you to configure Privilege Delegation Providers through functionality provided through its user interface. Using Cloud Control, you can avoid the command line interface while performing essentially the same functions.

The following sections describe the functions you can perform using the Cloud Control interface.

10.7.5.1 Configuring Sudo Settings For a Host Using Enterprise Manager Cloud Control Console

You can use Enterprise Manager to create a Sudo setting by using the Cloud Control console. You can create privilege delegation settings either by creating the setting directly on a host target, or by creating a PDP setting template that you can apply to multiple hosts.

To create a privilege delegation Sudo setting directly on a host, follow these steps:

1. Navigate to the *Manage Privilege Delegation Settings* page. From the Setup menu, select *Manage*, then select *Privilege Delegation Settings*.
2. For any host target appearing in the table, click **Edit**. Enterprise Manager takes you to the *Host Privilege Delegation Setting* page.
3. Select the **Sudo** privilege delegation type.
4. Enter the privilege delegation command to be used.
5. Click **Update** to apply the settings to the host.

Note: If the host has been configured with either the Sudo or Powerbroker setting, choosing *None* on this page will remove (or disable) the setting.

10.7.5.2 Configuring PowerBroker Settings For a Host Using the Cloud Control Console

You can create privilege delegation settings either by creating the setting directly on a host target, or by creating a PDP setting template that you can apply to multiple hosts.

To create a privilege delegation PowerBroker setting directly on a host, follow these steps:

1. Navigate to the *Manage Privilege Delegation Settings* page. From the Setup menu, select *Manage*, then choose *Manage Privilege Delegation Settings*.
2. For any host target appearing in the table, click **Edit**. Enterprise Manager takes you to the *Host Privilege Delegation Setting* page.
3. Select the **PowerBroker** privilege delegation type.
4. Enter the privilege delegation command to be used and the optional Password Prompt.
5. Click **Update** to apply the settings to the host.

Note: If the host has been configured with either the Sudo or Powerbroker setting, choosing *None* on this page will remove (or disable) the setting.

10.7.5.3 Applying Settings to Multiple Host Targets Using the Cloud Control Console

You apply Privilege Delegation settings to a target using Privilege Delegation setting templates. If no template with the desired Privilege Delegation settings exists, you must first create the template on the *Manage Privilege Delegation Settings Template* page.

To create a template, follow these steps:

1. Navigate to the *Manage Privilege Delegation Settings* page. From the Setup menu, select Manage, then choose Manage Privilege Delegation Settings.
2. From the Related Links section, click **Manage Privilege Delegation Setting Templates**.
3. Select a privilege delegation type (Sudo or PowerBroker), then click **Go**.
4. Fill in the requisite privilege delegation setting information.
5. Click **Save**.

If the desired privilege delegation settings template already exists, you need only apply the template to the desired host(s). To apply the template to the hosts, follow these steps:

1. Navigate to the *Manage Privilege Delegation Settings* page. From the Setup menu, select Manage, then choose Manage Privilege Delegation Settings.
2. Select the desired privilege delegation settings template from the Apply drop-down menu.
3. Click **Go** to access the *Apply Settings* page.
4. Add the targets (hosts) to which you want to apply the privilege delegation settings template.
5. Click **Apply**. Enterprise Manager displays the *Past Apply Operations* page where you can view the queue of scheduled apply operations along with those that are scheduled/pending. From this page, you can **Stop** or **Delete** apply operations.

You can also apply privilege delegation settings from the *Manage Privilege Delegation Setting Templates* page.

10.7.5.4 Disabling Host Privilege Delegation Provider Settings For One or More Hosts Using Cloud Control Console

You can disable a Privilege Delegation setting using the Cloud Control console. To disable a privilege delegation setting using this method, follow these steps:

1. Click **Setup** to access the *Enterprise Manager Configuration* page.
2. From the left menu, click **Manage Privilege Delegation Settings**.
Cloud Control displays the *Manage Privilege Delegation Settings Page*.
3. Select the host(s) from which to clear the privilege delegation settings.
4. Click **Clear**. Enterprise Manager asks you whether to proceed with the privilege setting disable operation.
5. Click **Yes**.

Configuring Enterprise Manager for Firewalls

Firewalls protect a company's Information Technology (IT) infrastructure by providing the ability to restrict network traffic by examining each network packet and determining the appropriate course of action.

Firewall configuration typically involves restricting the ports that are available to one side of the firewall, for example the Internet. It can also be set up to restrict the type of traffic that can pass through a particular port such as HTTP. If a client attempts to connect to a restricted port (a port not covered by a security "rule") or uses a protocol that is incorrect, then the client will be disconnected immediately by the firewall. Firewalls can also be used within a company Intranet to restrict user access to specific servers.

You can deploy the components of Oracle Enterprise Manager on different hosts throughout your enterprise. These hosts can be separated by firewalls. This chapter describes how firewalls can be configured to allow communication between the Enterprise Manager components.

This chapter contains the following sections:

- [Firewall Configuration Considerations](#)
- [Overview of Enterprise Manager Components and Ports](#)
- [Firewall Configurations for Enterprise Management Components](#)

11.1 Firewall Configuration Considerations

Firewall configuration should be the last phase of Enterprise Manager deployment. Before you configure your firewalls, make sure you are able to log in to the Enterprise Manager console and that your Oracle Management Agents (Management Agent) are up and monitoring targets.

If you are deploying Enterprise Manager in an environment where firewalls are already installed, open the default Enterprise Manager communication ports for all traffic until you have completed the installation and configuration processes and are certain that you are able to log in to Enterprise Manager and that your Management Agents are up and monitoring targets.

The default communication ports for Enterprise Manager are assigned during the installation. If you modify the default ports, be sure to use the new port assignments when you configure the firewalls.

If you are enabling Enterprise Manager Framework Security for the Oracle Management Service (OMS), the final step in that configuration process is to restrict

uploads from the Management Agents to secure channels only. Before completing that step, configure your firewalls to allow both HTTP and HTTPS traffic between the Management Agent and Management Repository and test to be sure that you can log in to Enterprise Manager and that data is being uploaded to the Management Repository.

After you have confirmed that the OMS and Management Agents can communicate with both protocols enabled, complete the transition to secure mode and change your firewall configuration as necessary. If you incrementally configure your firewalls, it will be easier to troubleshoot any configuration problems.

11.1.1 Enabling ICMP Echo Requests on Firewalls

OMS uses the Internet Control Message Protocol (ICMP) Echo Request to check the status target host machines. If the ICMP Echo Request is blocked by the firewall, a host machine will appear to be down.

To determine the status of any machine in the environment, ICMP Echo Requests must be enabled on the firewall. If the ICMP Echo Request is enabled, the ping command can be issued by the OMS to check the status of the machine.

By default, port 7 will be used for the ICMP Echo Request.

11.2 Overview of Enterprise Manager Components and Ports

As described in the previous sections of this chapter, it is important to understand and identify the ports used by each of the Enterprise Manager components before you configure your firewalls.

11.2.1 Viewing a Summary of the Ports Assigned During Installation

The last panel in the Enterprise Manager installer, which is displayed just before the actual installation is started, list all of the ports assigned during the installation.

Post-installation, you can view these values in the `staticports.ini` file at the following location on the OMS host:

`MIDDLEWARE_HOME/.gcinstall_temp/staticports.ini`

You can get the Middleware home value by viewing the Oracle Home target for the OMS in Enterprise Manager.

11.2.2 Default Port Assignments for Enterprise Manager Components

Table 11–1 notes the default ports and/or port ranges assigned to various Enterprise Manager components that should be accessible through a firewall. These components include WebLogic Server components created as part of the WebLogic domain the Enterprise Manager installation belongs to, as well as optional components such as JVM Diagnostics and Application Dependency and Performance.

Table 11–1 Default Ports and Port Ranges for Enterprise Manager Components

Port	Default Values
Enterprise Manager Upload HTTP Port	4889 - 4898
Enterprise Manager Upload HTTPS (SSL) Port	1159, 4899 - 4908

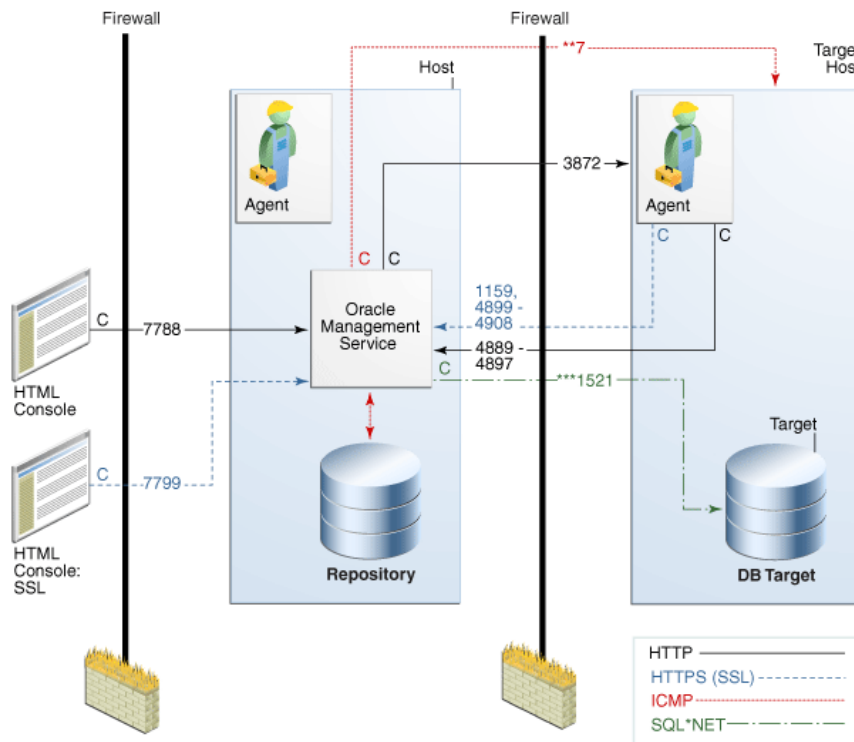
Table 11–1 (Cont.) Default Ports and Port Ranges for Enterprise Manager Components

Port	Default Values
Management Agent Port	3872, 1830 - 1849
Management Repository Database Port	1521
Cloud Control Console HTTP Port	7788 - 7798
Cloud Control Console HTTPS (SSL) Port	7799 - 7809
EM Domain WebLogic Admin Server HTTP Port	7001
EM Domain WebLogic Admin Server HTTPS (SSL) Port	7101 - 7200
Cloud Control Managed Server HTTP Port	7201 - 7300
Cloud Control Managed Server HTTPS (SSL) Port	7301 - 7400
WebLogic Node Manager HTTPS (SSL) Port	7401 - 7500
JVM Diagnostics Managed Server	3800
JVM Diagnostics Managed Server (SSL)	3801
Application Dependency and Performance RMI Registry Port	51099
Application Dependency and Performance Java Provider Port	5503
Application Dependency and Performance Remote Service Controller Port	55000
Real User Experience Insight HTTPS (SSL)	443

11.3 Firewall Configurations for Enterprise Management Components

Your main task in enabling Enterprise Manager to work in a firewall-protected environment is to take advantage of proxy servers whenever possible, to make sure only the necessary ports are open for secure communications, and to make sure that only data necessary for running your business is allowed to pass through the firewall.

[Figure 11–1](#) provides a topology of an Enterprise Manager environment that is using a firewall, and also illustrates the default ports that can be used.

Figure 11–1 Firewall Port Requirements (Default)

The conventions used in the preceding illustration are as follows:

Table 11–2 Conventions Used In Illustration

Convention	Description
C	Is the entity that is making the call.
*	Enterprise Manager will default to the first available port within an Enterprise Manager set range.
**	Enterprise Manager will default to the first available port.
***	Database listener ports.

Notes:

- The direction of the arrows specify the direction of ports.
- Port 1159, 4898-4989 indicates that 1159 is the default. If this port is not available, the Oracle Management Service will search in the specified range (4889 - 4897).
- To clone between two target hosts separated by a firewall, the agents will need to communicate to each other on the agent ports. The initiating Management Agent will make the call.

The following sections describe the ports and types of data required by Enterprise Manager in a secure, firewall-protected environment:

- [Firewalls Between Your Browser and the Enterprise Manager Console](#)

- [Configuring the Management Agent on a Host Protected by a Firewall](#)
- [Configuring the OMS on a Host Protected by a Firewall](#)
- [Firewalls Between the OMS and the Management Repository](#)
- [Firewalls Between Enterprise Manager and a Managed Database Target](#)
- [Firewalls Used with Multiple OMS Instances](#)
- [Configuring Firewalls to Allow ICMP and UDP Traffic for Beacons](#)

11.3.1 Firewalls Between Your Browser and the Enterprise Manager Console

Connections from your browser to the Enterprise Manager console are performed over the default port used for your Oracle HTTP Server.

For example, the default, non-secure port for the Oracle HTTP Server is usually port 7788. If you are accessing the Enterprise Manager console using the following URL and port, then you must configure the firewall to allow the Enterprise Manager console to receive HTTP traffic over port 7788:

```
http://omshost.example.com:7788/em
```

On the other hand, if you have enabled security for your Oracle HTTP Server, you are likely using the default secure port for the server, which is usually port 7799. If you are accessing the Enterprise Manager console using the following URL and port, then you must configure the firewall to allow the Enterprise Manager console to receive HTTPS traffic over port 7799:

```
https://omshost.example.com:7799/em
```

11.3.2 Configuring the Management Agent on a Host Protected by a Firewall

If your Management Agent is installed on a host that is protected by a firewall and the OMS is on the other side of the firewall, you must perform the following tasks:

- Configure the Management Agent to use a proxy server for its uploads to the OMS.
- Configure the firewall to allow incoming HTTP traffic from the OMS on the Management Agent port. Regardless of whether or not Enterprise Manager Framework Security has been enabled, the default port is 3872. Incoming traffic can be received only if the port corresponding to the Management Agent is open in the firewall.

[Figure 11–2](#) illustrates the connections the Management Agent must make when it is protected by a firewall.

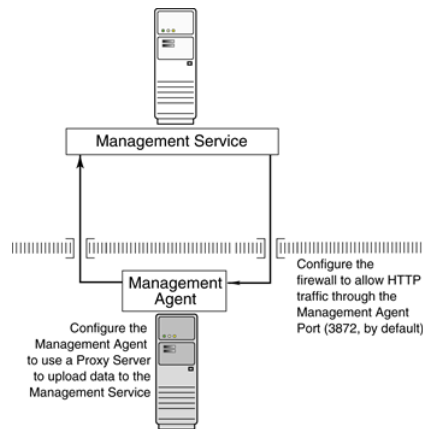
Figure 11–2 Configuration Tasks When the Management Agent Is Behind a Firewall

Illustration `firewall_agent.gif` shows a diagram of the Management Agent and the Management Service. A line representing the firewall appears between the Management Agent and the Management Service.

Two additional lines represent data being uploaded to the Management Service and the Management Service contacting the Management Agent, respectively. Text in the diagram explains how you need to:

- Configure the Management Agent to use a proxy server for uploads to the Management Service
- Open the Management Agent port (usually 1830) in the firewall so the Management Service can communicate with the Management Agent.

11.3.2.1 Configuring the Management Agent to Use a Proxy Server

You can configure the Management Agent to use a proxy server for its communications with an OMS outside the firewall, or to manage a target outside the firewall.

1. From the **Setup** menu, select **Agents**.
2. Click the Agent you want to configure in the Name column in the Management Agents table. The target home page for the Management Agent opens.
3. Select **Properties** from the **Agent** menu.
4. Select **Advanced Properties** from the pull down menu.
5. Supply the correct values for the `REPOSITORY_PROXYHOST` and `REPOSITORY_PROXYPORT` properties.
6. Click **Apply** to save your changes, which will be saved to the `AGENT_HOME/sysman/config/emd.properties` file.

Note: The proxy password will be obfuscated when you restart the Management Agent.

11.3.2.2 Configuring the Firewall to Allow Incoming Communication From the Management Service

While the Management Agents in your environment must upload data from your managed hosts to the OMS, the OMS must also communicate with the Management Agents. As a result, if the Management Agent is protected by a firewall, the OMS must be able to contact the Management Agent through the firewall on the Management Agent port.

By default, the Enterprise Manager installation procedure assigns port 3872 to the Management Agent. However, if that port is occupied, the installation may assign an alternate port number.

After you determine the port number assigned to the Management Agent, you must then configure the firewall to allow incoming HTTP or HTTPS traffic (depending upon whether or not you have enabled Enterprise Manager Framework Security) on that port.

11.3.3 Configuring the OMS on a Host Protected by a Firewall

If your OMS is installed on a host that is protected by a firewall and the Management Agents that provide management data are on the other side of the firewall, you must perform the following tasks:

- Configure the OMS to use a proxy server for its communications to the Management Agents.
- Configure the firewall to allow incoming HTTP traffic from the Management Agents on the Management Repository upload port.

If you have enabled Enterprise Manager Framework Security, the upload URL uses port 1159 by default. If this port is not available, Enterprise Manager will default to first available port in the range 4899-4908. If you have *not* enabled Enterprise Manager Framework Security, the upload port is the first available port in the range 4889 - 4897.

[Figure 11-3](#) illustrates the connections the Management Agent must make when it is protected by a firewall.

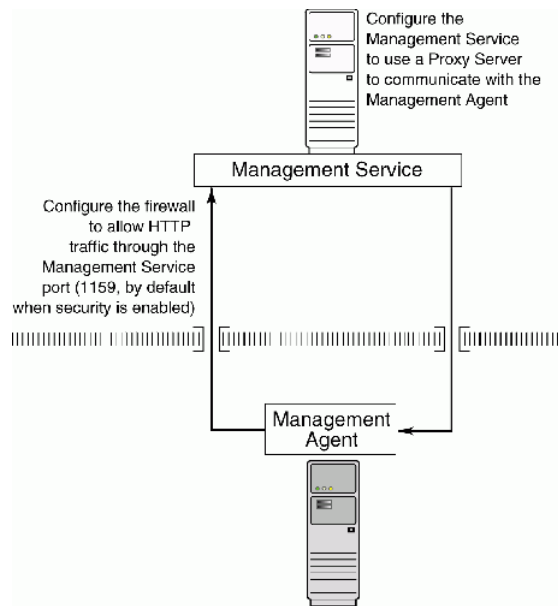
Figure 11–3 Configuration Tasks When the Management Service Is Behind a Firewall

Illustration firewall_oms.gif shows a diagram of the Management Agent and the Oracle Management Service. A line representing the firewall appears between them. The diagram includes text that explains how you must:

- Configure the Management Service to use a proxy server for connections to the Management Agent
- Open the upload URL port in the firewall so that data can be uploaded from the Management Agent to the Management Service.

11.3.3.1 Configuring the OMS to Use a Proxy Server to Communicate with Management Agents

This section describes how to configure the OMS to use a proxy server for its communications with Management Agents outside the firewall.

To configure the OMS to use a proxy server, do the following:

1. From the **Setup** menu, select **Proxy Settings**, then select **Agents**.

Note: The Proxy Settings for Agents page enables you to configure a proxy server that can be used for communication only from the OMS to the Management Agent, and not from the Management Agent to the OMS. Any proxy server you configure will be used for the communication between the OMS and all the Management Agents.

2. Select **Manual proxy configuration**.

3. Specify values for **Protocol**, **Proxy Server Host**, **Port**, and **No Proxy for**. If the specified proxy server has been configured using a security realm, login credentials, or both, then specify values for **Realm**, **User Name**, and **Password**.
4. Under the Test URL section, specify a Management Agent URL for **URL**, then click **Test** to test if the OMS can communicate with the specified Management Agent using the specified proxy server.
5. If the connection is successful, click **Apply** to save the proxy settings to the repository.
6. Restart the OMS. If you are using a multi-OMS setup, restart all the OMSes.
To restart an OMS that runs on a Unix based platform, run the following commands:

```
<OMS_HOME>/bin/emctl stop oms
<OMS_HOME>/bin/emctl start oms
```

To restart an OMS that runs on a Microsoft Windows platform, follow these steps:

1. Right-click **My Computer**, then select **Manage**.
2. In the Computer Management window, in the left pane, expand **Services and Applications**, then select **Services**.
3. Select the OracleManagementServer_EMGC_OMS* service, then click the restart button.

11.3.3.2 Configuring the Firewall to Allow Incoming Management Data From the Management Agents

While the Management Agents in your environment must contact the Management Agents on your managed hosts, the OMS must also be able to receive upload data from the Management Agents. If the OMS is behind a firewall, you must configure the firewall to allow the Management Agents to upload data on the upload port.

By default, the Enterprise Manager installation procedure assigns port 4889 as the Repository upload port. However, if that port is occupied, the installation will assign an alternate port number.

In addition, when you enable Enterprise Manager Framework Security, the upload port is automatically changed to the secure 1159 HTTPS port.

Administrators can also change the upload port after the installation.

After you determine the port number assigned to the OMS upload port, you must then configure the firewall to allow incoming HTTP or HTTPS traffic (depending upon whether or not you have enabled Enterprise Manager Framework Security) on that port.

11.3.3.3 Enabling OMS to Access My Oracle Support

Unless online access to the Internet is strictly forbidden in your environment, OMS should be enabled to access My Oracle Support. This access is necessary to enable updates and patches to be downloaded, for example.

At minimum, the following URLs should be made available through the firewall:

- aru-akam.oracle.com
- ccr.oracle.com
- login.oracle.com

- `support.oracle.com`
- `updates.oracle.com`

11.3.3.4 About the `dontProxyFor` Property

When you configure the OMS or a Management Agent to use a proxy server, it is important to understand the purpose of the `dontProxyFor` property, which identifies specific URL domains for which the proxy will not be used.

For example, suppose the following were true:

- You have installed the OMS and several Management Agents on hosts that are inside the company firewall. These hosts are in the internal `.example.com` and `.example.us.com` domains.
- You have installed several additional Management Agents on hosts that are outside the firewall. These hosts are installed in the `.example.uk` domain.
- You have configured Enterprise Manager to automatically check for critical software patches on My Oracle Support.

In this scenario, you want the OMS to connect directly to the Management Agents inside the firewall without using the proxy server. On the other hand, you want the OMS to use the proxy server to contact the Management Agents outside the firewall, as well as the My Oracle Support site, which resides at the following URL:

`http://support.oracle.com`

The following properties will prevent the OMS from using the proxy server for connections to the Management Agents inside the firewall. Connections to My Oracle Support and to Management Agents outside the firewall will be routed through the proxy server:

```
proxyHost=proxy42.example.com
proxyHost=80
dontProxyFor=.example.com, .example.us.com
```

11.3.4 Firewalls Between the OMS and the Management Repository

Secure connections between the OMS and the Management Repository are performed using features of Oracle Advanced Security. As a result, if the OMS and the Management Repository are separated by a firewall, you must configure the Oracle Net firewall proxy to allow the OMS to access the repository.

11.3.5 Firewalls Between Enterprise Manager and a Managed Database Target

When you are using the Enterprise Manager console to manage a database, you must log in to the database from the Enterprise Manager console in order to perform certain monitoring and administration tasks. If you are logging in to a database on the other side of a firewall, you will need to configure the firewall to allow Oracle Net firewall proxy access.

Specifically, to perform any administrative activities on the managed database, you must be sure that the firewall is configured to allow the OMS to communicate with the database through the Oracle Listener port.

You can obtain the Listener port by reviewing the Listener home page in the Enterprise Manager console.

11.3.6 Firewalls Used with Multiple OMS Instances

Enterprise Manager supports the use of multiple OMS instances that communicate with a common Management Repository. For example, using more than one OMS can be helpful for load balancing as you expand your central management capabilities across a growing e-business enterprise.

When you deploy multiple OMS instances in an environment protected by firewalls, be sure to consider the following:

- Each Management Agent is configured to upload data to one OMS. As a result, if there is a firewall between the Management Agent and its OMS, you must configure the firewall to allow the Management Agent to upload data to the OMS using the upload URL.

See Also: [Section 11.3.2, "Configuring the Management Agent on a Host Protected by a Firewall"](#)

[Section 11.3.3, "Configuring the OMS on a Host Protected by a Firewall"](#)

- In addition, each OMS must be able to contact any Management Agent in your enterprise so it can check for the availability of the Management Agent. As a result, you must be sure that your firewall is configured so that each OMS you deploy can communicate over HTTP or HTTPS with any Management Agent in your enterprise.

Otherwise, an OMS without access to a particular Management Agent may report incorrect information about whether or not the Management Agent is up and running.

See Also: "About Availability" in the Enterprise Manager online help for information about how Enterprise Manager determines host and Management Agent availability.

11.3.7 Configuring Firewalls to Allow ICMP and UDP Traffic for Beacons

Oracle Beacons provide application performance availability and performance monitoring. They are part of the Application Service Level Management features of Enterprise Manager.

See Also: "About Application Service Level Management" in the Enterprise Manager Online Help

Enterprise Manager uses the industry-standard Internet Control Message Protocol (ICMP) and User Datagram Protocol (UDP) to transfer data between Beacon and the network components you are monitoring. There may be situations where your Web application components and the Beacons you use to monitor those components are separated by a firewall. In those cases, you must configure your firewall to allow ICMP, UDP and HTTP traffic.

Sizing Your Enterprise Manager Deployment

Oracle Enterprise Manager Cloud Control 12c Release 12.1.0.3 has the ability to scale for hundreds of users and thousands of systems and services on a single Enterprise Manager implementation.

This chapter describes techniques for achieving optimal performance using the Oracle Enterprise Manager application. It can also help you with capacity planning, sizing and maximizing Enterprise Manager performance in a large scale environment. By maintaining routine housekeeping and monitoring performance regularly, you insure that you will have the required data to make accurate forecasts of future sizing requirements. Receiving good baseline values for the Enterprise Manager Cloud Control vital signs and setting reasonable warning and critical thresholds on baselines allows Enterprise Manager to monitor itself for you.

This chapter contains the following sections:

- [Overview of Oracle Enterprise Manager Cloud Control Architecture](#)
- [Enterprise Manager Cloud Control Sizing](#)
- [Enterprise Manager Cloud Control Performance Methodology](#)
- [Overview of Repository and Sizing Requirements for Fusion Middleware Monitoring](#)

12.1 Overview of Oracle Enterprise Manager Cloud Control Architecture

The architecture for Oracle Enterprise Manager Cloud Control exemplifies two key concepts in application performance tuning: distribution and parallelization of processing. Each component of Cloud Control can be configured to apply both these concepts.

The components of Enterprise Manager Cloud Control include:

- The Management Agent - A process that is deployed on each monitored host and that is responsible for monitoring all services and components on the host. The Management Agent is also responsible for communicating that information to the middle-tier Management Service and for managing and maintaining the system and its services.
- The Management Service - A J2EE Web application that renders the user interface for the Cloud Control console, works with all Management Agents to process monitoring and jobs information, and uses the Management Repository as its data store.

- The Management Repository - The schema is an Oracle Database that contains all available information about administrators, services, and applications managed within Enterprise Manager.

For more information about the Cloud Control architecture, see the Oracle Enterprise Manager Cloud Control 12c Release 12.1.0.3 documentation:

- *Oracle Enterprise Manager Grid Control Installation and Basic Configuration*
- *Oracle Enterprise Manager Concepts*

The Oracle Enterprise Manager 12c documentation is available at the following location on the Oracle Technology Network (OTN):

<http://www.oracle.com/technetwork/indexes/documentation/index.html>

12.2 Enterprise Manager Cloud Control Sizing

Oracle Enterprise Manager provides a highly available and scalable deployment topology. This chapter lays out the basic minimum sizing and tuning recommendations for initial capacity planning for your Oracle Enterprise Manager deployment. This chapter assumes a basic understanding of Oracle Enterprise Manager components and systems. A complete description of Oracle Enterprise Manager can be obtained from http://docs.oracle.com/cd/E24628_01/doc.121/e25353/overview.htm. This information is a starting point for site sizing. Every site has its own characteristics and should be monitored and tuned as needed.

Sizing is a critical factor for Enterprise Manager performance. Inadequately sized Enterprise Manager deployments will result in frustrated users and the overall benefits of Enterprise Manager may be compromised. The resources required for Enterprise Manager OMS and Repository tiers will vary significantly based on the number of monitored targets. While there are many additional aspects to be considered when sizing Enterprise Manager infrastructure, the following guidelines provide a simple methodology that can be followed to determine the minimum required hardware resources and initial configuration settings for the OMS and Repository tiers.

12.2.1 Overview of Sizing Guidelines

The following sections provide an overview of the sizing guidelines.

12.2.1.1 Hardware Information

The sizing guidelines outlined in this chapter were obtained by running a virtual environment on the following hardware and operating system combination.

- Hardware -- Oracle's Sun Fire X4170 M2
- Hypervisor -- 64 bit Linux Oracle Virtual Server
- Operating System of Virtual Machines -- 64 bit Oracle Enterprise Linux

The virtual environment setup had a one to one mapping of CPUs between the Oracle Virtual Server (OVS) host and the virtual machines running on it. The OVS servers had enough RAM to support all virtual machines without memory swapping.

This information is based on a 64 bit Oracle Enterprise Linux environment. If you are running on other platforms, you will need to convert the sizing information based on similar hardware performance. This conversion should be based on single-thread performance. Running on a machine with 24 slow cores is not equivalent to running

on a machine with 12 fast cores even though the total machine performance might be the same on a throughput benchmark. Single thread performance is critical for good Enterprises Manager user interface response times.

12.2.1.2 Sizing Specifications

The sizing guidelines for Oracle Enterprise Manager are divided into three sizes: Small, Medium and Large. The definitions of each size are shown in [Table 12-1](#).

Table 12-1 Oracle Enterprise Manager Site Sizes

Size	Agent Count	Target Count	Concurrent User Sessions
Small	< 100	< 1000	<10
Medium	>= 100, < 1000	>= 1000, < 10,000	>= 10, < 25
Large	>= 1000	>= 10,000	>= 25, <= 50*

For larger user loads see [Section 12.2.3.1, "Large Concurrent UI Load"](#).

12.2.1.3 Sizing for Upgraded Installs

For upgraded installs the following queries can be run as the sysman user to obtain the Management Agent and target counts for use in Table 1.

- Agent count - select count(*) from mgmt_targets where target_type = 'oracle_emd'
- Target count – select count(*) from mgmt_targets where target_type != 'oracle_emd'

12.2.1.4 Minimum Hardware Requirements

[Table 12-2](#) lists the minimum hardware requirements for the three configurations.

Table 12-2 Oracle Enterprise Manager Minimum Hardware Requirements

Size	OMS Machine Count*	Cores per OMS	Memory per OMS (GB)	Database Machine Count*	Cores per Database Machine	Memory per Database Machine (GB)
Small	1	2	6	1	2	6
Medium	2	4	8	2 (Oracle RAC)	4	8
Large	2	8	16	2 (Oracle RAC)	8	16
	4	4	8	2 (Oracle RAC)	8	16

*The OMS and database instances are not co-located

12.2.1.5 Network Topology Considerations

A critical consideration when deploying Enterprise Manager Cloud Control is network performance between tiers. Enterprise Manager Cloud Control ensures tolerance of network glitches, failures, and outages between application tiers through error tolerance and recovery. The Management Agent in particular is able to handle a less performant or reliable network link to the Management Service without severe impact to the performance of Enterprise Manager as a whole. The scope of the impact, as far as a single Management Agent's data being delayed due to network issues, is not likely to be noticed at the Enterprise Manager Cloud Control system wide level.

The impact of slightly higher network latencies between the Management Service and Management Repository will be substantial, however. Implementations of Enterprise Manager Cloud Control have experienced significant performance issues when the network link between the Management Service and Management Repository is not of sufficient quality.

The Management Service host and Repository host should be located in close proximity to each other. Ideally, the round trip network latency between the two should be less than 1 millisecond.

12.2.2 Software Configurations

The following sections provide information about small, medium and large configurations.

12.2.2.1 Small Configuration

The Small configuration is based on the minimum requirements that are required by the Oracle Enterprise Manager installer.

Minimum OMS Settings

No additional settings are required.

Minimum Database Settings

[Table 12–3](#) lists the minimum recommended database settings.

Table 12–3 Small Site Minimum Database Settings

Parameter	Minimum Value
processes	300
memory_target*	3GB
redo log file size	300M
shared_pool_size	600M
*pga_aggregate_target of 1024M and sga_target of 2G can be used in place of memory_target	

12.2.2.2 Medium Configuration

The Medium configuration modifies several out-of-box Oracle Enterprise Manager settings.

Minimum OMS Settings

The Oracle Management Service (OMS) heap size should be set to 4096m.

Minimum Repository Database Settings

[Table 12–4](#) lists the minimum repository database settings that are recommended for a Medium configuration.

Table 12–4 Medium Site Minimum Database Settings

Parameter	Minimum Value
processes	600
memory_target*	5.25GB
*pga_aggregate_target of 1280M and sga_target of 4G can be used in place of memory_target	

Table 12–4 (Cont.) Medium Site Minimum Database Settings

Parameter	Minimum Value
redo log file size	600M
shared_pool_size	600M
*pga_aggregate_target of 1280M and sga_target of 4G can be used in place of memory_target	

12.2.2.3 Large Configuration

The Large configuration modifies several out-of-box Oracle Enterprise Manager settings.

Minimum OMS Settings

Table 12–5 lists the minimum OMS settings that are recommended for Large configurations.

Table 12–5 Large Site Minimum OMS Settings

OMS Count	Heap Size Minimum Value
2	8192M
4	4096M

Minimum Repository Database Settings

Table 12–6 lists the minimum repository database settings that are recommended for a Large configuration.

Table 12–6 Large Site Minimum Database Settings

Parameter	Minimum Value
processes	1000
memory_target*	7.5GB
redo log file size	1000M
shared_pool_size	600M
*pga_aggregate_target of 1536M and sga_target of 6G can be used in place of memory_target	

12.2.2.4 Repository Tablespace Sizing

Table 12–7 lists the required minimum storage requirements for the Management Repository.

Table 12–7 Total Management Repository Storage

Deployment Size	Minimum Tablespace Sizes*				
	SYSTEM**	MGMT_TABLESPACE	MGMT_ECM_DEPOT_TS	MGMT_AD4J_TS	TEMP
Small	600 MB	50 GB	1 GB	100 MB	10 GB
Medium	600 MB	200 GB	4 GB	200 MB	20 GB
Large	600 MB	300 GB	Greater than 4 GB	400 MB	40 GB

*These are strictly minimum values and are intended as rough guidelines only. The actual size of the MGMT_TABLESPACE could vary widely from deployment to deployment due to variations in target type distribution, user customization, and several other factors. These tablespaces are defined with AUTOEXTEND set to ON by default to help mitigate space constraint issues. On raw file systems Oracle recommends using more than the minimum size to help prevent space constraint issues.

**The SYSTEM and TEMP tablespace sizes are minimums for Enterprise Manager only repositories. If Enterprise Manager is sharing the repository database with other application(s), these minimums may be too low.

Note: You can either set up TABLESPACE FULL alerts if you want to have greater control over the management of your tablespaces, or you can allow Oracle to grow your database and not alert you through the AUTOEXTEND feature. Therefore to exercise greater control of the TABLESPACE FULL alerts, you can turn off autoextend.

12.2.3 Additional Configurations

Some Enterprise Manager installations may need additional tuning settings based on larger individual system loads. Additional settings are listed below.

12.2.3.1 Large Concurrent UI Load

If more than 50 concurrent users are expected per OMS, the following settings should be altered as seen in [Table 12–8](#).

Table 12–8 Large Concurrent UI Load Additional Settings

Process	Parameter	Value	Where To Set
OMS	-Djbo.recyclethreshold	Number of concurrent users / number of OMS	Per OMS
OMS	-Djbo.ampool.maxavailab lesize	Number of concurrent users / number of OMS	Per OMS
OMS	Heap Size	Additional 4GB for every increment of 50 users	Per OMS
Database	sga_target	Additional 1GB for every increment of 50 users	Per Instance

Higher user loads will require more hardware capacity. An additional 2 cores for both the database and OMS hosts for every 50 concurrent users.

Example: A site with 1500 agents and 15,000 targets with 150 concurrent users would require at a minimum the setting modifications listed in [Table 12–9](#) (based on a LARGE 2 OMS configuration).

Table 12–9 Large Concurrent UI Load Additional Settings Example for 2 OMS Configurations

Process	Parameter	Value	Calculation
OMS	-Djbo.recyclethreshold	75 (set on each OMS)	150 users / 2 OMS

Table 12–9 (Cont.) Large Concurrent UI Load Additional Settings Example for 2 OMS Configurations

Process	Parameter	Value	Calculation
OMS	-Djbo.ampool.maxavailablesize	75 (set on each OMS)	150 users / 2 OMS
OMS	Heap Size	12GB (set on each OMS)	8GB (standard large setting) + ((150 users – 50 default large user load) / 2 OMS)* (4GB / 50 users)
Database	sga_target	8GB	6GB (standard large setting) + (150 users - 50 default large user load) * (1GB / 50 users)

Minimum Additional Hardware required is listed in [Table 12–10](#).

Table 12–10 Large Concurrent UI Load Minimum Additional Hardware Example For 2 OMS Configuration

Tier	Parameter	Value	Calculation
OMS	CPU cores	24 (total between all OMS hosts)	8 cores * 2 OMS (default large core count) + (150 users - 50 default large user load) *(2 cores * 2 OMS) / 50 users)
Database	CPU cores	24 (total between all Database hosts)	8 cores * 2 OMS (default large core count) + (150 users - 50 default large user load) *(2 cores * 2 OMS / 50 users)

The physical memory of each machine would have to be increased to support running this configuration as well.

You can alter the value of the following parameters: *-Djbo.recyclethreshold*, *-Djbo.ampool.maxavailablesize*, and *Heap Size*. By default these values are set as follows:

- *Djbo.recyclethreshold* is set to 50
- *Djbo.ampool.maxavailablesize* is set to 1
- *Heap Size* is set to *-Xms1024m -Xmx1740m*

You can set the values for these parameters in the *startEMServer.sh* file, which can be found in the following location:

gc_inst/user_projects/domains/GCDomain/bin

For the *-Djbo.recyclethreshold* and *-Djbo.ampool.maxavailablesize* parameters, you can add the first section below to the second section.

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Djava.security.egd=file:///dev/./urandom
-Dweblogic.debug.DebugSecurityAtn=true -Dweblogic.debug.DebugWebAppSecurity=true
-Dweblogic.SSL.LoginTimeoutMillis=300000 -Dj
ps.auth.debug=true -Xbootclasspath/p:/u01/EM12/oms/sysman/jlib/diagpatch_
bug11725986.jar -Djdkpatchlog=/u01/EM12/oms/sysman/log/diagpatch_bug11725986.log
-Doracle.apm.home=/u01/EM12/oms/apm/ -DAPM_
HELP_FILENAME=oesohwconfig.xml -Djava.util.logging.config.file=/tmp/logging.txt"
```

```
JAVA_OPTIONS="{JAVA_OPTIONS}" -Djbo.recyclethreshold=100
-Djbo.ampool.maxavailablesize=5 -Djava.security.egd=file:///dev/./urandom
-Dweblogic.debug.DebugSecurityAtn=true -Dweblogic.debug.DebugWebAppSecurity=true
-Dweblogic.SSL.LoginTimeoutMillis=300000 -Djps.auth.debug=true
-Xbootclasspath/p:/u01/EM12/oms/sysman/jlib/diagpatch_bug11725986.jar
-Djdkpatchlog=/u01/EM12/oms/sysman/log/diagpatch_bug11725986.log
-Doracle.apm.home=/u01/EM12/oms/apm/ -DAPM_HELP_FILENAME=oesohwconfig.xml
-Djava.util.logging.config.file=/tmp/logging.txt "
```

In the same file, you may change the heap size settings for the following section:

```
USER_MEM_ARGS="-Xms1024m -Xmx1740m -XX:MaxPermSize=1024M -XX:-DoEscapeAnalysis
-XX:+UseCodeCacheFlushing -XX:CompileThreshold=8000 -XX:PermSize=128m"
```

Note: Oracle does not recommend changing the Xms value.

12.2.3.2 BI Publisher Configuration

If you plan on integrating BI Publisher version 11.1.1.6 with Enterprise Manager Release 12c Cloud Control, which is required for BI Publisher reports to function, add 1.5 GB to the host memory requirements stated above.

12.3 Enterprise Manager Cloud Control Performance Methodology

An accurate predictor of capacity at scale is the actual metric trend information from each individual Enterprise Manager Cloud Control deployment. This information, combined with an established, rough, starting host system size and iterative tuning and maintenance, produces the most effective means of predicting capacity for your Enterprise Manager Cloud Control deployment. It also assists in keeping your deployment performing at an optimal level.

Here are the steps to follow to enact the Enterprise Manager Cloud Control sizing methodology:

1. If you have not already installed Enterprise Manager Cloud Control, choose a rough starting host configuration as listed in [Table 12-1](#).
2. Periodically evaluate your site's vital signs (detailed later).
3. Eliminate bottlenecks using routine DBA/Enterprise Manager administration housekeeping.
4. Eliminate bottlenecks using tuning.
5. Extrapolate linearly into the future to plan for future sizing requirements.

Step one need only be done once for a given deployment. Steps two, three, and four must be done, regardless of whether you plan to grow your Enterprise Manager Cloud Control site, for the life of the deployment on a regular basis. These steps are essential to an efficient Enterprise Manager Cloud Control site regardless of its size or workload. You must complete steps two, three, and four before you continue on to step five. This is critical. Step five is only required if you intend to grow the deployment size in terms of monitored targets. However, evaluating these trends regularly can be helpful in evaluating any other changes to the deployment.

12.3.1 Step 1: Choosing a Starting Platform Cloud Control Deployment

For information about choosing a starting platform Cloud Control deployment, see [Section 12.2.1, "Overview of Sizing Guidelines"](#).

12.3.2 Step 2: Periodically Evaluating the Vital Signs of Your Site

This is the most important step of the five. Without some degree of monitoring and understanding of trends or dramatic changes in the vital signs of your Enterprise Manager Cloud Control site, you are placing site performance at serious risk. Every monitored target sends data to the Management Repository for loading and aggregation through its associated Management Agent. This adds up to a considerable volume of activity that requires the same level of management and maintenance as any other enterprise application.

Enterprise Manager has "vital signs" that reflect its health. These vital signs should be monitored for trends over time as well as against established baseline thresholds. You must establish realistic baselines for the vital signs when performance is acceptable. Once baselines are established, you can use built-in Oracle Enterprise Manager Cloud Control functionality to set baseline warning and critical thresholds. This allows you to be notified automatically when something significant changes on your Enterprise Manager site. The following table is a point-in-time snapshot of the Enterprise Manager Cloud Control vital signs for two sites:

Module	Metrics	EM Site 1	EM Site 2
Site		emsite1	emsite2
Target Counts	Database Targets	192 (45 not up)	1218 (634 not up)
	Host Targets	833 (12 not up)	1042 (236 not up)
	Total Targets	2580 (306 not up)	12293 (6668 not up)
Overall Status	Overall Backoff Requests in the Last 10 Mins	0	500
Job Statistics	Estimated time for clearing current Job steps backlogJob	0.1	7804
Event Statistics	Pending Events Count	2	4000
Management Service Host Statistics	Average % CPU (Host 1)	9 (emhost01)	13 (emhost01)
	Average % CPU (Host 2)	6 (emhost02)	17 (emhost02)
	Average % CPU (Host 3)	N/A	38 (em6003)
	Average % CPU (Host 4)	N/A	12 (em6004)
	Number of cores per host	2 X 2.8 (Xeon)	4 X 2.4 (Xeon)
	Memory per Host (GB)	8	8
Management Repository Host Statistics	Average % CPU (Host 1)	12 (db01rac)	64 (em6001rac)
	Average % CPU (Host 2)	14 (db02rac)	78 (em6002rac)
	Number of CPU cores per host	4	8
	Memory target (GB)	5.25	7.5
	Memory per Host (GB)	8	16

Module	Metrics	EM Site 1	EM Site 2
	Total Management Repository Size (GB)	56	98
	Oracle RAC Interconnect Traffic (MB/s)	1	4
	Management Server Traffic (MB/s)	4	4
	Total Management Repository I/O (MB/s)	6	27
Enterprise Manager UI Page Response/Sec	Home Page	3	6
	All Host Page	3	30+
	All Database Page	6	30+
	Database Home Page	2	2
	Host Home Page	2	2

The two Enterprise Manager sites are at the opposite ends of the scale for performance.

EM Site 1 is performing very well with very few backoff requests. It also has a very low job and event backlogs. The CPU utilization on both the OMS and Management Repository Server hosts are low. Most importantly, the UI Page Response times are excellent. To summarize, Site 1 is doing substantial work with minimal effort. This is how a well configured, tuned and maintained Oracle Enterprise Manager Cloud Control site should look.

Conversely, EM Site 2 is having difficulty. The site has substantial amounts of backoffs and sizable job and event backlogs. Worst of all are the user interface page response times. There is clearly a bottleneck on Site 2, possibly more than one.

These vital signs are all available from within the Enterprise Manager interface. Most values can be found on the All Metrics page for each host, or the All Metrics page for the OMS. Keeping an eye on the trends over time for these vital signs, in addition to assigning thresholds for warning and critical alerts, allows you to maintain good performance and anticipate future resource needs. You should plan to monitor these vital signs as follows:

- Take a baseline measurement of the vital sign values seen in the previous table when the Enterprise Manager Cloud Control site is running well.
- Set reasonable thresholds and notifications based on these baseline values so you can be notified automatically if they deviate substantially. This may require some iteration to fine-tune the thresholds for your site. Receiving too many notifications is not useful.
- On a daily (or weekly at a minimum) basis, watch for trends in the 7-day graphs for these values. This will not only help you spot impending trouble, but it will also allow you to plan for future resource needs.

The next step provides some guidance of what to do when the vital sign values are not within established thresholds. Also, it explains how to maintain your site's performance through routine housekeeping.

12.3.3 Step 3: Using DBA and Enterprise Manager Tasks To Eliminate Bottlenecks

It is critical to note that routine housekeeping helps keep your Enterprise Manager Cloud Control site running well. The following are lists of housekeeping tasks and the interval on which they should be done.

12.3.3.1 Offline Monthly Tasks

Enterprise Manager Administrators should monitor the database built-in Segment Advisor for recommendations on Enterprise Manager Repository segment health. The Segment Advisor advises administrators which segments need to be rebuilt/reorganized and provides the commands to do so.

For more information about Segment Advisor and issues related to system health, refer to notes 242736.1 and 314112.1 in the My Oracle Support Knowledge Base.

12.3.4 Step 4: Eliminating Bottlenecks Through Tuning

The most common causes of performance bottlenecks in the Enterprise Manager Cloud Control application are listed below (in order of most to least common):

1. Housekeeping that is not being done (far and away the biggest source of performance problems)
2. Hardware or software that is incorrectly configured
3. Hardware resource exhaustion

When the vital signs are routinely outside of an established threshold, or are trending that way over time, you must address two areas. First, you must ensure that all previously listed housekeeping is up to date. Secondly, you must address resource utilization of the Enterprise Manager Cloud Control application. The vital signs listed in the previous table reflect key points of resource utilization and throughput in Enterprise Manager Cloud Control. The following sections cover some of the key vital signs along with possible options for dealing with vital signs that have crossed thresholds established from baseline values.

12.3.4.1 High CPU Utilization

When you are asked to evaluate a site for performance and notice high CPU utilization, there are a few common steps you should follow to determine what resources are being used and where.

1. Use the Processes display on the Enterprise Manager Host home page to determine which processes are consuming the most CPU on any Management Service or Management Repository host that has crossed a CPU threshold.
2. Once you have established that Enterprise Manager is consuming the most CPU, use Enterprise Manager to identify what activity is the highest CPU consumer. Typically this manifests itself on a Management Repository host where most of the Management Service's work is performed. Here are a few typical spots to investigate when the Management Repository appears to be using too many resources.
 - a. Click the CPU Used database resource listed on the Management Repository's Database Performance page to examine the SQL that is using the most CPU at the Management Repository.
 - b. Check the Database Locks on the Management Repository's Database Performance page looking for any contention issues.

- c. Check the SQL Monitoring on the Management Repository's Database for any resource intensive SQL.

High CPU utilization is probably the most common symptom of any performance bottleneck. Typically, the Management Repository is the biggest consumer of CPU, which is where you should focus. A properly configured and maintained Management Repository host system that is not otherwise hardware resource constrained should average roughly 40 percent or less total CPU utilization. An OMS host system should average roughly 20 percent or less total CPU utilization. These relatively low average values should allow sufficient headroom for spikes in activity. Allowing for activity spikes helps keep your page performance more consistent over time. If your Enterprise Manager Cloud Control site interface pages happen to be responding well (approximately 3 seconds) while there are no significant backlogs, and it is using more CPU than recommended, you may not have to address it unless you are concerned it is part of a larger upward trend.

The recommended path for tracking down the root cause of high Management Repository CPU utilization is captured under step 3.b and 3.c listed above. This allows you to start at the Management Repository Performance page and work your way down to the SQL that is consuming the most CPU in its processing. This approach has been used very successfully on several real world sites.

If you are running Enterprise Manager on Intel based hosts, the Enterprise Manager Cloud Control Management Service and Management Repository will both benefit from Hyper-Threading (HT) being enabled on the host or hosts on which they are deployed. HT is a function of certain late models of Intel processors, which allows the execution of some amount of CPU instructions in parallel. This gives the appearance of double the number of CPUs physically available on the system. Testing has proven that HT provides approximately 1.5 times the CPU processing power as the same system without HT enabled. This can significantly improve system performance. The Management Service and Management Repository both frequently have more than one process executing simultaneously, so they can benefit greatly from HT.

12.3.4.2 Loader Vital Signs

The vital signs for the loader indicate exactly how much data is continuously coming into the system from all the Enterprise Manager Agents. The most important item here is the "Number of Agents Sent Back in the Last Hour" metric. The metric can be found in the All Metrics page of each management service. This is the number of agents instructed to defer loading of data in the last hour. Ideally no agent should be instructed to defer loading, but some level of deferred loading is normal. If this value is above 2 percent of your deployed agent count and it is growing continuously, then action should be taken.

The number of Loader Threads is always set to 20 per OMS by default. Adding loader threads to an OMS increases the overall host CPU utilization. Customers can change this value as their site requires.

There are diminishing returns when adding loader threads if your repository does not have sufficient resources available. If you have available repository resources, as you add loader threads, you should see the "Number of Agents Sent Back in the Last Hour" metric decrease. If you are not seeing improvement you should explore other tuning or housekeeping opportunities.

To add more loader threads, you can change the following configuration parameter:

oracle.sysman.core.gloader.max_recv_thread

The default value is 20. This is a per OMS setting.

12.3.4.3 Rollup Vital Signs

The rollup process is the aggregation mechanism for Enterprise Manager Cloud Control. The two vital signs for the rollup are the rows/second and % of hour run. Due to the large volume of data rows processed by the rollup, it tends to be the largest consumer of Management Repository buffer cache space. Because of this, the rollup vital signs can be great indicators of the benefit of increasing buffer cache size.

Rollup rows/second shows exactly how many rows are being processed, or aggregated and stored, every second. This value is usually around 2,000 (+/- 500) rows per second on a site with a decent size buffer cache and reasonable speedy I/O. A downward trend over time for this value may indicate a future problem, but as long as % of hour run is under 100 your site is probably fine.

If rollup % of hour run is trending up (or is higher than your baseline), and you have not yet set the Management Repository buffer cache to its maximum, it may be advantageous to increase the buffer cache setting. Usually, if there is going to be a benefit from increasing buffer cache, you will see an overall improvement in resource utilization and throughput on the Management Repository host. The loader statistics will appear a little better. CPU utilization on the host will be reduced and I/O will decrease. The most telling improvement will be in the rollup statistics. There should be a noticeable improvement in both rollup rows/second and % of hour run. If you do not see any improvement in any of these vital signs, you can revert the buffer cache to its previous size. The old Buffer Cache Hit Ratio metric can be misleading. It has been observed in testing that Buffer Cache Hit Ratio will appear high when the buffer cache is significantly undersized and Enterprise Manager Cloud Control performance is struggling because of it. There will be times when increasing buffer cache will not help improve performance for Cloud Control. This is typically due to resource constraints or contention elsewhere in the application. Consider using the steps listed in the High CPU Utilization section to identify the point of contention. Cloud Control also provides advice on buffer cache sizing from the database itself. This is available on the database Memory Parameters page.

One important thing to note when considering increasing buffer cache is that there may be operating system mechanisms that can help improve Enterprise Manager Cloud Control performance. One example of this is the "large memory" option available on Red Hat Linux. The Linux OS Red Hat Advanced Server™ 2.1 (RHAS) has a feature called big pages. In RHAS 2.1, bigpages is a boot up parameter that can be used to pre-allocate large shared memory segments. Use of this feature, in conjunction with a large Management Repository SGA, can significantly improve overall Cloud Control application performance. Starting in Red Hat Enterprise Linux™ 3, big pages functionality is replaced with a new feature called huge pages, which no longer requires a boot-up parameter.

12.3.4.4 Rollup Process

The Rollup process introduces the concept of rollup participating instance; where rollup processing will be distributed among all participating instances. To add a candidate instance to the participating EMROLLUP group, the parameter `instance_groups` should be set on the instance level as follows:

- Add `EMROLLUP_1` to the `instance_group` parameter for node 1
Add `EMROLLUP_2` to the `instance_group` parameter for node 2
- Introduce the `PQ` and `PW` parallel processing modes where:
 - `PQ` is the parallel query/parallel dml mode. In this mode, each participating instance will have one worker utilizing the parallel degree specified.

- PW is the parallel worker mode. In this mode, each participating instance will have a number of worker jobs equal to the parallel level specified
- Distribute the work load for all participating Oracle RAC instances as follows:
 - Each participating instance will be allocated equal number of targets. So for (n) number of participating instances with total workload (tl), each instance will be allocated (tl/n) .
 - Each worker on any participating instance will be allocated equal number of targets of that instance workload. So for (il) number of targets per instance with (w) number of workers, each worker will be allocated (il/w) .
 - For each worker, the load is further divided into batches to control the number of times the rollup SQL is executed. The number of rows per batch will be the total number of rows allocated for the worker divided by the number of batches.

Use the following recommendations as guidelines during the Rollup process:

- Use the parallel worker (PW) mode, and utilize the participating EMROLLUP_xx instance group.
- The recommendation is to use the parallel worker mode.
- Splitting the work among more workers will improve the performance and scalability until a certain point where the diminishing returns rule will apply. This is dependent on the number of CPUs available on each Oracle RAC node. In this test case, running with 10 workers was the optimal configuration, balancing the response time, machine CPU and IO utilization.
- It is important to set a proper batch size (10 recommended). The optimal run was the one with 10 batches, attributed to balancing the number of executions of the main SQL (calling EMD_1HOUR_ROLLUP) and the sort space needed for each individual execution.
- Start by setting the number of batches to 10 bearing in mind the number of batches can be changed based on the data distribution.

The recommendations above will yield the following results. Using the multi-instance parallel worker (8 PW) mode (with the redesigned code described earlier) improves the performance by a factor of 9-13 when utilizing two participating Oracle RAC instances.

Rollup row count (in millions) in MGMT_METRICS_1HOUR			
	Time (min)	Workers	Batch Size
29.5	30	8	1
9.4	5	8	10

** For the entire test there were 15779 distinct TARGET_GUID

** The test produced "29.5 Million" new rollup rows in MGMT_METRICS_1HOUR

Run **	Rows/Workers	Batches/Workers	Rows/Batch	Time (min)
8 PW /1 instance	3945	3945	1	40
8 PW /2 instances	1973	1973	1	30

12.3.4.5 Job, Notification, and Alert Vital Signs

Jobs, notifications, and alerts are indicators of the processing efficiency of the Management Service(s) on your Enterprise Manager Cloud Control site. Any negative trends in these values are usually a symptom of contention elsewhere in the application. The best use of these values is to measure the benefit of running with more than one OMS. There is one job dispatcher in each OMS. Adding OMS instances will not always improve these values. In general, adding OMS instances will improve overall throughput for Cloud Control when the application is not otherwise experiencing resource contention issues. Job, Notification, and Alert vital signs can help measure that improvement.

12.3.4.6 I/O Vital Signs

Monitoring the I/O throughput of the different channels in your Enterprise Manager Cloud Control deployment is essential to ensuring good performance. At minimum, there are three different I/O channels on which you should have a baseline and alert thresholds defined:

- Disk I/O from the Management Repository instance to its data files
- Network I/O between the OMS and Management Repository
- Oracle RAC interconnect (network) I/O (on Oracle RAC systems only)

You should understand the potential peak and sustained throughput I/O capabilities for each of these channels. Based on these and the baseline values you establish, you can derive reasonable thresholds for warning and critical alerts on them in Cloud Control. You will then be notified automatically if you approach these thresholds on your site. Some Cloud Control site administrators can be unaware or mistaken about what these I/O channels can handle on their sites. This can lead to Enterprise Manager Cloud Control saturating these channels, which in turn cripples performance on the site. In such an unfortunate situation, you would see that many vital signs would be impacted negatively.

To discover whether the Management Repository is involved, you can use Cloud Control to check the Database Performance page. On the Performance page for the Management Repository, click the wait graph showing the largest amount of time spent. From this you can continue to drill down into the actual SQL code or sessions that are waiting. This should help you to understand where the bottleneck is originating.

Another area to check is unexpected I/O load from non-Enterprise Manager Cloud Control sources like backups, another application, or a possible data-mining co-worker who engages in complex SQL queries, multiple Cartesian products, and so on.

Total Repository I/O trouble can be caused by two factors. The first is a lack of regular housekeeping. Some of the Cloud Control segments can be very badly fragmented causing a severe I/O drain. Second, there can be some poorly tuned SQL statements consuming much of the site I/O bandwidth. These two main contributors can cause most of the Cloud Control vital signs to plummet. In addition, the lax housekeeping can cause the Management Repository's allocated size to increase dramatically.

One important feature of which to take advantage is asynchronous I/O. Enabling asynchronous I/O can dramatically improve overall performance of the Cloud Control application. The Sun Solaris™ and Linux operating systems have this capability, but may be disabled by default. The Microsoft Windows™ operating system uses asynchronous I/O by default. Oracle strongly recommends enabling of this operating

system feature on the Management Repository hosts and on Management Service hosts as well.

Automatic Storage Management (ASM) is recommended for Enterprise Manager Cloud Control repository database storage.

12.3.4.7 About the Oracle Enterprise Manager Performance Page

There may be occasions when Enterprise Manager user interface pages are slow in the absence of any other performance degradation. The typical cause for these slow downs will be an area of Enterprise Manager housekeeping that has been overlooked. The first line of monitoring for Enterprise Manager page performance is the use of Enterprise Manager Beacons. These functionalities are also useful for web applications other than Enterprise Manager.

Beacons are designed to be lightweight page performance monitoring targets. After defining a Beacon target on an Management Agent, you can then define UI performance transactions using the Beacon. These transactions are a series of UI page hits that you will manually walk through once. Thereafter, the Beacon will automatically repeat your UI transaction on a specified interval. Each time the Beacon transaction is run, Enterprise Manager will calculate its performance and store it for historical purposes. In addition, alerts can be generated when page performance degrades below thresholds you specify.

When you configure the Enterprise Manager Beacon, you begin with a single predefined transaction that monitors the home page you specify during this process. You can then add as many transactions as are appropriate. You can also set up additional Beacons from different points on your network against the same web application to measure the impact of WAN latency on application performance. This same functionality is available for all Web applications monitored by Enterprise Manager Cloud Control.

After you are alerted to a UI page that is performing poorly, you can then use the second line of page performance monitoring in Enterprise Manager Cloud Control. This new end-to-end (or E2E) monitoring functionality in Cloud Control is designed to allow you to break down processing time of a page into its basic parts. This will allow you to pinpoint when maintenance may be required to enhance page performance. E2E monitoring in Cloud Control lets you break down both the client side processing and the server side processing of a single page hit.

The next page down in the Middle Tier Performance section will break out the processing time by tier for the page. By clicking the largest slice of the Processing Time Breakdown pie chart, which is JDBC time above, you can get the SQL details. By clicking the SQL statement, you break out the performance of its execution over time.

The JDBC page displays the SQL calls the system is spending most of its page time executing. This SQL call could be an individual DML statement or a PL/SQL procedure call. In the case of an individual SQL statement, you should examine the segments (tables and their indexes) accessed by the statement to determine their housekeeping (rebuild and reorg) needs. The PL/SQL procedure case is slightly more involved because you must look at the procedure's source code in the Management Repository to identify the tables and associated indexes accessed by the call.

Once you have identified the segments, you can then run the necessary rebuild and reorganization statements for them with the OMS down. This should dramatically improve page performance. There are cases where page performance will not be helped by rebuild and reorganization alone, such as when excessive numbers of open alerts, system errors, and metric errors exist. The only way to improve these calls is to address (for example, clean up or remove) the numbers of these issues. After these

numbers are reduced, then the segment rebuild and reorganization should be completed to optimize performance. These scenarios are covered in [Section 12.3.3](#). If you stay current, you should not need to analyze UI page performance as often, if at all.

12.3.4.8 Determining the Optimum Number of Middle Tier OMS Servers

Determining the optimum number of middle tier OMS servers is not a trivial task. A number of data points must be considered for an informed, justified and acceptable decision for introducing additional OMS instances. The number of monitored targets is one of the first considerations, but its weight in decision making is normally not substantial.

The following items should be considered and examined as part of this exercise:

- The volume of job automation and scheduling used
- The number of administrators working simultaneously in the console
- Network bandwidth and data channel robustness from agents to the OMS servers
- Number of triggered violations and notifications
- Speed and stability of the IO system the OMS servers use

Careful investigation of each category is essential to making an informed decision. In some cases, just adding an OMS server or providing more CPU or memory to the same host may not make any difference in performance enhancement. You can use the current running OMS instances to collect accurate statistics on current OMS performance to calculate the number of required OMS servers for current or future deployments. Enterprise Manager has "vital signs" that reflect its health. These vital signs should be monitored for trends over time as well as against established baseline thresholds.

12.3.5 Step 5: Extrapolating Linearly Into the Future for Sizing Requirements

Determining future storage requirements is an excellent example of effectively using vital sign trends. You can use two built-in Cloud Control charts to forecast this: the total number of targets over time and the Management Repository size over time.

Both of the graphs are available on the All Metrics page for the Management Service. It should be obvious that there is a correlation between the two graphs. A straight line applied to both curves would reveal a fairly similar growth rate. After a target is added to Enterprise Manager Cloud Control for monitoring, there is a 31-day period where Management Repository growth will be seen because most of the data that will consume Management Repository space for a target requires approximately 31 days to be fully represented in the Management Repository. A small amount of growth will continue for that target for the next year because that is the longest default data retention time at the highest level of data aggregation. This should be negligible compared with the growth over the first 31 days.

When you stop adding targets, the graphs will level off in about 31 days. When the graphs level off, you should see a correlation between the number of targets added and the amount of additional space used in the Management Repository. Tracking these values from early on in your Enterprise Manager Cloud Control deployment process helps you to manage your site's storage capacity proactively. This history is an invaluable tool.

The same type of correlation can be made between CPU utilization and total targets to determine those requirements. There is a more immediate leveling off of CPU utilization as targets are added. There should be no significant increase in CPU cost

over time after adding the targets beyond the relatively immediate increase. Introducing new monitoring to existing targets, whether new metrics or increased collections, would most likely lead to increased CPU utilization.

12.3.6 Using Returning Query Safeguards to Improve Performance

On the All Targets page, Enterprise Manager uses a safeguard that prevents a flood of data from slowing performance and consuming excessive resources within the OMS by limiting the number of rows that can be returned from a query. By default, the limit is set to 2000, but an Enterprise Manager administrator can modify the limit with the following command:

```
emctl set property -name oracle.sysman.core.uifwk.maxRows -value 2000
```

Providing a value equal to 0 will turn off the safeguard and fetch all rows. The new value takes immediate effect; no OMS restart is required. If the value is less than 0, the default value (2000) will be used instead. The only way to indicate that no limiting should be performed is to set the value to exactly 0.

When there are too many results returned from a query and this limit comes into effect, the following message appears under the results table:

"This table of search results is limited to 2000 targets. Narrow the results by using Refine Search or Search Target Name. See the tuning guide for how to modify this limit."

Similar behaviors (and messages) are applied to other large tables throughout Enterprise Manager. The same OMS property (`oracle.sysman.core.uifwk.maxRows`) controls the maximum limit for all of them together. This matches the behavior (and reuses the existing property) from previous Enterprise Manager releases.

12.4 Overview of Repository and Sizing Requirements for Fusion Middleware Monitoring

A Fusion Middleware target is like any other Enterprise Manager target. Therefore any repository or sizing guideline that is applicable for an Enterprise Manager target would be applicable on a Fusion Middleware target.

One major concern in the case of Fusion Middleware discovery is that too many targets may be discovered, created and monitored. This adds additional load on the OMS instance, repository and agent. In the case of very large number of targets, after target discovery Oracle recommends that users should review all the targets and their respective metrics.

Based on requirements, users should finalize which targets and metrics should be monitored and the required frequency those targets should be monitored.

After discovery, Oracle recommends you allow Fusion Middleware/ADP/JVMD monitoring to run for some duration (a few days to possibly a few weeks) and continuously monitor the database size and Operating System file system growth (in the case of ADP; ADP Manager requires a minimum of 10GB of disk space) until it becomes constant. You can then fine tune various parameters associated with these different features.

In version 12c of Enterprise Manager, both ADP and JVMD use Enterprise Manager repository as their repository. Their data are stored in the `MGMT_AD4J_TS` tablespace.

12.4.1 ADP Monitoring

Use the following information when utilizing ADP Monitoring.

- ADP Manager Resources Requirement

While managing 70K managed entities, if the number of managed entities is high you must allocate resources accordingly.

Resource	Amount
Physical Memory	2 GB
Minimum Disk Space	10 GB

- ADP Data requirement

To monitor each entity per JVM, the MGMT_AD4J_TS tablespace must have 8 MB available.

- ADP Data Retention Policy

ADP maintains sophisticated multi-tiered logic for aggregation (or compression) of performance data. This helps to optimize performance of interaction with the internal data repository both when querying data for presentation or inserting new performance metrics.

Users who want to store longer term data should look for this section in *Acsera.properties*:

Example 12-1

```
#####
# Production setting
# NOTE: use Model.GlobalSamplingRateSecs to configure Metric.Grain.0
#####
Metric.Grain.0 0s
Metric.TableInterval.0 = 4h
Metric.DataLife.0 = 2d

Metric.Grain.1 = 3m
Metric.TableInterval.1 =1d
Metric.DataLife.1 = 8d

#Metric.Grain.2 = 30m
#Metric.TableInterval.2 = 7d
#Metric.DataLife.2 = 420d
```

Uncomment the last 3 lines for the *Metric.*.2* properties.

12.4.2 JVMD Monitoring

Use the following information when employing JVMD Monitoring.

- JVMD Manager Resources Requirement

To manage 200-300 jvms, JVMD manager requires physical memory of 1 GB. JVMD manager caches monitoring data in the TEMP space for each pool and flushes to the database frequently. Usually, depending on the number of pools the manager is monitoring and the amount of data being gathered from each pool, the size requirement of these temporary cache files varies, but it is rare to see more

than a few MBs for each pool. If this is a concern, the TEMP space should be allocated accordingly.

- **JVMD Data requirement**

To monitor every JVM with OOB settings, the MGMT_AD4J_TS tablespace must have 50-100MB available.

- **JVM Diagnostics Historical Data and its Retention policy**

Historical data is available at three summary levels 0, 1 and 2.

- Summary level 0 - is raw sample data taken at the specified pool polling interval (default 2 seconds). If you look at data within one hour on the Performance Diagnostics page, it shows summary level 0 data. Level 0 data is retained for 24 hours and subsequently purged. It can be changed via the Console Setup page, but before increasing the value, you should ensure that the repository is tuned properly to handle such large amounts of data.
- Summary level 1 - is aggregated data. If you view data after more than one hour but less than 5 hours, it is summary level 1 data. The default aggregation interval is 90 seconds. This value can be changed via the Console Setup page. Level 1 data is retained for 20 days and subsequently purged.
- Summary level 2 - is further aggregated data. If you view data more than five hours old, it is summary level 2 data. This data is aggregated every 60 minutes. Level 2 data is retained for 400 days and subsequently purged.

There are two JVMD features that can drastically affect MGMT_AD4J_TS tablespace usage:

- **JVMD Heap Dumps**

Analyzing heap requires massive tablespace resources. Oracle recommends having 5 times the size of the heap dump file you are loading free in your tablespace. Since you will have the heap dump file and know its size before you run the load script, you should ensure that you have adequate space to accommodate the dump before you load it into your database.

- **Thread Traces**

While these are smaller than heaps by an order of magnitude, these are loaded into the database automatically by default when you initiate a trace at the console. The size of these traces can vary dramatically depending on the number of active threads during the trace, the duration of the trace, and the sample interval of the trace. They should generally be under 100MB each, but a user utilizing a large number of these could manually fill up the database quickly. Again, since these are created only by manual intervention, you should ensure that there is adequate space to accommodate traces before initiating them.

Installing ADP with Advanced Installation Options

This chapter describes how you can install Application Dependency and Performance (ADP) in the Enterprise Manager Cloud Control environment.

In particular, this chapter covers the following:

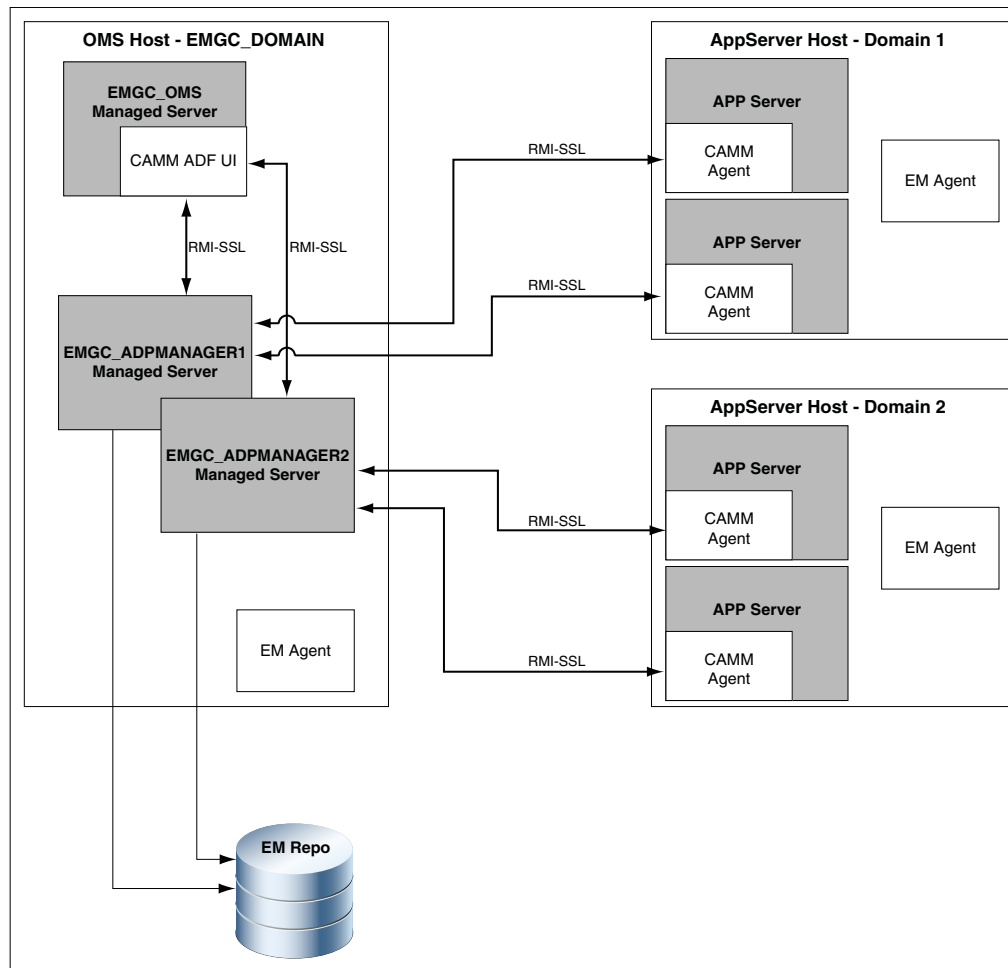
- [Application Dependency and Performance Architecture](#)
- [Before you Begin](#)
- [Prerequisites](#)
- [Installation Procedure](#)
- [After You Install](#)

13.1 Application Dependency and Performance Architecture

Application Dependency and Performance (ADP) is one of the critical functionalities in Enterprise Manager Cloud Control that allows you to analyze Java EE, SOA, and Portal applications. It captures the complex relationships among various application building blocks in its application schema model - the core of the Oracle intelligent platform. To manage these applications effectively, enterprises must first gain an understanding of the complex relationships among the business functions, associated interconnected components, and the underlying runtime environments. To enable clear and accurate understanding, IT organizations need holistic, service-oriented views that span across heterogeneous environments.

Using the insights stored in Application Schema, ADP is able to deliver an Application Service Management (ASM) environment that self-customizes out-of-the-box, evolves with change, minimizes expert involvement, and delivers a holistic, service-oriented view across heterogeneous environments.

ADP employs a multi-tier, fully distributed, configurable architecture to provide the scalability and flexibility to meet the changing needs of enterprise deployments.

Figure 13–1 ADP Architecture

ADP Engine is the core analytical engine of the ADP ASM system. In real-time, ADP Engine performs complex mathematical modeling and statistical calculations with summarized data from all ADP Java Agents. ADP Engine can be configured with a backup to provide higher level of availability.

ADP Java Agents are the data collectors of the ADP ASM system. ADP Java Agents are deployed to all managed application servers to perform a series of tasks including collecting performance managements, tracking contextual relationships, and summarizing data in real-time while introducing as little overhead as possible.

13.2 Before you Begin

Before installing ADP Engine or ADP Agent, review the points outlined in *Oracle Enterprise Manager Basic Installation Guide*.

13.3 Prerequisites

Before installing ADP Engine or ADP Agent, ensure that you meet the prerequisites described in *Oracle Enterprise Manager Basic Installation Guide*.

13.4 Installation Procedure

This section describes the following:

- [Deploying ADP Engines](#)
- [Deploying ADP Agents Manually Using `deploy_adpagent.pl`](#)

13.4.1 Deploying ADP Engines

This section describes the methods to deploy ADP Engines. It consists of the following:

- [Deploying ADP Engine on a Remote Host](#)
- [Deploying ADP Engine Manually Using `ApmEngineSetup.pl`](#)

13.4.1.1 Deploying ADP Engine on a Remote Host

To deploy ADP Engine on a remote host (that is, any host on which Oracle Management Service is not installed), follow these steps:

1. [Meet the Prerequisites.](#)
2. [Deploy ADP Engine on the Remote Host.](#)

13.4.1.1.1 Meet the Prerequisites

Note: This section will use the following convention:

- `host-a` is the host where the OMS is running.
 - `host-b` is the remote host that does not have an OMS running.
-

1. Install a Management Agent on `host-b` (the remote host), and point it to the OMS running on a Managed Server present in the Enterprise Manager Cloud Control domain (`EMGC_DOMAIN`).

For information about installing a Management Agent, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

2. Install WebLogic Server on `host-b` using the Enterprise Manager Software Only installation option.

To install ADP Engine on a remote host successfully, the remote WebLogic Server version and patch level should match with the Managed Servers present in the Enterprise Manager Cloud Control domain (`EMGC_DOMAIN`). To ensure that the versions and patch levels match, Oracle recommends that you install WebLogic Server by selecting the Software Only install option in the Enterprise Manager OUI install.

For information about performing a software only install, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

These WebLogic Server bits must be registered with the Enterprise Manager domain running on `host-a`, so that all the Managed Servers appear under the same WebLogic domain.

3. Configure a new Managed Server using the WebLogic Server Administration Console as follows:
 - a. Log into the Enterprise Manager WebLogic Domain console (`EMGC_DOMAIN`) of `host-a`.

The WebLogic Server Administration Console home page appears.

- b. In Weblogic Server Administration Console, from the Domain Structure section, select Environment and then click **Servers**.
- c. On the Create a New Server page, enter **Server Name**, **Server Listen Address**, and **Server Listen Port**.

Note: Ensure that the Server Listen Address corresponds to the listen address of the remote host, and the Server Listen port is free on the remote host.

4. Configure a new machine using the WebLogic Server Administration Console as follows:

- a. Log into the Enterprise Manager WebLogic Domain console (EMGC_DOMAIN) of host-a.

The WebLogic Server Administration Console home page appears.

- b. In Weblogic Server Administration Console, from the Domain Structure section, select **Environment** and click **Machines**.
- c. On the Create a New Machine page, to associate this machine with the node manager running on host-b, enter the **Listen Address** of the remote host, and the node manager port number which is 5556 by default.

This node manager primarily controls the starting and stopping of a remote host.

- d. Click **Finish** to create the machine.
5. Select the newly created machine, then click on **Servers** to add the Managed Server you created to this machine. This step associates the machine with the nodemanager running on host-b.
6. To extend the WebLogic Domain, a template of the Enterprise Manager Cloud Control domain running on host-a is created using the following command:

```
./pack.sh -domain = $DOMAIN_HOME -template = <absolute_path_to_the_new_weblogic_template> - template_name="My WebLogic Domain" -managed={true}
```

Where:

\$DOMAIN_HOME is the location of EMGC domain on host-a.

<absolute_path_to_the_new_weblogic_template> is the location where you want to create the template.

7. Copy emgcdomain.jar from host-a (where the OMS is running) to host-b (remote host).
8. Run the following command to unpack emgcdomain.jar template on host-b:

```
./unpack.sh -domain = $DOMAIN_HOME -template= <absolute_path_to_domain_template_created>
```

Where:

\$DOMAIN_HOME is the domain location of EMGC on host-b (remote host)

<absolute_path_to_domain_template_created> is the location of the template on

host-b where emgcdomain.jar template is present.

9. To enroll the WebLogic Domain with node manager, perform the following steps on host-b:

- a. Run the following command to update the node manager properties file so that it can start monitoring the remote host:

```
$WEBLOGIC_HOME/common/bin/wlst.sh
nmEnroll($DOMAIN_HOME)
```

- b. Start the Node Manager as follows:

```
<$WEBLOGIC_HOME>server/bin/startNodeManager.sh
```

Note: Ensure that you set the property in the nodemanager property file before starting the Node Manager. You can set the property in one of the following methods:

- Manually edit the nodemanager.properties file to set the property startScriptEnabled=true.
 - Run the script setNMProps.sh as follows: \$MIDDLEWARE_HOME/oracle_common/common/bin/setNMProps.sh
-

- c. Perform the following steps to modify startWebLogic.sh:

- a. Navigate to the following location:

```
- On Unix      : $DOMAIN_HOME/bin/startWebLogic.sh
- On Windows : $DOMAIN_HOME/bin/startWebLogic.cmd
```

- b. Set maximum heap size (-Xmx) to 1.7 GB for 64 bit systems, and maximum permanent generation (-XX:MaxPermSize) to 768M for 64-bit systems, as follows:

```
USER_MEM_ARGS="-Xms256m -Xmx1740m -XX:MaxPermSize=768m"
```

Note: If the remote Managed Server is started using a Sun JVM, then you must add following memory options to USER_MEM_ARGS: XX:+UnlockDiagnosticVMOptions and XX:+UnsyncloadClass.

- c. Set maximum heap size to 1.4 GB for 32-bit systems, and maximum permanent generation to 512M for 32-bit systems, as follows:

```
USER_MEM_ARGS="-Xms256m -Xmx1434m -XX:MaxPermSize=512m"
```

10. Perform the following steps on host-a, then start the newly created Managed Server as follows:

- a. Copy the emreposauthbean.jar located in \$OMS_HOME/sysman/jlib, to <middleware_home>/wlserver_10.3/server/lib/mbeantypes. Where, \$OMS_HOME is the location of the OMS server on host-a, and <middleware_home> is on host-b.
- b. Copy the emCoreCommon.jar from \$WEBLOGIC_HOME/sysman/jlib on host-a to \$WEBLOGIC_HOME/server/lib on host-b.
- c. Import SSL Certificate to Enterprise Manager Agent Trust store present on the host where Managed Server is running.

- d. Start the Managed Server from the WebLogic Server Administration Console to complete the WebLogic Server setup.
11. Perform the following steps to discover the new Managed Server running on `host-b`:
 - a. In Cloud Control, from the **Targets** menu, select **Middleware**.

On the Middleware page, from the list of WebLogic servers running, select the WebLogic domain where the new Managed Server is deployed (that is, `EMGC_DOMAIN`).
 - b. On the Cloud Control Domain page, from the **WebLogic Domain** menu, select **Refresh WebLogic Domain**.

The new Managed Server now gets registered in the Enterprise Manager Cloud Control domain.
12. Restart the Managed Server for all the changes to take effect.

13.4.1.1.2 Deploy ADP Engine on the Remote Host

To deploy ADP Engine on a remote host (that is, any host that does not have Oracle Management Service installed), follow these steps:

1. From the **Setup** menu, select **Middleware Management**, then select **Application Performance Management**.
2. On the Application Performance Management page, from the **Add** menu, select Application Dependency and Performance Engine.
3. On the Deploy ADP Engine page, select **Deploy on an existing managed server**.

For **Managed server**, select the Managed Server running on the remote host on which you want to deploy ADP Engine. The drop-down list displays all the Managed Servers present in the Enterprise Manager WebLogic domain.

For **ADP Engine Registry Port**, **ADP Engine Java Provider Port**, and **ADP Engine Controller Port**, enter the port values you want to use. Ensure that the port values you enter are not already in use. By default, these fields are assigned the values 51099, 55003, and 55000 respectively.

4. Specify values for **Oracle WebLogic Administration Server Host Credentials**, **Oracle WebLogic Server Domain Credentials**, and **Oracle WebLogic Managed Server Host Credentials**.

Oracle WebLogic Administration Server Host Credentials are the host credentials for the host on which the WebLogic Administration Server (for the Enterprise Manager WebLogic domain) is deployed. Oracle WebLogic Domain Credentials are the credentials for the Administration Server of the Enterprise Manager WebLogic domain. Oracle WebLogic Managed Server Host Credentials are the host credentials for the host on which the WebLogic Managed Server is deployed (that is, the host credentials for the remote host).

5. Click **Deploy** to submit a deployment job to the Enterprise Manager system.

Note: When you click **Deploy**, you may receive a warning mentioning that the WebLogic domain is already in edit mode, and mentioning the number of unsaved changes and non active changes. If there are no unsaved or non active changes, or if you are sure that the changes will not affect the ADP Engine deployment, ignore this warning and proceed.

The ADP Engine Deployment Status page appears with a link to the job status. Click the link to view the status of the job that you submitted.

13.4.1.2 Deploying ADP Engine Manually Using ApmEngineSetup.pl

You can deploy ADP Engine manually, using the ApmEngineSetup.pl script. You can run this script in the following ways:

- In interactive mode, where you are prompted for input details in an interactive manner
- In silent mode, where you specify all the input details using a properties file

Important: You can use the ApmEngineSetup.pl script to deploy ADP Engine only on a host that is running the OMS, and not on a remote host.

To deploy ADP Engine manually using the ApmEngineSetup.pl script, follow these steps:

1. Navigate to the following location on the OMS host:


```
$<MIDDLEWARE_HOME>/plugins/oracle.sysman.emas.oms.plugin_12.1.0.4.0/archives/jvmd/deployment_Scripts/engine/
```
2. View the README.txt file, for information on using the ApmEngineSetup.pl script.
3. Run the ApmEngineSetup.pl script.

If you want to run the ApmEngineSetup.pl script in interactive mode, such that you are prompted for the input details, use the following command:

```
perl ApmEngineSetup.pl
```

Ensure that you specify the operation as `deploy`, and the Engine Type as `ADP`.

If you want to run the ApmEngineSetup.pl script in silent mode, specify all the input details in a properties file, then use the following command:

```
perl ApmEngineSetup.pl -silent -file <properties_file_name> -password <password>
```

<properties_file_name> is the name of the properties file where the ADP Engine and operation details are provided. <password> is the WebLogic console password.

To learn how to specify the input details in a properties file, view the sample properties file `SAMPLE_engine.properties`.

13.4.2 Deploying ADP Agents Manually Using deploy_adpagent.pl

You can deploy ADP Agents manually, using the `deploy_adpagent.pl` script. You can run this script only in silent mode, that is, you must specify all the input details using a properties file.

To deploy ADP Agents manually using `deploy_adpagent.pl`, follow these steps:

1. Navigate to the following location on the OMS host:


```
$<MIDDLEWARE_HOME>/plugins/oracle.sysman.emas.oms.plugin_12.1.0.4.0/archives/jvmd/deployment_Scripts/agent/adp/
```
2. View the README.txt file, for information on using the `deploy_adpagent.pl` script.

3. Specify all the inputs in a properties file, then use the following command:

```
perl deploy_adpagent.pl <properties_file_name>
```

If you do not pass the name of the properties file as a parameter while running `deploy_adpagent.pl`, `deploy_adpagent.pl` looks for a properties file named `adpagent.properties` in the same folder. To learn how to specify the input details in a properties file, view the sample properties file `SAMPLE_adpagent.properties`.

13.5 After You Install

This section describes the tasks you can perform after installing ADP Engines and ADP Agents. It consists of the following:

- [Verifying ADP Engine and ADP Agent Installation](#)
- [Configuring Oracle SOA Suite for Secure Connectivity](#)
- [Configuring Oracle WebLogic Server or Oracle WebLogic Portal \(WLP\) for Secure Connectivity](#)
- [Importing a Certificate into ADP Engine's Keystore](#)
- [Configuring ADP Agent When WebLogic Is Installed As a Windows Service](#)

13.5.1 Verifying ADP Engine and ADP Agent Installation

For information on verifying the ADP Engine and ADP Agent installations, refer *Oracle Enterprise Manager Basic Installation Guide*.

13.5.2 Configuring Oracle SOA Suite for Secure Connectivity

The Oracle SOA Suite may be configured to support RMIS (RMI over SSL) connectivity. In this case, ADP can be configured to use this secure connection. To configure ADP to do this, perform the following steps:

1. In the Oracle SOA Suite install, look at `ORACLE_HOME/j2ee/<instance>/config/rmi.xml`, locate the `<ssl-config>` element, and identify the path in the keystore attribute.
2. Copy the KeyStore file indicated to ADP Engine's `config` directory (for example, `em10/config`)
3. Import this KeyStore file following the instructions in [Section 13.5.4](#).

13.5.3 Configuring Oracle WebLogic Server or Oracle WebLogic Portal (WLP) for Secure Connectivity

To configure Oracle WebLogic Server 10.0 to handle connectivity using t3s, the location of the KeyStore files needs to be updated through the console. To do this, follow these steps:

1. Log in to the WebLogic Server Administration console and select the servers from the **Environment Servers** list that you plan to manage with ADP.
2. Select a server from the server list.
3. Select the **Keystores** tab, then click **Load & Edit** to update the KeyStore.
4. Identify the KeyStore and TrustStore file paths from the following properties:

Identity

Custom Identity Keystore

Trust

Custom Trust Keystore: location of the trust file

5. Repeat Steps 2 to 4 for additional server instances that you want to manage using ADP.
6. Copy the identified KeyStore and TrustStore files to the ADP Engine.
7. Copy the BEA_HOME/license.bea to the ADP Engine's config directory (for example, em11g/config).
8. Import the KeyStore and TrustStore files following the instructions in [Section 13.5.4](#).
9. Locate the following properties in the Acsera.properties file, and set them as follows:

```
weblogic.security.TrustKeyStore=CustomTrust
weblogic.security.CustomTrustKeyStoreFileName=AcseraManagerTrust.jks
weblogic.security.CustomTrustKeyStorePassPhrase=acseramanager
```

13.5.4 Importing a Certificate into ADP Engine's Keystore

To import entries from a Keystore or TrustStore, perform the following steps, replacing ServerStoreFile.jks with the KeyStore or TrustStore from your application server. You will generally need to complete these steps twice, once for the KeyStore and once for the TrustStore.

1. List the key aliases in the KeyStore/TrustStore file from the server:

```
keytool -list -keystore ServerStoreFile.jks -storepass
DemoIdentityKeyStorePassPhrase
```

Output:

```
Keystore type: jks
Keystore provider: SUN
```

Your keystore contains 1 entry:

```
demoidentity, Wed Nov 19 13:34:56 PST 2008, keyEntry, Certificate fingerprint
(MD5): 36:06:C2:44:31:0A:28:FC:06:19:F7:AB:C0:7D:27:6A
```

2. Export a key entry to an intermediate file:

```
keytool -export -alias demoidentity -keystore ServerStoreFile.jks -storepass
DemoIdentityKeyStorePassPhrase -file demo103
```

Output:

Certificate stored in file <demo103>

3. Import the key into the ADP store file (either AcseraManagerKey.jks or AcseraManagerTrust.jks in the ADP Engine's config directory)

```
keytool -import -alias demoidentity1 -keystore AcseraManagerKey.jks
-storepass acseramanager -file demo103
```

Output:

```
Owner: CN=b91, OU=FOR TESTING ONLY, O=MyOrganization, L=MyTown, ST=MyState,
```

```

C=US
Issuer: CN=CertGenCAB, OU=FOR TESTING ONLY, O=MyOrganization, L=MyTown,
ST=MyState, C=US
Serial number: 510fb3d4b2872e3a093d436fcbe9b24b
Valid from: Tue Nov 18 13:34:47 PST 2008 until: Sun Nov 19 13:34:47 PST 2023
Certificate fingerprints:
    MD5: 36:06:C2:44:31:0A:28:FC:06:19:F7:AB:C0:7D:27:6A
    SHA1: BB:85:6D:4C:0B:4A:92:63:CA:5E:E9:A8:54:42:80:2D:0D:BE:7C:91
Trust this certificate? [no]: yes
Certificate was added to keystore

```

4. Verify that the key was imported successfully:

```
keytool -list -keystore AcseraManagerKey.jks -storepass acseramanager
```

Output:

```

Keystore type: jks
Keystore provider: SUN

```

Your keystore contains 3 entries:

```

demoidentity1, Wed Apr 01 13:03:21 PST 2009, trustedCertEntry, Certificate
fingerprint (MD5): 36:06:C2:44:31:0A:28:FC:06:19:F7:AB:C0:7D:27:6A
demoidentity, Fri Mar 13 15:15:06 PST 2009, trustedCertEntry, Certificate
fingerprint (MD5): 0B:11:02:B5:44:0D:2A:CC:7F:C5:30:5C:1A:C9:A1:6C
mykey, Thu May 19 16:57:36 PDT 2005, keyEntry, Certificate fingerprint (MD5):
5D:B0:EC:28:14:33:26:1F:44:F5:BE:DD:A8:50:15:9D

```

5. Repeat Steps 2 to 4 for each key entry listed in Step 1.
6. Locate the following properties in the `Acsera.properties` file, and set them as follows:

```

weblogic.security.TrustKeyStore=CustomTrust
weblogic.security.CustomTrustKeyStoreFileName=AcseraManagerTrust.jks
weblogic.security.CustomTrustKeyStorePassPhrase=acseramanager

```

At present, with ADP running with a bundled Sun HotSpot JDK, it is not possible for ADP to configure with PKCS12 type key/trust stores for secure connections. IBM JDK has built-in enhancements that allow it to work with PKCS12 key/trust stores, such as WebSphere 6.1's default key.p12 and trust.p12 stores. Also, there is a WebSphere 6.1 automatic function that is enabled with the property `com.ibm.ssl.enableSignerExchangePrompt=true` that allows a client connecting to a secure WebSphere port that allows automatic download of server's signer certificate and update of client's truststore. However, this automatic function is only available when ADP is running with an IBM JDK, which is not the case at present. This is the reason why we need to follow the above procedure to connect with a secured WebSphere 6.1.

13.5.5 Configuring ADP Agent When WebLogic Is Installed As a Windows Service

When the monitored WebLogic Server is installed as a Windows service, the automatic startup changes to deploy ADP Agent need to be manually applied to the registry entries that control the WebLogic startup.

The parameters that need to be changed are in the Windows registry key:

```

HKEY_LOCAL_MACHINE\SYSTEM\Current
ControlSet\Services\$ServiceName\Parameters

```

Users should then consult the file on the ADP Engine:

`deploy/agent/bea9/bin/agentoptions.bat` (for WebLogic 9.x and higher)

Inspect this file and resolve the net results of its execution as parameters in the registry.

Installing JVMD with Advanced Install Options

This chapter describes how you can install JVM Diagnostics (JVMD) in the Enterprise Manager Cloud Control environment.

In particular, this chapter covers the following:

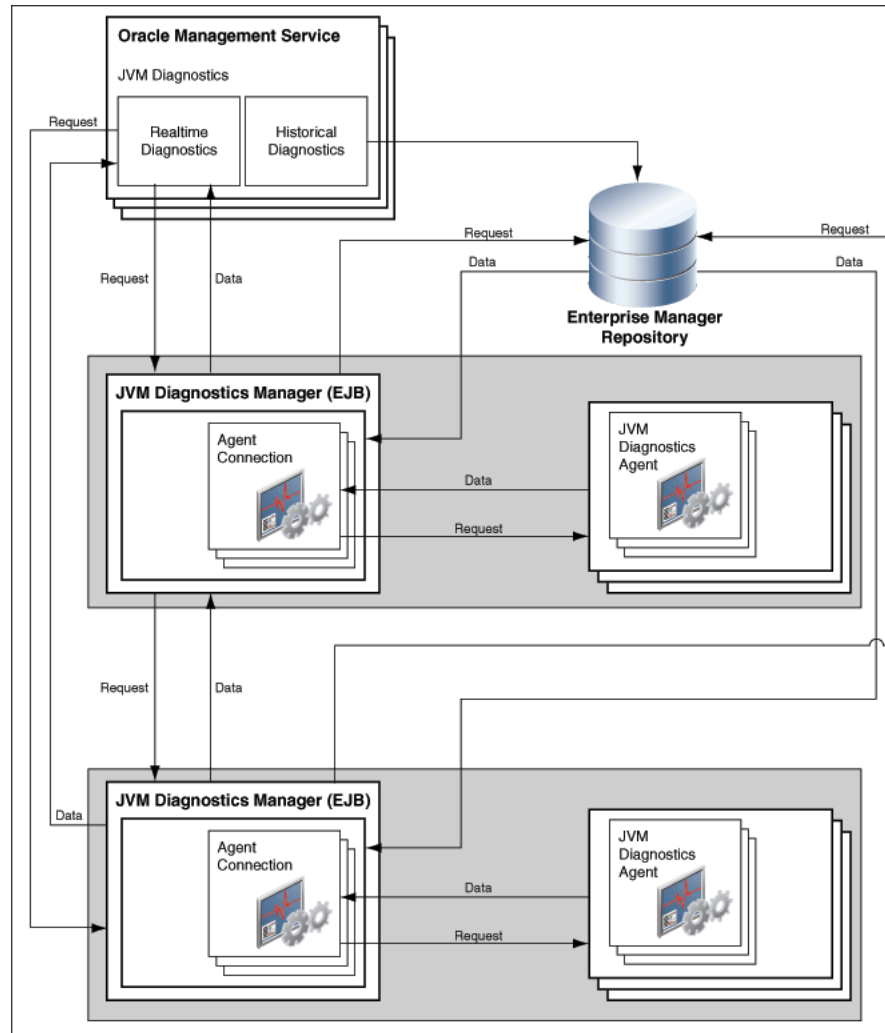
- [JVMD Architecture](#)
- [Before you Begin](#)
- [Prerequisites](#)
- [Installation Procedure](#)
- [After You Install](#)

14.1 JVMD Architecture

JVM Diagnostics is integrated with Oracle Enterprise Manager Cloud Control. It primarily enables administrators to diagnose performance problems in Java applications in the production environment. By eliminating the need to reproduce problems, it reduces the time required to resolve these problems, thus improving application availability and performance. Using JVMD, administrators can identify the root cause of performance problems in the production environment, without having to reproduce them in the test or development environment.

The following diagram shows the JVMD Architecture:

Figure 14–1 JVMD Architecture



JVMD Engine is the core analytical engine of the JVMD monitoring system. JVMD Engine collects runtime data from JVMD Agents on request from the OMS, and stores the data in the repository. Multiple JVMD Engines can be configured.

JVMD Agents are the data collectors of the target JVM. JVMD Agents are deployed to managed application servers to collect JVM monitoring data related to JVM threads, stacks, heap and CPU usage, and so on, in real-time, while introducing minimal overhead.

The JVMD Engine runs as an Enterprise JavaBeans (EJB) technology on a WebLogic Server. The JVMD Agent is deployed on the targeted JVM (the one running a production WebLogic Server). It collects real-time data and transmits it to the JVM Diagnostics Engine. This data is stored in the Management Repository, and the collected information is displayed on the Enterprise Manager Cloud Control console for monitoring purposes. The communication between JVMD Engine and JVMD Agent can be secure (SSL), or non-secure.

14.2 Before you Begin

Before installing JVMD Engine or JVMD Agent, review the points outlined in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

14.3 Prerequisites

Before installing JVMD Engine or JVMD Agent, ensure that you meet the prerequisites described in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

14.4 Installation Procedure

This section describes how to deploy JVMD Engine and JVMD Agent. It consists of the following:

- [Deploying JVMD Engine](#)
- [Deploying JVMD Agents](#)

14.4.1 Deploying JVMD Engine

This section describes the methods to deploy JVMD Engine on a Managed Server. It consists of the following:

- [Deploying JVMD Engine on a Remote Host](#)
- [Deploying JVMD Engine Manually](#)
- [Deploying JVMD Engine Manually Using ApmEngineSetup.pl](#)

14.4.1.1 Deploying JVMD Engine on a Remote Host

To deploy JVMD Engine on a remote host (that is, any host on which Oracle Management Service is not installed), follow these steps:

1. [Meet the Prerequisites](#).
2. [Deploy JVMD Engine on the Remote Host](#).

14.4.1.1.1 Meet the Prerequisites

Note: This section will use the following convention:

- `host-a` is the host where the OMS is running.
 - `host-b` is the remote host that does not have an OMS running.
-

1. Install a Management Agent on `host-b` (the remote host), and point it to the OMS running on a Managed Server present in the Enterprise Manager Cloud Control domain (`EMGC_DOMAIN`).

For information about installing a Management Agent, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

2. Install WebLogic Server on `host-b` using the Enterprise Manager Software Only installation option.

To install JVMD Engine on a remote host successfully, the remote WebLogic Server version and patch level should match with the Managed Servers present in the Enterprise Manager Cloud Control domain (`EMGC_DOMAIN`). To ensure that the

versions and patch levels match, Oracle recommends that you install WebLogic Server by selecting the Software Only install option in the Enterprise Manager OUI install.

For information about performing a software only install, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

These WebLogic Server bits must be registered with the Enterprise Manager domain running on `host-a`, so that all the Managed Servers appear under the same WebLogic domain.

3. Configure a new Managed Server using the WebLogic Server Administration Console as follows:
 - a. Log into the Enterprise Manager WebLogic Domain console (EMGC_DOMAIN) of `host-a`.

The WebLogic Server Administration Console home page appears.
 - b. In Weblogic Server Administration Console, from the Domain Structure section, select Environment and then click **Servers**.
 - c. On the Create a New Server page, enter **Server Name**, **Server Listen Address**, and **Server Listen Port**.

Note: Ensure that the Server Listen Address corresponds to the listen address of the remote host, and the Server Listen port is free on the remote host.

4. Configure a new machine using the WebLogic Server Administration Console as follows:
 - a. Log into the Enterprise Manager WebLogic Domain console (EMGC_DOMAIN) of `host-a`.

The WebLogic Server Administration Console home page appears.
 - b. In Weblogic Server Administration Console, from the Domain Structure section, select **Environment** and click **Machines**.
 - c. On the Create a New Machine page, to associate this machine with the node manager running on `host-b`, enter the **Listen Address** of the remote host, and the node manager port number which is 5556 by default.

This node manager primarily controls the starting and stopping of a remote host.
 - d. Click **Finish** to create the machine.
5. Select the newly created machine, then click on **Servers** to add the Managed Server you created to this machine. This step associates the machine with the nodemanager running on `host-b`.
6. To extend the WebLogic Domain, a template of the Enterprise Manager Cloud Control domain running on `host-a` is created using the following command:

```
./pack.sh -domain = $DOMAIN_HOME -template = <absolute_path_to_the_new_
weblogic_template> - template_name="My WebLogic Domain" -managed={true}
```

Where:

`$DOMAIN_HOME` is the location of EMGC domain on `host-a`.

`<absolute_path_to_the_new_weblogic_template>` is the location where you want to create the template.

7. Copy `emgcdomain.jar` from host-a (where the OMS is running) to host-b (remote host).

8. Run the following command to unpack `emgcdomain.jar` template on host-b:

```
./unpack.sh -domain = $DOMAIN_HOME -template= <absolute_path_to_domain_
template_created>
```

Where:

`$DOMAIN_HOME` is the domain location of EMGC on host-b (remote host)

`<absolute_path_to_domain_template_created>` is the location of the template on host-b where `emgcdomain.jar` template is present.

9. To enroll the WebLogic Domain with node manager, perform the following steps on host-b:

- a. Run the following command to update the node manager properties file so that it can start monitoring the remote host:

```
$WEBLOGIC_HOME/common/bin/wlst.sh
nmEnroll($DOMAIN_HOME)
```

- b. Start the Node Manager as follows:

```
<$WEBLOGIC_HOME>server/bin/startNodeManager.sh
```

Note: Ensure that you set the property in the nodemanager property file before starting the Node Manager. You can set the property in one of the following methods:

- Manually edit the `nodemanager.properties` file to set the property `startScriptEnabled=true`.
 - Run the script `setNMProps.sh` as follows: `$MIDDLEWARE_HOME/oracle_common/common/bin/setNMProps.sh`
-

- c. Perform the following steps to modify `startWebLogic.sh`:

- a. Navigate to the following location:

```
- On Unix      : $DOMAIN_HOME/bin/startWebLogic.sh
- On Windows : $DOMAIN_HOME/bin/startWebLogic.cmd
```

- b. Set maximum heap size (`-Xmx`) to 1 GB for 64 bit systems, and maximum permanent generation (`-XX:MaxPermSize`) to 768M for 64-bit systems, as follows:

```
USER_MEM_ARGS="-Xms256m -Xmx1024m -XX:MaxPermSize=768m"
```

Note: If the remote Managed Server is started using a Sun JVM, then you must add following memory options to `USER_MEM_ARGS`: `XX:+UnlockDiagnosticVMOptions` and `XX:+UnsyncloadClass`.

- c. Set maximum heap size to 1 GB for 32-bit systems, and maximum permanent generation to 512M for 32-bit systems, as follows:

```
USER_MEM_ARGS="-Xms256m -Xmx1024m -XX:MaxPermSize=512m"
```

10. Perform the following steps on host-a, then start the newly created Managed Server as follows:
 - a. Copy the `emreposauthbean.jar` located in `$OMS_HOME/sysman/jlib`, to `<middleware_home>/wlserver_10.3/server/lib/mbeantypes`. Where, `$OMS_HOME` is the location of the OMS server on host-a, and `<middleware_home>` is on host-b.
 - b. Copy the `emCoreCommon.jar` from `$WEBLOGIC_HOME/sysman/jlib` on host-a to `$WEBLOGIC_HOME/server/lib` on host-b.
 - c. Import SSL Certificate to Enterprise Manager Agent Trust store present on the host where Managed Server is running.
 - d. Start the Managed Server from the WebLogic Server Administration Console to complete the WebLogic Server setup.
11. Perform the following steps to discover the new Managed Server running on host-b:
 - a. In Cloud Control, from the **Targets** menu, select **Middleware**.
On the Middleware page, from the list of WebLogic servers running, select the WebLogic domain where the new Managed Server is deployed (that is, `EMGC_DOMAIN`).
 - b. On the Cloud Control Domain page, from the **WebLogic Domain** menu, select **Refresh WebLogic Domain**.
The new Managed Server now gets registered in the Enterprise Manager Cloud Control domain.
12. Restart the Managed Server for all the changes to take effect.

14.4.1.1.2 Deploy JVMD Engine on the Remote Host

To deploy JVMD Engine on a remote host (that is, a host that does not have Oracle Management Service installed), follow these steps:

1. From the **Setup** menu, select **Middleware Management**, then select **Application Performance Management**.
2. On the Application Performance Management page, from the **Add** menu, select **JVM Diagnostics Engine**.
3. On the Deploy JVM Diagnostics Engine page, select **Deploy on an existing managed server**.
For **Managed server**, select the Managed Server running on the remote host on which you want to deploy JVMD Engine. The drop-down list displays all the Managed Servers present in the Enterprise Manager WebLogic domain.
4. Specify values for **Oracle WebLogic Administration Server Host Credentials**, **Oracle WebLogic Server Domain Credentials**, and **Oracle WebLogic Managed Server Host Credentials**.

Oracle WebLogic Administration Server Host Credentials are the host credentials for the host on which the WebLogic Administration Server (for the Enterprise Manager WebLogic domain) is deployed. Oracle WebLogic Domain Credentials are the credentials for the Administration Server of the Enterprise Manager WebLogic domain. Oracle WebLogic Managed Server Host Credentials are the host credentials for the host on which the WebLogic Managed Server is deployed (that is, the host credentials for the remote host).

5. Click **Deploy** to submit a deployment job to the Enterprise Manager job system.

Note: When you click **Deploy**, you may receive a warning mentioning that the WebLogic domain is already in edit mode, and mentioning the number of unsaved changes and non active changes. If there are no unsaved or non active changes, or if you are sure that the changes will not affect the JVM Engine deployment, ignore this warning and proceed.

The JVM Engine Deployment Status page appears with a link to the job status. Click the link to view the status of the job that you submitted.

14.4.1.2 Deploying JVM Engine Manually

To deploy JVM Engine manually, follow these steps:

1. [Download jvmd.zip](#)
2. [Deploy JVM Engine](#)

14.4.1.2.1 Download jvmd.zip

Before deploying JVM Engine, ensure that you have downloaded `jvmd.zip`. To do so, in Enterprise Manager 12c, navigate to the following default location:

```
<MIDDLEWARE_HOME>/plugins/oracle.sysman.emas.oms.plugin_
12.1.0.4.0/archives/jvmd.zip
```

You can download this file onto your local machine, and then run the following command to extract the contents of the zip file:

```
unzip jvmd.zip
```

The following is the output of this command:

```
Archive:  jvmd.zip
  inflating: jamagent.war
  inflating: jammanager.ear
  inflating: jammanager_dummy.ear
  extracting: loadheap.zip
  inflating: DeployJVMDEngine.cmd
  inflating: DeployJVMDEngine.py
  inflating: DeployJVMDEngine.sh
  creating: customprov/
  inflating: customprov/DeployJVMDAgent.cmd
  inflating: customprov/DeployJVMDAgent.py
  inflating: customprov/DeployJVMDAgent.sh
  inflating: customprov/deploy_jvmdagent.pl
  inflating: customprov/README.txt
  inflating: customprov/sample_jvmdagent_deploy.properties
  creating: upgrade/
  inflating: upgrade/jvmd_monitoringupgrade11_12.sql
  inflating: upgrade/jvmd_targetupgrade11_12.sql
  inflating: upgrade/jvmd_traceupgrade11_12.sql
  inflating: upgrade/README.txt
```

The `jvmd.zip` file contains the following:

- `DeployJVMDEngine.cmd`: This script enables you to deploy JVM Engine on a Windows host.

- `DeployJVMDEngine.sh`: This script enables you to deploy JVMD Engine on a Linux host.
- `DeployJVMDEngine.py`: This script is invoked by the `DeployJVMDEngine.cmd` and `DeployJVMDEngine.sh` scripts to deploy JVMD Engine.
- `jamagent.war`: JVMD Agent.
- `jammanager_dummy.ear`: A dummy JVMD Engine is deployed by the deployment scripts on the OMS. This JVMD Engine is deleted when JVMD Engine deployment is complete.
- `jammanager.ear`: JVMD Engine.
- `loadheap.zip`: This zip file contains the process log for each platform, and the scripts for loading the heap.
- `customprov` directory: The `customprov` directory contains the scripts used to deploy JVMD Agent from the command line, and is suitable for mass deployment.
- `upgrade` directory: The `upgrade` directory contains scripts for upgrade.

14.4.1.2.2 Deploy JVMD Engine

To deploy JVMD Engine from the command line, follow these steps:

1. Navigate to the following location, then transfer the `jvmd.zip` file here:
`<MIDDLEWARE_HOME>/oms/jvmd`
2. Run the following command to extract the scripts from the `jvmd.zip` file:
`unzip jvmd.zip`
3. Select the SSL port or the Non-SSL ports to be assigned to the Managed Server that will be created on the host where you want to deploy JVMD Engine.

Note: To verify if the required ports are free, run the following command:

```
netstat -a|grep <port_number>
```

4. Run the following script from the command line to deploy JVMD Engine:

On Linux:

```
./DeployJVMDEngine.sh
```

On Windows:

```
DeployJVMDEngine.cmd
```

The script updates the default values for many of the parameters. If you want to change any of the parameter values, you can provide them when prompted. If not, press **Enter** to select the default values.

Note: A temporary file `jammanager_dummy.ear` is deployed on the OMS so that JVMD Engine can access the repository. This file is deleted once the deployment is complete.

Once the deployment is successful, you will see the status as follows:

Current Status of your Deployment:

```
Deployment command type : deploy
Deployment State       : completed
Deployment Message     : no message
```

5. Once a connection to the repository is established, a server is created in the Enterprise Manager Cloud Control WebLogic domain on which JVMMD Engine is deployed. By default, this server is called `EMGC_JVMDMANAGER1`. The displayed output is as follows:

```
Starting server EMGC_JVMDMANAGER1
Server with name EMGC_JVMDMANAGER1 started successfully
```

6. Refresh the Enterprise Manager Cloud Control domain.

To do this, log in to the Enterprise Manager console. Navigate to the Enterprise Manager Cloud Control domain home page. From the **Farm** menu, select **Refresh WebLogic Domain**.

14.4.1.3 Deploying JVMMD Engine Manually Using `ApmEngineSetup.pl`

You can deploy JVMMD Engine manually, using the `ApmEngineSetup.pl` script. You can run this script in the following ways:

- In interactive mode, where you are prompted for input details in an interactive manner
- In silent mode, where you specify all the input details using a properties file

Important: You can use the `ApmEngineSetup.pl` script to deploy JVMMD Engine only on a host that is running the OMS, and not on a remote host.

To deploy JVMMD Engine manually using the `ApmEngineSetup.pl` script, follow these steps:

1. Navigate to the following location on the OMS host:

```
$<MIDDLEWARE_HOME>/plugins/oracle.sysman.emas.oms.plugin_
12.1.0.4.0/archives/jvmd/deployment_Scripts/engine/
```

2. View the `README.txt` file, for information on using the `ApmEngineSetup.pl` script.
3. Run the `ApmEngineSetup.pl` script.

If you want to run the `ApmEngineSetup.pl` script in interactive mode, such that you are prompted for the input details, use the following command:

```
perl ApmEngineSetup.pl
```

Ensure that you specify the operation as `deploy`, and the Engine Type as `JVMD`.

If you want to run the `ApmEngineSetup.pl` script in silent mode, specify all the input details in a properties file, then use the following command:

```
perl ApmEngineSetup.pl -silent -file <properties_file_name> -password
<password>
```

`<properties_file_name>` is the name of the properties file where the JVMMD Engine and operation details are provided. `<password>` is the WebLogic console password.

To learn how to specify the input details in a properties file, view the sample properties file `SAMPLE_engine.properties`.

14.4.2 Deploying JVMD Agents

This section contains the following:

- [Deploying JVMD Agents Manually](#)
- [Deploying JVMD Agents Manually Using `deploy_jvmdagent.pl`](#)
- [Deploying JVMD Agents for High Availability](#)
- [Deploying JVMD Database Agent](#)
- [Connecting JVMD Agent to the JVMD Engine Secure Port](#)

14.4.2.1 Deploying JVMD Agents Manually

To deploy JVMD Agents manually, follow these steps:

1. [Download `javadiagnosticagent.ear` or `jamagent.war`.](#)
2. [Deploy JVMD Agent.](#)

14.4.2.1.1 Download `javadiagnosticagent.ear` or `jamagent.war`

Note: Oracle recommends that you use `javadiagnosticagent.ear` to deploy a JVMD Agent on Oracle WebLogic Server. To deploy a JVMD Agent on an application server other than Oracle WebLogic Server, use `jamagent.war`.

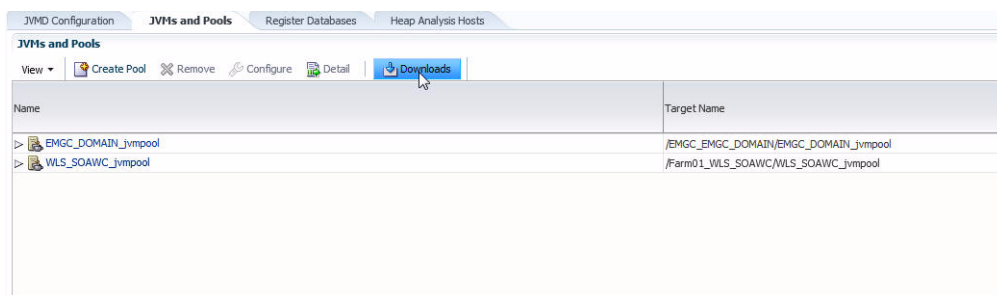
This section describes how to download the `javadiagnosticagent.ear` or `jamagent.war` file. It consists of the following:

- [Downloading `javadiagnosticagent.ear` or `jamagent.war` Using Cloud Control](#)
- [Downloading `jamagent.war` Using `javadiagnosticagent.ear`](#)

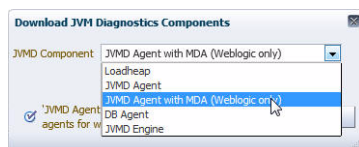
Downloading `javadiagnosticagent.ear` or `jamagent.war` Using Cloud Control

To download `javadiagnosticagent.ear` or `jamagent.war` using Cloud Control, follow these steps:

1. In Cloud Control, from the **Setup** menu, select **Middleware Management**, then select **Application Performance Management**.
2. On the Application Performance Management page, select **JVM Diagnostics Engine**.
3. Click **Configure**. The JVM Diagnostics Setup page appears.
4. On the JVM Diagnostics Setup page, click **JVMs and Pools**, then click **Download**. The Download JVM Diagnostics Component dialog box appears.



5. From the **JVMD Component** menu, to download `javadiagnosticagent.ear`, select **JVMD Agent with MDA (Weblogic only)**, then click **OK**. To download `jamagent.war`, from the **JVMD Component** menu, select **JVMD Agent**, then click **OK**. The JVM Diagnostics Agent `web.xml` parameters dialog box appears.

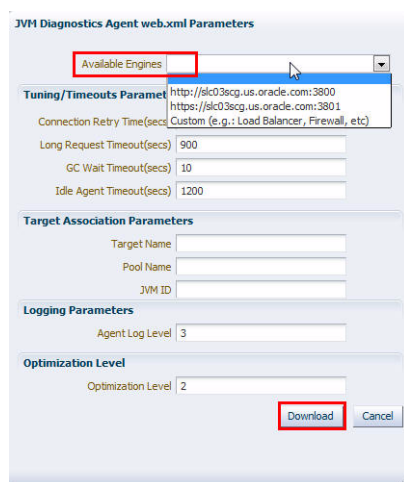


6. From the **Available Engines** menu, select an option from the list, then click **Download**:
 - Select the HTTP URL if you want the JVMD Agent to connect to the JVMD Engine using a non-secure connection.
 - Select the HTTPS URL if you want the JVMD Agent to connect to the JVMD Engine using a secure connection.
 - Select **Custom** if you want the JVMD Agent to connect to a JVMD Engine through a load balancer. Specify the host name and the port that the JVMD Agent must connect to.

For example:

HTTP: `http://slc01.us.example.com:3800`

HTTPS: `https://slc01.us.example.com:3801` (secure communication)



7. Click **Download** to download `javadiagnosticagent.ear` or `jamagent.war`.

Downloading jamagent.war Using javadiagnosticagent.ear

To download jamagent.war using javadiagnosticagent.ear, follow these steps:

1. Download the javadiagnosticagent.ear file to the following location:
`<middleware_home>/oms/jvmd`
The javadiagnosticagent.ear file can be downloaded from the following location:
`<MIDDLEWARE_HOME>/plugins/oracle.sysman.emas.oms.plugin_12.1.0.4.0/archives/javadiagnosticagent.ear`
2. Run the following command to extract the JVMD Agent script present in javadiagnosticagent.ear:
`jar -xvf javadiagnosticagent.ear`
3. Navigate to WEB-INF/web.xml.
4. Edit the web.xml file to update the values of the jamconshost and jamconspport parameters, where jamconshost is the IP of the host on which JVMD Engine is deployed, and jamconspport is the port of the same host.

Note: To enable secure communication for the selected JVMD Engine, make the following change to the web.xml file:

```
jamsecureCommunication = 1
```

For example:

```
<init-param>
  <param-name>jamconshost</param-name>
  <param-value>slc01axn</param-value>
  <description>Jam console host - demolnx.auptyma.com</description>
</init-param>
<init-param>
  <param-name>jamconspport</param-name>
  <param-value>3800</param-value>
  <description>Jam console port</description>
</init-param>
```

Note: Once JVMD Engine is deployed, the IP and the port appear on the JVMD Deployment page as: <Machine Name:Port Number>

5. Run the following command to reassemble the jamagent.war file:

```
jar -cMvf jamagent.war META-INF WEB-INF jamagent oracle
```

The updated jamagent.war file is now ready for deployment.

14.4.2.1.2 Deploy JVMD Agent

This section describes how to deploy JVMD Agent on various application servers. It consists of the following:

- [Deploying JVMD Agent on WebLogic Server](#)
- [Deploying JVMD Agent on Glassfish](#)
- [Deploying JVMD Agent on JBoss](#)

- [Deploying JVMD Agent on Tomcat](#)
- [Deploying JVMD Agent on Websphere](#)
- [Deploying JVMD Agent on OC4J](#)

Deploying JVMD Agent on WebLogic Server

To deploy JVMD Agent on a Weblogic Managed Server manually, follow these steps:

1. Make a copy of the deployment profile `sample_jvmdagent_deploy.properties` available in the `jvmd.zip` file. Update the location of the `javadiagnosticagent.ear` file, the name of the WebLogic domain, and the server information. Save the profile as `jvmdagent_deploy.properties`.

For more information about the parameters, view the `README.txt` file present in the `customprov` folder of the `jvmd.zip` file.

2. Run the following perl script available in the `customprov` folder of the `jvmd.zip` file to deploy JVMD Agent on all the specified servers.

```
perl deploy_jvmdagent.pl
```

Note: Ensure that the deployment profile `jvmdagent_deploy.properties` and the perl scripts are available in the same folder.

Deploying JVMD Agent on Glassfish

To deploy JVMD Agent on Glassfish manually, follow these steps:

1. Log in to the Glassfish Administration console.
2. In the Common Tasks section, click **Applications**.
3. In the Deployed Applications section, click **Deploy**.
4. For **Location**, select **Packaged File to Be Uploaded to the Server**, then specify the location on your local host where `jamagent.war` is present.
5. For **Selected Targets**, add the server on which you want to deploy `jamagent.war`.
6. Click **OK**.

Deploying JVMD Agent on JBoss

To deploy JVMD Agent on JBoss manually, follow these steps:

1. Log in to the JBoss Administration console.
2. Under **Applications**, click **Web Application (WAR)s**.
3. Click **Add a new resource**.
4. Enter the absolute path to `jamagent.war` present on your local host.
5. For both **Deploy Exploded** and **Deploy Farmed**, select **No**.
6. Click **Continue**.

To deploy JVMD Agent on JBoss manually, you can also do the following:

1. Transfer `jamagent.war` to the following location:

```
<JBOSS_HOME>/server/all/deploy
```

2. Restart the application server.

Deploying JVMD Agent on Tomcat

To deploy JVMD Agent on Tomcat manually, follow these steps:

1. Transfer `jamagent.war` to the following location:
`$CATALINA_BASE/webapps`
2. Restart the application server.

For the latest versions of Tomcat, if the `autoDeploy` flag is set to `true` in `$CATALINA_BASE/conf/server.xml`, you do not need to restart the application server. Tomcat will pick up `jamagent.war` at runtime.

Deploying JVMD Agent on Websphere

To deploy JVMD Agent on Websphere manually, follow these steps:

1. Log in to the Websphere Administration console.
2. Expand **Applications**, then click **New Application**.
3. Click **New Enterprise Application**.
4. For **Path to the new application**, select **Local file system**, then specify the location on your local host where `jamagent.war` is present.
5. Provide the context root for `jamagent.war`.
6. Save the configuration.
7. Start the application.

Deploying JVMD Agent on OC4J

To deploy JVMD Agent on OC4J manually, follow these steps:

1. Log in to the OC4J Administration console.
2. Click **Applications**.
3. Click **Deploy**.
4. Select **Archive is present on local host**. For **Archive Location**, specify the location on your local host where `jamagent.war` is present. Click **Next**.
5. For **Application Name**, enter `jamagent`. For **Context Root**, enter `/jamagent`.
6. Click **Deploy**.

Deploying JVMD Agent on a Standalone JVM

A JVMD Agent can be deployed on a standalone JVM such that the inputs are read from `web.xml`, or such that you specify the inputs on the command line.

To deploy a JVMD Agent on a standalone JVM such that all the inputs are read from `web.xml`, run the following command from the command line:

```
java -cp <absolute_path_to_jamagent.war> jamagent.jamrun <java_class_with_a_main_method>
```

To deploy a JVMD Agent on a standalone JVM by specifying all the inputs on the command line, run the following command from the command; line:

```
java -cp <absolute_path_to_jamagent.war> jamagent.jamrun <java_class_with_a_main_method> jamconshost=<jvmd_engine_host> jamconsport=<jvmd_engine_
```

```
listen_port> jamjvmid=<unique_jvmd_identifier> jamtimeout=<timeout_period_
in_seconds> jamloglevel=<jvmd_agent_log_level>
```

Note: When `jamagent.war` is run using an IBM Java Development Kit (JDK), you may see the following warning in the logs:

```
*****can_tag_objects capability is not set.Copy library
libjamcapability to another directory and restart Java with
argument "-agentpath:<absolute_path_to_libjamcapability.so>" *****
```

To troubleshoot this warning, include the `libjamcapability.so` library and restart the IBM JVM:

```
/scratch/IBM/WebSphere/AppServer/java/bin/java
-agentpath:/scratch/libjamcapability.so -cp
/scratch/jamagent.war jamagent.jamrun MyFirstProgram
```

14.4.2.2 Deploying JVMD Agents Manually Using `deploy_jvmdagent.pl`

You can deploy JVMD Agents manually, using the `deploy_jvmdagent.pl` script. You can run this script only in silent mode, that is, you must specify all the input details using a properties file.

To deploy JVMD Agents manually using `deploy_jvmdagent.pl`, follow these steps:

1. Navigate to the following location on the OMS host:

```
$<MIDDLEWARE_HOME>/plugins/oracle.sysman.emas.oms.plugin_
12.1.0.4.0/archives/jvmd/deployment_Scripts/agent/jvmd/
```

2. View the `README.txt` file, for information on using the `deploy_jvmdagent.pl` script.
3. Specify all the inputs in a properties file, then use the following command:

```
perl deploy_jvmdagent.pl <properties_file_name>
```

If you do not pass the name of the properties file as a parameter while running `deploy_jvmdagent.pl`, `deploy_jvmdagent.pl` looks for a properties file named `jvmdagent_deploy.properties` in the same folder. To learn how to specify the input details in a properties file, view the sample properties file `sample_jvmdagent_deploy.properties`.

14.4.2.3 Deploying JVMD Agents for High Availability

If you have multiple JVMD Engines deployed in your setup, and have configured a load balancer for them, you can deploy JVMD Agents such that they connect to the load balancer, and not to any of the individual JVMD Engines. This increases the availability of the JVMD Agents, and creates a failover mechanism, that is, even if a particular JVMD Engine goes down, the JVMD Agents remain active.

You can deploy a JVMD Agent for high availability using the following methods:

- [Deploying JVMD Agents for High Availability Using the Application Performance Management Page](#)
- [Deploying JVMD Agents for High Availability Manually](#)

14.4.2.3.1 Deploying JVMD Agents for High Availability Using the Application Performance Management Page

To deploy JVMD Agents for high availability using the Application Performance Management page, follow these steps:

1. Follow the steps mentioned in *Oracle Enterprise Manager Cloud Control Basic Installation Guide* to deploy a JVMD Agent.
2. On the JVMD Agents Configurations page, for **Available JVMD Engines**, select **Other**. Provide the load balancer host name and port.

Click **Next**.

3. On the Review page, review all the information, then click **Deploy**.

Note: By default, the JVMD Agent connects to the load balancer using HTTP. If you want the JVMD Agent to connect to the load balancer using HTTPS, you must deploy the JVMD Agent manually, as described in [Section 14.4.2.3.2](#).

14.4.2.3.2 Deploying JVMD Agents for High Availability Manually

To deploy JVMD Agents for high availability manually, follow these steps:

1. Follow the steps mentioned in [Downloading javadiagnosticagent.ear or jamagent.war Using Cloud Control](#) to download `javadiagnosticagent.ear` or `jamagent.war`.
2. When the JVM Diagnostics Agent `web.xml` parameters dialog box is displayed, from the **Available Engines** menu, select **Custom**. Provide the load balancer host name and port.

Click **Download**.

3. Deploy the JVMD Agent as mentioned in [Section 14.4.2.1.2](#).

Note: By default, the JVMD Agent connects to the load balancer using HTTP. If you want the JVMD Agent to connect to the load balancer using HTTPS, you must use a certificate, as described in [Section 14.4.2.5](#). Ensure that the common name of the certificate you use matches the host name of the load balancer.

14.4.2.4 Deploying JVMD Database Agent

To deploy JVMD Database Agent, download JVMD Agent from Cloud Control, as it can serve as a JVMD Database Agent too. If JVMD Agent is downloaded and deployed on the same host as Oracle Database, then you do not require a separate JVMD Database Agent. JVMD Agent itself orchestrates between the database and JVMD Engine. However, if JVMD Agent and the database are on separate hosts, then you need a JVMD Database Agent to collect the database specific information, and transmit the collected data to JVMD Engine.

Note: JVMD Database Agents are supported on the platforms on which JVMD Agents are supported, except for Microsoft Windows. JVMD Database Agent needs Java 1.4.X or higher to run.

To download and deploy JVMD Database Agent, do the following:

1. Follow the steps listed in [Downloading javadiagnosticagent.ear or jamagent.war Using Cloud Control](#) to download the jamagent.war file using Cloud Control.
2. To start the JVMD Database Agent, run the following command:

```
$JAVA_HOME/bin/java -Xms126M -Xmx512M -cp ./jamagent.war jamagent.Dbagent
jamconshost=<Host on which engine is running> jamconspport=<Port of the server
on which JVMD Engine is installed>
```

```
For Example: /usr/local/packages/jdk14/bin/java -Xms126M -Xmx512M -cp
./jamagent.war jamagent.Dbagent jamconshost=adc2190661.us.example.com
jamconspport=3900
```

Note: If you encounter the error message `TIMEOUT` from console `JAM Agent: Error receiving data from console`, then restart the JVMD Database Agent with the option `jamconsretr = 5`.

14.4.2.5 Connecting JVMD Agent to the JVMD Engine Secure Port

To ensure secure communication with JVMD Engine, the JVM should have access to a KeyStore in which the certificate of the Managed Server on which JVMD Engine is deployed is added. The KeyStore of the Enterprise Manager Cloud Control domain in which the JVMD Engine Managed Server is created can be used for the same.

If you have access to the Enterprise Manager Cloud Control domain, then do the following to connect JVMD Agent to the JVMD Engine secure port:

1. Locate the KeyStore. It is normally available in the following location:

```
<WEBLOGIC_HOME>/server/lib/DemoTrust.jks
```

Where `WEBLOGIC_HOME` refers to the installation directory of WebLogic Server.

2. Add the following to the command line, and start JVMD Agent:

```
-Djavax.net.debug=ssl -Djavax.net.ssl.trustStore=<location of
DemoTrust.jks of the engine server>
-Djavax.net.ssl.trustStorePassword=DemoTrustKeyStorePassPhrase
```

Note: The default password for the WebLogic KeyStore is `DemoTrustKeyStorePassPhrase`.

If you do not have access to the Enterprise Manager Cloud Control domain, then do the following to connect JVMD Agent to the JVMD Engine secure port:

1. If the target server already has a KeyStore, for example `DemoTrust.jks`, then use `DemoTrust.jks`. Otherwise, you need to create a new KeyStore, for example `Keystore.jks`. To create a new KeyStore, see Step 3.
2. Follow these steps to download the certificate of the Managed Server:
 - a. Access the following URL using a browser:


```
https://<jamconshost>:<jamconspport (secure)>
```
 - b. On the home page of JVMD Agent, select the **Details** Tab, then click **Export**.
 - c. Save the certificate as `myCert.crt`.
3. To add a certificate to an existing KeyStore `DemoTrust.jks`, or to create a new KeyStore `keystore.jks`, and add a certificate to it, run the following command:

```
keytool -import -trustcacerts -alias root -file myCert.crt -keystore  
<keystore/DemoTrust>.jks
```

This command creates a new KeyStore with the default password changeit.

Note: When a WebLogic Managed Server running on a Sun or JRockit Java Virtual Machine (JVM) attempts to connect to an external resource using HTTPS, you may encounter the following exception:

```
java.lang.ClassCastException:  
weblogic.net.http.SOAPHttpsURLConnection
```

This exception occurs because a HTTP API attempts to use an underlying WebLogic implementation, instead of using the Sun implementation. To avoid this exception, using the runtime argument, set the following flag:

```
-DUseSunHttpHandler=true
```

14.5 After You Install

After installing JVMD Engine or JVMD Agent, follow the steps outlined in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

Integrating BI Publisher with Enterprise Manager

Oracle Business Intelligence (BI) Publisher is Oracle's primary reporting tool for authoring, managing, and delivering all your highly formatted documents. BI Publisher ships standard with Enterprise Manager Cloud Control 12c.

IMPORTANT: Only BI EE 11.1.1.6.0, which contains BI Publisher 11.1.1.6.0, is supported for use with Enterprise Manager 12c Cloud Control Release 3 (12.1.0.3.0).

WARNING: Do NOT attempt to install BI EE 11.1.1.6.0 onto Enterprise Manager 12c Cloud Control Release 1 (12.1.0.1.0)

This chapter covers the following topics:

- [Overview](#)
- [BI Publisher Installation and Integration with Enterprise Manager 12c](#)
- [Verifying Integration of BI Publisher with Enterprise Manager](#)
- [Allowing Access to BI Publisher for Enterprise Manager Administrators](#)
- [Limiting access to BI Publisher features](#)
- [Allowing Access to BI Publisher for Enterprise Manager Administrators in an underlying LDAP Authentication security model environment](#)
- [Securing BI Publisher with a Secure Socket Layer \(SSL\) Certificate](#)
- [BI Publisher Administration](#)
- [Post-Upgrade Steps to take after upgrading to BI Publisher to 11.1.1.6.0](#)
- [EMBIP* Roles: Granting Access to Folders and Catalog Objects](#)
- [Access to Enterprise Manager Repository](#)
- [Troubleshooting](#)
- [Managing Enterprise Manager - BI Publisher Connection Credentials](#)
- [Managing the BI Publisher Server](#)
- [Configuring BI Publisher behind a Load-Balancer](#)

15.1 Overview

In order to integrate BI Publisher with Enterprise Manager 12c, BI Publisher is installed separately, but shares the same Middleware home, as Enterprise Manager. This installation is performed using the standard Business Intelligence Enterprise Edition 11.1.1.6.0 installation that is specific to the platform on which Enterprise Manager is installed. BI Publisher is then integrated into the same WebLogic Server domain as Enterprise Manager using the *configureBIP* script. Once configured, you will be able to take advantage of the standard features BI Publisher offers, such as:

- Highly formatted, professional quality, reports, with pagination and headers/footers.
- PDF, Excel, Powerpoint, Word, and HTML report formats.
- Develop your own custom reports against the Enterprise Manager repository (read-only repository access).
- Integration with Enterprise Manager Security.
- Grant varying levels of BI Publisher functionality to different Enterprise Manager administrators.
- Use BI Publisher's scheduling capabilities and delivery mechanisms such as e-mail and FTP.

Note: The Information Publisher (IP) reporting framework, though still supported in Enterprise Manager 12c Cloud Control, was deprecated as of Enterprise Manager 12c release 12.1.0.1. No further report development will occur using the IP framework.

15.1.1 Limitations

The following are limitations apply to the use of reports and data sources.

- Out-of-box reports cannot be edited.
- If Out-of-box reports are copied, there is no guarantee that the copies will work with future product releases.

15.1.2 Downloading Oracle BI Publisher

Only Oracle Business Intelligence (BI) Publisher version 11.1.1.6.0 can be used with Enterprise Manager 12c Cloud Control Release 3 (12.1.0.3). Versions of Business Intelligence Publisher older than 11.1.1.6.0 are not compatible with Enterprise Manager Cloud Control Release 3 (12.1.0.3). You can download Oracle Business Intelligence Publisher version 11.1.1.6.0 directly from the Enterprise Manager Cloud Control download Web site.

<http://www.oracle.com/technetwork/oem/grid-control/downloads/index.html>

See the link titled *Oracle Business Intelligence Publisher 11.1.1.6.0*.

Determining BI Publisher Platform Support

To determine whether your software platform is supported by BI Publisher, refer to *Chapter 2: System Requirements and Certification* of the Oracle® Fusion Middleware Quick Installation Guide for Oracle Business Intelligence 11g Release 1 (11.1.1) for BI EE system requirements.

For system requirements and certification information, refer to the Oracle Business Intelligence chapter in the Oracle Fusion Middleware Release Notes for your platform. The documents are available on Oracle Technology Network (OTN) at the following location:

<http://www.oracle.com/technetwork/indexes/documentation/index.html>

15.2 BI Publisher Installation and Integration with Enterprise Manager 12c

The following procedures assume that you are familiar with both BI Publisher and Enterprise Manager. Refer to the *Oracle Enterprise Manager Basic Installation Guide* and the *Oracle Enterprise Manager Advanced Installation and Configuration Guide* for detailed information about Enterprise Manager.

15.2.1 Enterprise Manager and BI Publisher Inventory

Both Enterprise Manager and BI Publisher must be installed with a centralized inventory file. This means that `/etc/oraInst.loc` (or the Windows registry) points to the same directory for both installs. Although it is possible to install both products with an inventory file specific to each product, this configuration is not supported and will not allow complete integration between Enterprise Manager 12c and BI Publisher 11g.

15.2.2 Installing Enterprise Manager and Required Infrastructure

In order to support the required resources for BI Publisher, the first OMS system (where BI Publisher is initially installed) needs the following additional system requirements above and beyond what is already required by Enterprise Manager:

- +1.5 GB of RAM
- +10 GB of disk space
- Any additional OMS(s) that is added to the domain, after BI Publisher has been installed on the first OMS, will also require an additional 10 GB of disk space.

For additional resource requirements, see the following support note:

How to Determine the Number of Servers Needed to Run BI Publisher Enterprise in a Production 10g or 11g Environment? (Doc ID 948841.1)

Installing Plug-in-Specific Reports: Some Enterprise Manager-provided BI Publisher reports belong to specific plug-ins. These plug-ins must be installed in order for these reports to be available. A plug-in can be installed before or after BI Publisher is configured to work with Enterprise Manager 12c. Enterprise Manager plug-ins can be installed using different mechanisms. All of these mechanisms support the installation of BI Publisher reports that are part of a plug-in.

Note: Refer to the *Oracle Enterprise Manager Basic Installation Guide* for complete installation specifics.

15.2.2.1 Installing BI EE Using Software-only Install

Note: The BI EE Software-only Install instructions apply in the case of a new installation or in the case of an upgrade from 12.1.0.2 to 12.1.0.3 where 12.1.0.3 has been installed into a new Fusion Middleware Home.

As mentioned at the beginning of this chapter, **ONLY** Oracle Business Intelligence Enterprise Edition 11g 11.1.1.6.0 can be used to integrate with Enterprise Manager 12c Release 3 (12.1.0.3). No other product combination is compatible.

Integrating BI Publisher with Enterprise Manager requires changing the domain configuration and the Middleware home used by the Oracle Management Service. Backing up the entire Enterprise Manager Oracle Management Service installation ensures that you can recover the OMS in the event that errors occur during installation and configuration of BI Publisher.. For instructions on performing OMS backup, see the "Backing up Enterprise Manager" chapter of the Oracle® Enterprise Manager Cloud Control Administrator's Guide. Go to the section *Oracle Management Service Backup*.

Once the correct version of Business Intelligence Enterprise Edition 11g is downloaded, and the OMS backup has been performed, perform a software-only install of BI Enterprise Edition using the following steps:

1. Run the BI Enterprise Edition Publisher Installer:

Linux/UNIX: Disk1/runInstaller

Windows: Disk1/setup.exe

Note: Insure that you use the correct media or download for BI EE 11.1.1.6.0.

Note: Insure that you use the correct media or download for BI EE that is appropriate for your hardware and operating system platform.

2. (Optional) Choose E-Mail address for updates and click **Next**.
3. **VERY IMPORTANT:** Choose **Software-only Install**.
4. Click **Next**. Prerequisite checks will run.
5. After passing the prerequisite checks, click **Next**.
6. Choose the Middleware home of your Enterprise Manager installation. This is the Middleware home that you created previously.
7. BI Oracle home name must be left as the default *Oracle_BI1*. Click **Next**.
8. (Optional) Enter My Oracle Support (MOS) credentials to be notified of any security updates. Click **Next**.

When the software-only install of BI EE completes successfully, proceed to [Section 15.2.2.2](#).

15.2.2.2 Integrating BI Publisher with Enterprise Manager using the configureBIP Script

Integrating BI Publisher with Enterprise Manager requires changing the domain configuration. However, you must first back up the domain in case configuration problems occur. File permissions for the domain must be maintained when creating a backup, therefore the ZIP utility is the preferred mechanism to do so. For example:

```
cd <Instance-Home>/user_projects/domains
zip -r GCDomain.zip GCDomain
```

IMPORTANT: The *configureBIP* script must be run as the same operating system user who owns the Oracle Middleware Home.

DO NOT run *configureBIP* as the Unix Super User (root).

There are two scenarios in which you would run *configureBIP*:

For both the fresh install and upgrade scenarios, in order to install and integrate BI Publisher 11.1.1.6.0 with Enterprise Manager 12c Release 3 (12.1.0.3), it is first necessary to do a software-only install of BI Enterprise Edition 11.1.1.6.0. However, when running the *configureBIP* script, there are additional command-line arguments that are necessary in the upgrade scenario.

- Scenario 1: Fresh install of 12.1.0.3

The fresh install case is used when either of these conditions are met:

- You are installing or upgrading to Enterprise Manager 12c for the first time. did not have a previous version of Enterprise Manager 12c installed previously.
- You are upgrading to Enterprise Manager 12c Release 3 (12.1.0.3) from a previous version of Enterprise Manager 12c and you had previously installed and integrated the appropriate version of BI Publisher with Enterprise Manager

- Scenario 2: Upgrade from 12.1.0.1 or 12.1.0.2 to 12.1.0.3

Use the *configureBIP* script in upgrade mode if both of the following conditions are true:

- You have already upgraded Enterprise Manager 12c Release 1 (12.1.0.1) or Enterprise Manager 12c Release 2 (12.1.0.2) to Enterprise Manager 12c Release 3 (12.1.0.3)
- The previous installation of Enterprise Manager 12c had been integrated with the appropriate version of BI Publisher.

Regardless of whether you run the *configureBIP* script in normal mode or upgrade mode, the script requires the following credentials in order to operate:

- An Oracle account with SYSDBA privilege; normally the SYS account.
- The database password for this account.
- The WebLogic Admin Server password.
- The Node Manager password.

Make sure to gather the above credentials before proceeding.

Both the normal mode and upgrade mode of *configureBIP* are discussed in detail in the following two sections. Be sure to operate the *configureBIP* script in the appropriate mode for your installation scenario.

15.2.2.2.1 Integrating BI Publisher with Enterprise Manager using the *configureBIP* Script in Normal Mode

1. From the OMS instance's ORACLE_HOME/bin directory (of the current Enterprise Manager 12c Release 3 (12.1.0.3) installation), execute the *configureBIP* script from the command line. For example:

```
cd /oracle/EM12cR2/middleware/oms/bin
./configureBIP
```
2. The script prompts for the necessary credentials.
3. The script executes the Repository Creation Utility (RCU), since this is normal mode, to create the BI Publisher database schema.
4. The script prompts for two inputs for the port(s) to use for the BI Publisher Managed Server: One port for non-SSL (not recommended) and one port for SSL.
5. The script then performs the extend-domain operations.
6. The last step the script performs is to deploy the Enterprise Manager-supplied BI Publisher Reports to the newly installed BI Publisher Web application.

Script Input

1. Confirm that you have backed up your domain by answering the confirmation prompt with YES.
2. Enter a database user with SYSDBA privileges (typically SYS), and then enter the password (Enterprise Manager Repository database).
3. Enter the *adminserver* and then the *nodemanager* password. These accounts are part of Enterprise Manager WebLogic Domain.

Script Operation - Normal Mode (RCU):

Since you are installing BI Publisher for the first time, the schema will be created. You should see the something like the following output:

```
Checking for SYSMAN_BIPLATFORM schema...
Attempting to create SYSMAN_BIPLATFORM schema...
Processing command line ....
Repository Creation Utility - Checking Prerequisites
Checking Global Prerequisites
Repository Creation Utility - Checking Prerequisites
Checking Component Prerequisites
Repository Creation Utility - Creating Tablespaces
Validating and Creating Tablespaces
Repository Creation Utility - Create
Repository Create in progress.
Percent Complete: 0
Percent Complete: 10
Percent Complete: 30
Percent Complete: 50
Percent Complete: 50
Percent Complete: 100
Repository Creation Utility: Create - Completion Summary
Database details:
Connect Descriptor: jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_
```

```

LIST=(ADDRESS=(PROTOCOL=TCP) (HOST=host.com) (PORT=1521)) (CONNECT_DATA=(SID=orcl))
Connected As: sys
Prefix for (prefixable) Schema Owners : SYSMAN
RCU Logfile: .../middleware/oms/cfgtoollogs/bip/emBIPLATFORM.log
Component schemas created:
Component Status Logfile
Business Intelligence Platform Success
.../middleware/oms/cfgtoollogs/bip/biplatform.log
Repository Creation Utility - Create : Operation Completed

```

Extend Domain Steps

1. You will then be asked to enter BI Publisher HTTP and HTTPS (SSL) ports (either one or both). The script will identify free ports and ask if you want to take them as a default. Once entered, *Extend Domain* will then run. The ports can be in the range 9701-49152. Default port numbers are provided.
2. The Enterprise Manager-supplied BI Publisher Reports will be deployed to the newly installed BI Publisher Web application.
3. Once processing is complete, screen output similar to the following will be shown:

```

Extending domain with BI Publisher. This may take a few minutes...
BI Publisher server running at https://host.com:9701/xmlpserver.
Registering BI Publisher with Enterprise Manager and deploying reports...
Successfully setup BI Publisher with Enterprise Manager

```

15.2.2.2.2 Integrating BI Publisher with Enterprise Manager Using the *configureBIP* Script in Upgrade Mode

From the OMS instance's `ORACLE_HOME/bin` directory (of the current Enterprise Manager 12c Release 3 (12.1.0.3) installation), execute the *configureBIP* script with the *-upgrade* command-line argument. For example:

```

cd /oracle/EM12cR2/middleware/oms/bin
./configureBIP -upgrade

```

1. The script prompts for the necessary credentials.
2. The script prompts for the full directory path to the domain of the prior Enterprise Manager 12c installation. This installation already contains the BI Publisher report definitions and certain configuration data.
3. The script then executes the Patch Set Assistant (PSA) steps to upgrade the BI Publisher database schema, since this is an upgrade from a prior release of the BI Publisher.
4. The script prompts for two inputs for the port(s) to use for the BI Publisher Managed Server. One port for non-SSL (not recommended) and one for SSL.
5. The script then performs the extend-domain operations, but does not start the BI Publisher Managed Server.
6. The script migrates the reports and certain configuration data from the prior installation of BI Publisher, if needed, that was installed onto the prior release of Enterprise Manager 12c.
7. The script then starts the BI Publisher Managed Server.
8. The last step the script performs is to deploy the Enterprise Manager-supplied BI Publisher Reports to the newly installed BI Publisher Web application.

Note: During an upgrade of BI Publisher 11.1.1.6.0 onto Enterprise Manager 12c Release 3 (12.1.03), the existing BI Publisher schema will be upgraded from the prior version to 11.1.1.6.0. This means that when performing an upgrade, all existing BI Publisher schedules will be carried over to the new installation of BI Publisher.

Optional: If your BI Publisher file system-based repository is in a shared storage location from the prior install, and you also want to continue to use this shared location for the new install, then the report and configuration migration performed in step 6 above is not required. In this situation, you can run *configureBIP* using the following syntax:

```
./configureBIP -upgrade -nomigrate
```

Script Input

1. Confirm that you have backed up your domain by answering the confirmation prompt with "yes".
2. Enter a database user with SYSDBA privileges (typically 'sys'), then enter the password. (Enterprise Manager repository database).
3. Enter the *adminserver* and then the *nodemanager* password. These accounts are part of Enterprise Manager WebLogic Domain.
4. Enter the full directory path to the domain from the prior Enterprise Manger 12c installation. For example:

```
/oracle/em12cR1/middleware/gc_inst/user_projects/domains/GCDomain
```

When executing the script on a Windows operating system, use double-backslashes to separate directory entries. For example:

```
C:\EMInstall\middleware\gc_inst\user_projects\domains\GCDomain
```

5. The patch set assistant then runs to upgrade the BI Publisher schema. Output similar to the following will be generated.

```
Upgrading from a prior release of BI Publisher With a file-system repository
Located at: /oracle/em12cR1/middleware/gc_inst/user_projects/domains/GCDomain
Checking for SYSMAN_BIPLATFORM schema...
Attempting to upgrade SYSMAN_BIPLATFORM schema...
EM 12c BIPLATFORM 11.1.1.5.0 schema detected. Begin upgrade process to
11.1.1.6.0 ...
Begin to execute Oracle Fusion Middleware Patch Set Assistant (PSA) ...
PSA returns with status: 0
Successfully upgraded SYSMAN_BIPLATFORM schema...
```

Extend Domain Steps

1. You will then be asked to enter BI Publisher HTTP and HTTPS (SSL) ports (either one or both). The script will identify free ports and ask if you want to take them as a default. The ports can be in the range 9701-49152. Defaults are provided. Once entered, *Extend Domain* will run, but the BI Publisher Managed Server will not be started until step three.
2. Certain reports and configurations from the prior BI Publisher installation will be migrated (unless the "-nomigrate" option was supplied on the command-line).
3. The BI Publisher Managed Server will be started

4. The Enterprise Manager-supplied BI Publisher Reports will be deployed to the newly installed BI Publisher Web application.
5. Once processing is complete, screen output similar to the following will be generated.

```
Extending domain with BI Publisher. This may take a few minutes...
Migrating BI Publisher Filesystem repository from
"/oracle/em12cR1/middleware/gc_inst/user_projects/domains/GCDomain
/config/bipublisher/repository" to "/oracle/emNewInstall/middleware/gc_
inst/user_projects/domains/GCDomain /config/bipublisher/repository"...
Starting the Upgraded BI Publisher Managed Server...
BI Publisher server running at https://host.com:9704/xmlpserver.
Registering BI Publisher with Enterprise Manager and deploying reports...
Successfully setup BI Publisher with Enterprise Manager
```

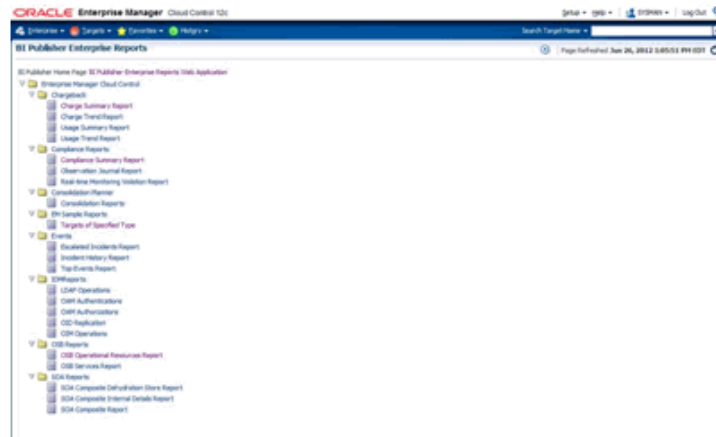
15.3 Verifying Integration of BI Publisher with Enterprise Manager

1. Log in to Enterprise Manager as a Super Administrator.
2. From the **Enterprise** menu, select **Reports** and then **BI Publisher Enterprise Reports**.

Prior to BI Publisher being integrated with Enterprise Manager, the BI Publisher Reports page appears as follows:



3. Once BI Publisher has been integrated with Enterprise Manager, you may have to click the refresh icon at the top right of the Enterprise Manager window (highlighted in the previous graphic) in order for the UI to reflect the changes.
4. Enterprise Manager displays a tree list showing all of the Enterprise Manager-supplied BI Publisher reports as shown in the following graphic



This graphic shows the list of reports after all plug-ins have been installed. The report list will vary in size depending on the number of plug-ins that have been installed.

5. Click on the provided **EM Sample Reports** and the select **Targets of Specified Type**.
6. Log in to BI Publisher using your Enterprise Manager credentials.
7. You will see the sample report rendered on the screen. You can then use the full capabilities of BI Publisher such as PDF report generation and e-mail delivery.

15.4 Allowing Access to BI Publisher for Enterprise Manager Administrators

BI Publisher shares the same security model, via WebLogic, that Enterprise Manager is configured to use. The security model is used both for authenticating access to BI Publisher, and also setting up access to different features of BI Publisher. The items to be discussed in the following sections are:

- [Enterprise Manager Authentication Security Model](#)
- [BI Publisher security model](#)
- [BI Publisher Permissions](#)
- [BI Publisher OPSS Application Roles](#)
- [Authenticating and limiting access BI Publisher features](#)

15.4.1 Enterprise Manager Authentication Security Model

Once integrated, BI Publisher reports conform to the Enterprise Manager authentication security model.

Enterprise Manager supports a variety of security models, as defined in the Oracle® Enterprise Manager Cloud Control Administrator's Guide (Configuring Security). To summarize, the security models that Enterprise Manager 12c supports are:

- Repository-Based Authentication
- Oracle Access Manager (OAM) SSO
- SSO-Based Authentication

- Enterprise User Security Based Authentication, with 2 options
- LDAP Authentication Options: Oracle Internet Directory and Microsoft Active Directory

15.4.2 BI Publisher security model

When BI Publisher is integrated with Enterprise Manager, it shares the same security model as Enterprise Manager. Security Model 1 - Repository-Based authentication, uses the Oracle database for authentication. The remaining 4 security models use an underlying LDAP server to authenticate users. For the purposes of this document, we classify the BI Publisher security model into one of these two categories:

- Repository-Based Authentication
- Underlying LDAP-based Authentication

Note: When the BI Publisher security model is configured to use *Underlying LDAP-based Authentication*, no additional BI Publisher configuration is required. For example, you do not need to access the *BI Publisher Administration* screen and change the security model to LDAP. Because Enterprise Manager and BI Publisher are configured in the same WebLogic domain, they automatically share the same security and authentication mechanisms.

The primary security attributes that apply to BI Publisher Reports are:

- [BI Publisher Permissions](#)
- [BI Publisher OPSS Application Roles](#)

Each of these security attributes is detailed in the following sections.

15.4.3 BI Publisher Permissions

Enterprise Manager ships with certain Oracle-provided BI Publisher catalog objects. These catalog objects consist of:

- Folders
- Reports (layout definitions and translations)
- Datamodels (SQL queries against the Enterprise Manager repository)
- Subtemplates (standard Enterprise Manager header shown above all pages of all report output)

These catalog objects are created when BI Publisher is installed and integrated with Enterprise Manager. They are placed in the "Enterprise Manager Cloud Control" folder. These catalog objects are created with certain permissions that, combined with the roles/groups discussed below, achieve the desired security model.

15.4.4 BI Publisher OPSS Application Roles

The domain policy store (OPSS) is used to control Enterprise Manager administrator access to objects in the BI Publisher catalog and conditional access to the BI Publisher "Administration" button.

OPSS is the repository of system and application-specific policies. Details regarding OPSS can be found in the Oracle® Fusion Middleware Application Security Guide. In

a given domain, there is one store that stores all policies (and credentials) that all applications deployed in the domain may use. As both Enterprise Manager and BI Publisher are separate applications in the same domain, it is necessary to grant specific BI Publisher OPSS application roles to Enterprise Manager administrators in order for them to access and use BI Publisher.

When BI Publisher is installed, four OPSS application roles are created. These four OPSS application roles are combined with the permissions on the BI Publisher catalog objects in the "Enterprise Manager Cloud Control Folder" to achieve the rules shown in the following sections. In addition, when the underlying LDAP authentication security model is used, the LDAP groups can be mapped to these OPSS application roles.

In the Repository-based authentication security model, the domain policy store (OPSS) is used solely to control Enterprise Manager administrator's access to BI Publisher.

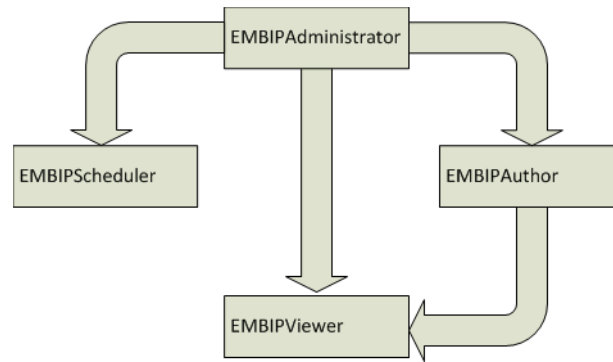
15.4.5 Authenticating and limiting access BI Publisher features

Below is a list of the OPSS application roles, and a description of the effective security model placed on BI Publisher catalog objects that ship with Enterprise Manager.

- **None** - Enterprise Manager administrators without any BI Publisher role can access BI Publisher Reports via any delivery channel that BI Publisher supports, and that has been configured and made accessible the BI Publisher System Administrator. For example, any user can receive BI Publisher Reports via the BI Publisher scheduling and e-Mail delivery mechanism, if configured.
- **EMBIPViewer** - Enterprise Manager administrators with this BI Publisher role can receive e-mails plus can view the Enterprise Manager-supplied BI Publisher reports.
- **EMBIPScheduler** - Enterprise Manager administrators with this BI Publisher role can receive e-mails and can schedule the Enterprise Manager-supplied BI Publisher reports if they also have the **EMBIPViewer** role.
- **EMBIPAuthor** - Enterprise Manager administrators with this BI Publisher role can receive e-mails, view the Enterprise Manager-supplied BI Publisher reports, and can create new reports in their private folder. They can also copy the Enterprise Manager-supplied BI Publisher reports into their private folder and customize them.
- **EMBIPAdministrator** (Super Users) - Enterprise Manager administrators with this BI Publisher role have complete access to BI Publisher.

The following diagram shows the hierarchy of the above roles:

Note: Access to the BI Publisher "Administration" button is granted via the OPSS application role. This button is used to perform advanced configuration on BI Publisher, such as setting up the e-mail server.



Enterprise Manager Super Administrators

When the repository-based authentication security model is used, all Enterprise Manager Super Administrators are automatically granted the **EMBIPAdministrator** OPSS application role to facilitate setting up BI Publisher.

When an underlying LDAP authentication security model is used, Enterprise Manager Super Administrators are not automatically granted EMBIPAdministrator access to BI Publisher. See Section 16.x for more information on allowing access to BI Publisher for Enterprise Manager Administrators in an underlying LDAP-based Authentication security Model environment.

15.5 Limiting access to BI Publisher features

Granting the previously discussed four OPSS application roles is somewhat different depending on the BI Publisher security model that is in place. To review, the 2 security models that BI Publisher supports are:

- Repository-Based Authentication
- Underlying LDAP-based Authentication

15.5.1 Granting BI Publisher OPSS Application Roles to Enterprise Manager Administrators in Repository-Based Authentication Mode Using *wlst*

wlst.sh can be used to grant access to the BI Publisher to Enterprise Manager administrators. The following *wlst.sh* usage example demonstrates using *wlst.sh* to grant VIEW access to the Enterprise Manager administrator named "JERRY" (italicized items are entered at the command-line). It is important to use uppercase letters for Enterprise Manager Administrator names.

Note: If you have just upgraded to BI Publisher 11.1.1.6.0 on Enterprise Manager 12c Release 3 (12.1.0.3) from a prior installation of BI Publisher on Enterprise Manager 12c Release 1 (12.1.0.1) or Release 2 (12.1.0.2). It is not necessary to grant access to BI Publisher to specific Enterprise Manager administrators that had already been granted access. In order to grant access to additional, or revoke access from existing, Enterprise Manager administrators, this step is still required.

To run the script:

1. Connect to the Administration Server over the t3s protocol using the `connect ()` command. The command takes three arguments:

- Username: Always 'weblogic'.
 - Password: This is the password that you used when you setup Enterprise Manager 12c Cloud Control.
 - Protocol: t3s (ssl), the host, and the port. These are the values for the WLS Administration Server. The port number is the same port number that you use when you connect to the WLS Administration Console in a browser. For example: https:<host>:<port>/console).
2. Grant EMBIP* role(s) to individual Enterprise Manager 12c Cloud Control administrators. Administrator "JERRY" is used in this example.

Example Session

```
$MW_HOME/oracle_common/common/bin/wlst.sh [linux]
wlst.cmd [windows]
...
...
Initializing WebLogic Scripting Tool (WLST) ...

Welcome to WebLogic Server Administration Scripting Shell

Type help() for help on available commands

wls:/offline> connect('weblogic','<pw>','t3s://host:port')
...
...
Successfully connected to Admin Server 'EMGC_ADMINSERVER' that belongs to domain
'GCDomain'.

wls:/GCDomain/serverConfig>
grantAppRole(appStripe="obi",appRoleName="EMBIPViewer",principalClass="weblogic.se
curity.principal.WLSUserImpl",principalName="JERRY")

Location changed to domainRuntime tree. This is a read-only tree with DomainMBean
as the root.

For more help, use help(domainRuntime)
wls:/GCDomain/serverConfig> exit()
```

Revoking VIEW Access to BI Publisher Reports

In the following example session you revoke VIEW access to BI Publisher reports from user "JERRY" (case is important).

```
$MW_HOME/oracle_common/common/bin/wlst.sh [linux]
wlst.cmd [windows]
...
...
Initializing WebLogic Scripting Tool (WLST) ...

Welcome to WebLogic Server Administration Scripting Shell

Type help() for help on available commands

wls:/offline> connect('weblogic','<pw>','t3s://host:port')
...
...
Successfully connected to Admin Server 'EMGC_ADMINSERVER' that belongs to domain
'GCDomain'.
```

```
wls:/GCDomain/serverConfig>  
revokeAppRole(appStripe="obi",appRoleName="EMBIPViewer",principalClass="weblogic.s  
ecurity.principal.WLSUserImpl",principalName="JERRY")
```

Location changed to domainRuntime tree. This is a read-only tree with DomainMBean as the root.

```
For more help, use help(domainRuntime)  
wls:/GCDomain/serverConfig> exit()
```

15.5.2 Propagation Time for Changes to OPSS

When changing an Enterprise Manager administrator's BI Publisher access privileges (**EMBIPViewer**, **EMBIPAdministrator**, **EMBIPScheduler**, **EMBIPAuthor**) the Super Administrator needs to wait 15 or more minutes for the changes to propagate through OPSS and become effective. The change will then be effective the next time the administrator logs into BI Publisher.

15.6 Allowing Access to BI Publisher for Enterprise Manager Administrators in an underlying LDAP Authentication security model environment

Enterprise Manager and BI Publisher are separate applications. When using an underlying LDAP-based authentication model, LDAP groups defined in the external LDAP server can also be used to manage access to BI Publisher. These LDAP groups allow varying levels of access to BI Publisher. Hence, you can add an LDAP user as a member of one or more of these LDAP group and appropriate capabilities of BI Publisher will be exposed. These LDAP groups, which either need to be created or existing ones used, are coordinated with the permissions of the catalog object in the "Enterprise Manager Cloud Control" folder.

Note: Because BI Publisher and Enterprise Manager are configured within the same WebLogic domain, it is not necessary to perform any specific LDAP configuration in the BI Publisher application. The following steps are sufficient to configure LDAP.

In an underlying LDAP-based authentication security model, the following steps are required:

- The administrator of the LDAP server needs to use four external groups of any chosen name. These groups need to be grouped hierarchically. Existing groups can be used, or new ones can be created.

Important: The group names must be all upper-case.

Group Name Examples:

- EMBIPADMINISTRATOR
- EMBIPVIEWER
- EMBIPSCHEDULER
- EMBIPAUTHOR

- The administrator of the LDAP server must then make the additional changes below in order to achieve the necessary hierarchical structure shown in the hierarchy diagram above. For example, using the sample LDAP group names above:

Make EMBIPADMINISTRATOR a member of EMBIPAUTHOR

Make EMBIPADMINISTRATOR a member of EMBIPSCHEDULER

Make EMBIPAUTHOR a member of EMBIPVIEWER

Note: In LDAP, the terminology and concepts can seem backwards and confusing. For example, you want the EMBIPAUTHORS group to have as a member the EMBIPADMINISTRATORS group.

Then, in order to grant access to BI Publisher and its catalog objects, the administrator of the LDAP server needs to make respective LDAP users a members of one or more of the above LDAP groups.

15.6.1 Mapping LDAP Groups to BI Publisher OPSS Application Roles

In order to map the four LDAP groups to the OPSS application roles described above, the LDAP groups need to be mapped using wlst.sh.

Note: If you have just upgraded to BI Publisher 11.1.1.6.0 on Enterprise Manager 12c Release 3 (12.1.0.3) from a prior installation of BI Publisher on Enterprise Manager 12c Release 1 (12.1.0.1) or Release 2 (12.1.0.2), and the names of your LDAP groups have not changed, this step is not necessary, as the prior OPSS application grants are carried over to the new installation.

For example, using the LDAP groups above (case is very important):

```
$MW_HOME/oracle_common/common/bin/wlst.sh [linux]
wlst.cmd [windows]
...
...
Initializing WebLogic Scripting Tool (WLST) ...

Welcome to WebLogic Server Administration Scripting Shell

Type help() for help on available commands

wls:/offline> connect('weblogic','<pw>','t3s://host:port')
...
...
Successfully connected to Admin Server 'EMGC_ADMINSERVER' that belongs to domain
'GCDomain'.

wls:/GCDomain/serverConfig>
grantAppRole(appStripe="obi",appRoleName="EMBIPViewer",principalClass="weblogic.se
curity.principal.WLSGroupImpl",principalName="EMBIPVIEWER")
Location changed to domainRuntime tree. This is a read-only tree with DomainMBean
as the root.
For more help, use help(domainRuntime)

wls:/GCDomain/serverConfig>
```

```
grantAppRole(appStripe="obi",appRoleName="EMBIPAuthor",principalClass="weblogic.se
curity.principal.WLSGroupImpl",principalName="EMBIPAUTHOR")
Already in Domain Runtime Tree

wls:/GCDomain/serverConfig>
grantAppRole(appStripe="obi",appRoleName="EMBIPScheduler",principalClass="weblogic
.security.principal.WLSGroupImpl",principalName="EMBIPSCHEDULER")
Already in Domain Runtime Tree

wls:/GCDomain/serverConfig>
grantAppRole(appStripe="obi",appRoleName="EMBIPAdministrator",principalClass="webl
ogic.security.principal.WLSGroupImpl",principalName="EMBIPADMINISTRATOR")
Already in Domain Runtime Tree

wls:/GCDomain/serverConfig> exit()
```

15.7 Securing BI Publisher with a Secure Socket Layer (SSL) Certificate

The BI Publisher WebLog Server is configured with a default identity keystore (DemoIdentity.jks) and a default trust keystore (DemoTrust.jks). In addition, WebLogic Server trusts the CA certificates in the JDK cacerts file. This default keystore configuration is appropriate for testing and development purposes. However, these keystores should not be used in a production environment.

There are two scenarios in which it would be necessary to provide a custom SSL certificate for the BI Publisher WebLogic Server.

- If you have Configured Enterprise Manager to use a trusted custom certificate, as documented in the Oracle® Enterprise Manager Cloud Control Security Guide- "Configuring Custom Certificates for WebLogic Server"
- If you wish to access BI Publisher in a development environment via browsers that restrict access to SSL web servers with a 1024-bit public key.

Scenario 1 - Setting Up BI Publisher to Share the Same Custom SSL Certificate as the Enterprise Manager Management Service.

In scenario 1, you have configured Enterprise Manager to use a custom trusted certificate. You should also setup BI Publisher to use the same certificate. Two types of certificates are supported with Enterprise Manager: Java Keystore (JKS) format, and Oracle PKCS12 wallets.

1. First setup and configure Enterprise Manager as documented in the above section. (make sure to stop and start Enterprise Manager after the "emctl secure wls" command).
2. Then, configure BI Publisher to use the same certificate using the "emctl secure bip" command. The command-line arguments to the "emctl secure bip" command are the same as the "emctl secure wls" commands. So, for example, if your certificate resided in \$HOME/TRUST, and has a private key alias "pvtkeyalias", these steps would be followed.
3. *A: Secure the Enterprise Management Servers using a Java Keystore:*

```
$ emctl secure wls -jks_loc $HOME/TRUST/emidentity.jks -jks_pvtkey_alias
pvtkeyalias
$ emctl stop oms -all
$ emctl start oms
```

B. Secure BI Publisher using the same Java Keystore:

```
$ emctl secure bip -jks_loc INSTANCE_HOME/sysman/config/keystore/emidentity.jks
-alias pvtkeyalias
```

Notice that you must provide the same keystore that Enterprise Manager has been configured with in Step A. This is found in the `INSTANCE_HOME` directory as specified above. If you try to specify a different keystore, you will get an error message.

```
Stop BI Publisher using the WebLogic Administration Console
$ emctl stop oms -all
$ emctl start oms
Start BI Publisher using the WebLogic Administration Console
```

Alternatively, you may also use an Oracle Wallet. In the following example, the `ewallet.p12` file resides in the directory `$HOME/TRUST/wallet`:

A. Secure the Enterprise Management Server using an Oracle Wallet.

```
$ emctl secure wls -wallet $HOME/TRUST/wallet
$ emctl stop oms -all
$ emctl start oms
```

B. Secure BI Publisher with the same wallet:

```
$ emctl secure bip -wallet $HOME/TRUST/wallet
Stop BI Publisher using the WebLogic Administration Console
$ emctl stop oms -all
$ emctl start oms
Start BI Publisher using the WebLogic Administration Console
```

Scenario 2 - Setting Up BI Publisher with a Self-signed Certificate

First, create a self-signed certificate. In this example, the Java "keytool" utility is used to create a self-signed Java Keystore (JKS) certificate with the private key alias "selfsigned".

```
$ keytool -genkey -keyalg RSA -alias selfsigned -keystore
$HOME/SELFSIGNED/keystore.jks -validity 360 -keysize 2048
Enter keystore password: <some password>
Re-enter new password: <repeat>
What is your first and last name?
[Unknown]: somehost.example.com
What is the name of your organizational unit?
[Unknown]: Organization
What is the name of your organization?
[Unknown]: Sample Corporation
What is the name of your City or Locality?
[Unknown]: City
What is the name of your State or Province?
[Unknown]: California
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=somehost.example.com, OU=Organization, O=Sample Corporation, L=City,
ST=California, C=US correct?
[no]: yes
Enter key password for <selfsigned>
(RETURN if same as keystore password): <some password>
$ keytool -list -keystore $HOME/SELFSIGNED/keystore.jks
Enter keystore password: <password from above>
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 1 entry
```



```
selfsigned, May 23, 2013, PrivateKeyEntry,
Certificate fingerprint (MD5): XX:YY:ZZ...
```

Now, configure BI Publisher to use the following certificate:

```
$ emctl secure bip -jks_loc $HOME/SELFSIGNED/keystore.jks -jks_pvtkey_alias
selfsigned
```

Stop the BI Publisher Managed Server from the WebLogic Administration Console.

```
$ emctl stop oms -all
$ emctl start oms
```

Start the BI Publisher Managed Server from the WebLogic Administration Console.

Rolling back BI Publisher to the Demonstration Certificate

If you rollback the Enterprise Manager to use the demonstration certificate, as documented in the Enterprise Manager Cloud Control Security Guide - "Rolling back to the Demonstration Certificate", it may be desirable to roll back BI Publisher to the demonstration certificate as well. First, follow the instructions in the above section:

1. Stop the OMS.

```
<OMS_Home>/bin/emctl stop oms
```

2. Run the following command:

```
<OMS_Home>/bin/emctl secure wls -use_demo_cert
```

3. Stop the OMS.

```
<OMS_Home>/bin/emctl stop oms -all
```

4. Start the OMS.

```
<OMS_Home>/bin/emctl start oms
```

Now, you can rollback BI Publisher to the demonstration certificate as well:

1. `emctl secure bip -use_demo_cert`
2. Stop the BI Publisher Managed Server from the WebLogic Administration Console.
3. `emctl stop oms -all`
4. `emctl start oms`
5. Start the BI Publisher Managed Server from the WebLogic Administration Console.

15.8 BI Publisher Administration

Please refer to the BI Publisher documentation for instructions on configuring BI Publisher settings.

Common administrative tasks:

- Configuring server properties, such as e-mail servers.
- Configuring report delivery channels, such as FTP.

15.9 Post-Upgrade Steps to take after upgrading to BI Publisher to 11.1.1.6.0

When performing an upgrade (using the *configureBIP -upgrade* command) from Enterprise Manager 12c Cloud Control Release 1 (12.1.0.1) that contains an installed BI Publisher 11.1.1.5.0, to Enterprise Manager 12c Cloud Control Release 3 (12.1.0.3), containing BI Publisher 11.1.1.6.0, you need to perform post-upgrade steps. This is required due to the removal of the underscores on all Enterprise Manager-supplied BI Publisher Catalog objects.

1. Any schedules associated with the following eight reports must be stopped [note the underscores]

EM_Sample_Reports

Targets_of_Specified_Type

[Chargeback]

Charge_Summary_Report

Charge_Trend_Report

Usage_Summary_Report

Usage_Trend_Report

[Consolidation_Planner]

Consolidation_Reports

[Events reports]

Escalated_Incidents_Report

Incident_History_Report

Top_Events_Report

2. The following datamodels [note the underscores] should be deleted from the EM_Datamodels folder:

Charge_Summary_Report

Charge_Trend_Report

Consolidation_Reports

Escalated_Incidents_Report

Incident_History_Report

Target_of_Specified_Type

Top_Events_Report

Usage_Summary_Report

Usage_Trend_Report

3. Delete these folders:

EM_Sample_Reports

Consolidation_Planner

4. The following reports must be deleted from their respective folders:

[Chargeback]
 Charge_summary_report
 Charge_trend_report
 Usage_summary_report
 Usage_trend_report
 [Events]
 Escalated_Incidents_Report
 Incident_History_Report
 Top_Events_Report

Any desired schedules from above that were stopped need to be restarted on the new report names **without** underscores.

15.10 EMBIP* Roles: Granting Access to Folders and Catalog Objects

By default, the shipping security model (as described in [Section 15.4.5](#), applies to BI Publisher catalog objects that are inside the "Enterprise Manager Cloud Control" folder. This is due to the fact that the catalog objects that exist in this folder are set up with a default set of permissions. See [Section 15.4.3](#). BI Publisher catalog objects that are outside of this folder will not automatically contain these same permissions. For example, BI Publisher ships with numerous reports in a shared folder called "Samples". If it is desired to grant access to this folder to Enterprise Manager/BI Publisher users, other than EMBIPAdministrator, it is necessary for a BI Publisher super administrator (EMBIPAdministrator) to change the permissions of this folder. They do so by selecting the folder "Samples" and choosing "Permissions" in the bottom left task bar. They then need to add the four privileges (EMBIPAdministrator, EMBIPViewer, EMBIPAuthor, EMBIPScheduler) and grant appropriate access to that privilege such as VIEW report, run report online, to EMBIPViewer. The administrator can model the appropriate privileges to grant based on any of the shipping Enterprise Manager reports (for example, *Targets of Specified Type*).

Individual users, who have the EMBIPAuthor OPSS application role, can develop reports in their own private folders. These reports will not be available to other users.

Note: The shared folder "Enterprise Manager Cloud Control" contains Enterprise Manager-provided BI Publisher Reports and is reserved for such. No custom-developed reports may be added to this folder hierarchy. The default security model that ships with Enterprise Manager specifically prohibits this.

Note: Only reports in the "Enterprise Manager Cloud Control" folder will show up in the Enterprise Manager BI Publisher Enterprise Reports menu (From the **Enterprise** menu, select **Reports**, and then **BI Publisher Enterprise Reports**).

If a BI Publisher administrator (EMBIPAdministrator) wishes to create a new shared folder outside of the "Enterprise Manager Cloud Control" folder, they can do so. These reports would not show up in the Enterprise Manager BI Publisher reports menu but

would be available to other Enterprise Manager administrators as long as appropriate permissions are granted as previously described.

15.11 Access to Enterprise Manager Repository

All BI Publisher reports are granted read-only access to the Enterprise Manager Repository. This access is via the BI Publisher data source named **EMREPOS**. This access is via the Enterprise Manager user **MGMT_VIEW**, which is a special internal Enterprise Manager user who has read-only access to the Enterprise Manager Published **MGMT\$** database views. In addition, when reports are run, they are further restricted to the target-level security of the user running the report. For example, if user JOE has target-level access to "hostabc" and "database3", when user JOE runs a BI Publisher report (any report) he can only view target-level data associated with these two targets.

15.12 Troubleshooting

The following sections provide common strategies that can be used if problems occur with the Enterprise Manager/BI Publisher integration.

15.12.1 Rerunning configureBIP

It is sometimes necessary to rerun configureBIP if certain error conditions occur. Before attempting to re-run configureBIP, be sure to use the WebLogic console to shutdown the existing BI Publisher managed server.

15.12.2 BI Publisher Log File Locations

The following log files can be used to trace problems to their point of origin.

15.12.2.1 configureBIP Log Files

Location: `ORACLE_HOME(oms)/cfgtoollogs/bip/*`

- Creating/upgrading the BI Publisher schema in the database
 - "emBIPLATFORM.log
 - "emBIPLATFORMcreate_<date>.log
 - "biplatform.log
 - "emBIPLATFORMcreate.err
- Extending the Enterprise Manager domain with BI Publisher
 - "bipca_<date>.log

15.12.2.2 Enterprise Manager BI Publisher Tree and EM CLI Log File Output

emoms.trc

emoms.log

Messages specific to the BI Publisher integration can be found by searching for "BIP" (all caps) in the log files.

15.12.2.3 BI Publisher Runtime

Location: Domain home. For example, `gc_inst/user_projects/domains/GCDomain`

- servers/BIP/logs/*
- servers/BIP/logs/bipublisher.log

15.12.3 Additional Troubleshooting

If BI Publisher is able to run successfully, but BI Publisher registration with Enterprise Manager fails, you can retry the registration by running:

```
emcli login -username=<admin username> -password=<admin password>
emcli sync
emcli setup_bipublisher -proto=http[s] -host=<bip_host> -port=<bip_port>
-uri=xmlpserver
```

15.12.4 Redeploying All Enterprise Manager-Supplied BI Publisher Reports

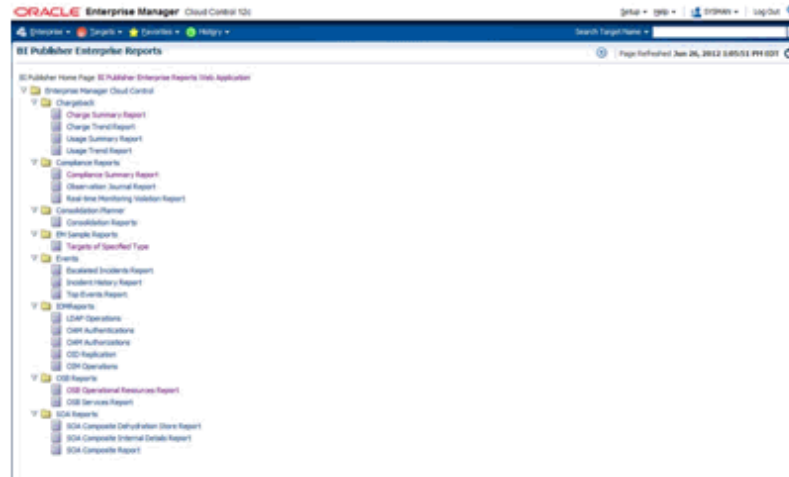
If a plug-in is installed subsequent to BI Publisher being installed and configured to work with Enterprise Manager, the BI Publisher reports that are part of the plug-in can be deployed from the Enterprise Manager installation to BI Publisher using the following commands:

```
emcli login -username=sysman
Password: <pw>
emcli sync
emcli deploy_bipublisher_reports -force
```

This procedure can also be used to restore reports on BI Publisher if they become damaged.

15.13 Managing Enterprise Manager - BI Publisher Connection Credentials

Accessing BI Publisher from Enterprise Manager requires a direct connection between the two products in order to retrieve, display, and manage report definitions. Example: From the **Enterprise** menu, choose **Reports** and then **BI Publisher Enterprise Reports**. A tree view displaying BI Publisher reports within the Enterprise Manager Cloud Control shared folder appears as shown in the following graphic.



The first time you run the `configureBIP` script to configure BI Publisher to integrate with Enterprise Manager, a dedicated WebLogic user is automatically created with the requisite credentials solely for the purpose of installation/configuration. Beginning with Enterprise Manager 12c Cloud Control release 12.1.0.1, you can configure these credentials using the EMCTL command `config oms`.

Verb Syntax

```
emctl config oms -store_embipws_creds [-admin_pwd <weblogic_pwd>] [-embipws_user
<new_embipws_username>] [-embipws_pwd <new_embipws_pwd>]
```

The `config oms` command allows you to change the password, and optionally the username, used by Enterprise Manager to access the installed BI Publisher Web Server. Running the `config oms` command requires the WebLogic Admin user's password.

Note 1: The `config oms` command only changes the user credentials required for the Enterprise Manager - BI Publisher connection. The Enterprise Manager - BI Publisher connection credentials should match the credentials used elsewhere by the user. Example: Enterprise Manager users (database authentication), LDAP users, and WebLogic Server users. Use the corresponding application/console to create or manage the user within the installed credential store.

Note 2: This command is operational only if BI Publisher has been installed.

Note 3: It is not necessary to restart any managed server, such as `EMGC_OMSnnnn` or `BIPnnnn`.

Any valid credential that WebLogic supports is acceptable as long as that user also has the `EMBIPAdministrators` privilege (either in OPSS or LDAP, as appropriate).

Example: You have configured Enterprise Manager to use single sign-on (SSO) (backed by an LDAP credential store). The following steps illustrate the credential update process:

1. Create the LDAP user. Example: Create `EM_BIP_INTERNAL_USER` and assign this LDAP user a password such as `XYZ123`.

2. Make EM_BIP_INTERNAL_USER a member of the EMBIPADMINISTRATORS LDAP group. For more information about LDAP groups and Enterprise Manager-BI Publisher integration, see [Section 15.6, "Allowing Access to BI Publisher for Enterprise Manager Administrators in an underlying LDAP Authentication security model environment"](#).

3. Execute the EMCTL config oms command:

```
emctl config oms -store_embipws_creds -embipws_user EM_BIP_INTERNAL_USER
Oracle Enterprise Manager Cloud Control 12c Release 2
Copyright (c) 1996, 2012 Oracle Corporation. All rights reserved.
Enter Admin User's Password: <pw>
Enter new password that Enterprise Manager will use to connect to BI Publisher:
XYZ123
Successfully updated credentials used by Enterprise Manager to connect to BI
Publisher.
```

If you later change the EM_BIP_INTERNAL_USER password in the LDAP server, you can change the LDAP user's password by executing the config oms command with the -store_embipws_creds option. In the following example, the password is changed to ABC123.

```
emctl config oms -store_embipws_creds
Oracle Enterprise Manager Cloud Control 12c Release 2
Copyright (c) 1996, 2012 Oracle Corporation. All rights reserved.
Enter Admin User's Password: <pw>
Enter new password that Enterprise Manager will use to connect to BI Publisher
: ABC123
Successfully updated credentials used by Enterprise Manager to connect to BI
Publisher.
```

15.14 Managing the BI Publisher Server

BI Publisher operates as a separate, managed server in the same WebLogic domain that contains the OMS(s) and the AdminServer.

In order to shut down the BI Publisher managed server, do the following:

1. Log in to the AdminServer console as the WebLogic user with the correct password.
2. Click Servers.
3. Click the Control tab underneath the text Summary of Servers.
4. Place a check-mark next to the managed server BIP.
5. Double-check to make sure the check mark is next to the BI Publisher managed server, as opposed to EMGS_OMS1 or EMGC_ADMINSERVER managed servers.
6. Click Shutdown and choose when work completes.
7. Wait until BI Publisher has shut down. You can monitor the status of this operation by clicking on the refresh icon (the two arrows in a circle) above the text Customize this Table.

To start the BI Publisher managed server, do the following:

1. Navigate to the control page using steps 1-4 above.
2. Place a check mark next to the managed server BIP.

3. Double-check to make sure the check mark is next to the BI Publisher managed server and not the EMGS_OMS1x or EMGC_ADMINSERVER managed servers.
4. Click Start.
5. Wait until BI Publisher has started. You can monitor the status of this operation by clicking on the refresh icon (the two arrows in a circle) above the text Customize this Table.

15.15 Configuring BI Publisher behind a Load-Balancer

If BI Publisher is to be run behind a load-balancer, as detailed in the Oracle® Enterprise Manager Cloud Control Administrator's Guide, issue the following commands after all configuration is complete:

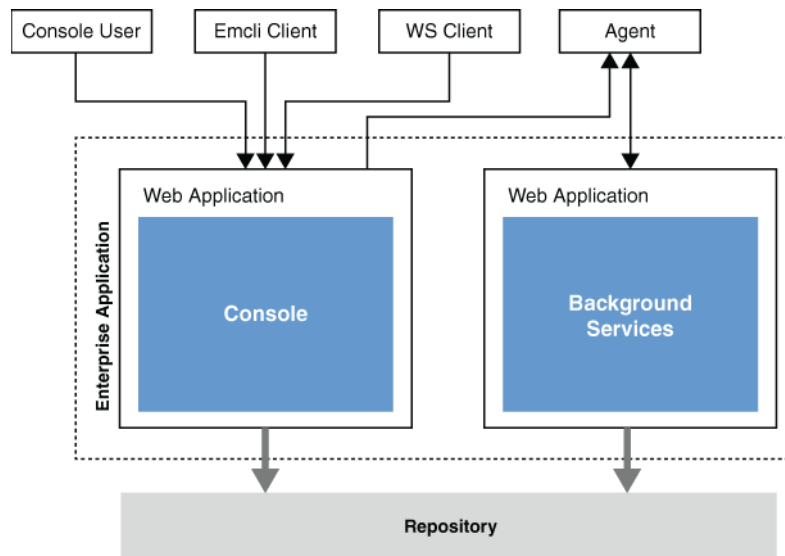
```
emcli login -username=sysman
Password: <sysman_password>
emcli setup_bipublisher -proto=https -host=<load_balancer_host> -port=<load
balancer port> -uri=xmlpserver -force -nodeploy
```


Running OMS in Console-Only Mode

Oracle Management Service (OMS) is designed to run two types of services, mainly the console services and the background services. While the console services are required to render a GUI-rich console for Enterprise Manager, the background services are required to run critical jobs, upload operations, business logics, and so on.

Figure 16-1 illustrates the functioning of an OMS where both console services and background services are running.

Figure 16-1 *Functioning of OMS with Active Console and Background Services*



In a multi-OMS environment, to have a dedicated OMS for UI operation or to not run background services in SSA OMS, you can choose to shut down the background services, and run only the UI services, thus turning the OMS into a pure, console-only mode. In such a case, the Management Agents upload data to other OMS instances where both background services and UI services are running.

To run the OMS in console-only mode, follow these steps:

1. Stop the OMS using the following command.

```
$emctl stop oms
```
2. Set the start up mode to console-only, using the following command.

```
$emctl config oms -set_startup_mode console_only
```
3. Start the OMS using the following command.

```
$emctl start oms
```

Note: Only the Additional OMS instances can be run in console-only mode, while the OMS instance that shares the host with the Admin Server cannot.

To revert the OMS instances to Normal mode, run the following command, and restart the OMS.

```
$emctl config oms -set_startup_mode normal
```

Part VI

Deinstallation

In particular, this part contains the following chapters:

- [Chapter 17, "Deinstalling Enterprise Manager \(Single and Multi-OMS Environments\)"](#)
- [Chapter 18, "Deinstalling Oracle Management Agent"](#)
- [Chapter 19, "Deinstalling ADP and JVMD"](#)
- [Chapter 20, "Removing Standby Oracle Management Services"](#)

Deinstalling Enterprise Manager (Single and Multi-OMS Environments)

This chapter describes how you can deinstall an entire Enterprise Manager system, and also how you can remove the entries of an Oracle Management Service (OMS) from the Oracle Management Repository (Management Repository) in case you lost the host where the OMS was running.

In particular, this chapter covers the following:

- [Deinstalling Enterprise Manager](#)
- [Deinstalling or Undeploying Only Plug-ins from the OMS](#)
- [Deleting OMS Entries from the Management Repository](#)

17.1 Deinstalling Enterprise Manager

This section covers the following subsections to describe how you can deinstall the entire Enterprise Manager system—single OMS environment or multi-OMS environment with additional Oracle Management Services (OMS).

- [Prerequisites for Deinstalling Only the OMS and Retaining the Management Repository](#)
- [Prerequisites for Deinstalling the Entire Enterprise Manager System](#)
- [Deinstallation Procedure](#)
- [After You Deinstall](#)

Caution: Make sure you meet the prerequisites before deinstalling the software. Make sure you follow the flow or sequence outlined in this chapter. For example, make sure you drop the schemas as described in the prerequisites section before deinstalling the software binaries. Do NOT change the order of instructions.

17.1.1 Prerequisites for Deinstalling Only the OMS and Retaining the Management Repository

Before you deinstall Enterprise Manager, meet the following prerequisites:

1. *(For Multi-OMS Environment)* Deconfigure and delete all the additional OMS instances by running the following command from each of their homes:

```
$<OMS_HOME>/bin/omsca delete -OMSNAME <oms_name>
```

Note:

- Run this command on each of the additional OMS instances.
 - You are prompted to confirm your action, and furnish the AdminServer credentials and the repository database details such as the database host name, listener port, SID, and password. Once you provide the required details, the command automatically stops the OMS, Oracle WebLogic Server, and also Oracle WebTier.
-

For example, if you have two additional OMS instances named `EMGC_Addln_OMS2` and `EMGC_Addln_OMS3`, on two different hosts, then on the first additional OMS, run the following command:

```
/u01/app/Oracle/Middleware/oms/bin/omsca delete -OMSNAME EMGC_Addln_OMS2
```

Then, on the second additional OMS, run the following command:

```
/u01/app/Oracle/Middleware/oms/bin/omsca delete -OMSNAME EMGC_Addln_OMS3
```

2. *(For Multi-OMS Environment)* Manually delete the following WebLogic targets of the deleted OMS:
 - `/EMGC_GCDomain/GCDomain/EMGC_OMS2` (Oracle WebLogic Server)
 - `/EMGC_GCDomain/instance2/ohs2` (Oracle HTTP Server)
3. *(For Multi-OMS Environment)* Stop all the Oracle Management Agents (Management Agent), which are running on the additional OMS hosts, by running the following command from each of their homes:

```
$<AGENT_HOME>/bin/emctl stop agent
```

Note: Run this command on each of the Management Agents configured with the additional OMS instances.

For example, if you have two additional OMS instances with a Management Agent on each of them, then on the first additional OMS host where the first Management Agent is running, run the following command:

```
/u01/app/Oracle/agent/core/12.1.0.3.0/bin/emctl stop agent
```

Then, on the second additional OMS host where the second Management Agent is running, run the following command:

```
/u01/app/Oracle/agent/core/12.1.0.3.0/bin/emctl stop agent
```

4. Deconfigure and delete the first (main) OMS where the Admin Server is configured:

```
$<OMS_HOME>/bin/omsca delete -full
```

For example,

```
/u01/app/Oracle/Middleware/oms/bin/omsca delete -full
```

Note: You are prompted to confirm your action, and furnish the AdminServer credentials and the repository database details such as the database host name, listener port, SID, and password. Once you provide the required details, the command automatically stops the OMS, Oracle WebLogic Server, and also Oracle WebTier.

5. Stop the Management Agent running on the first (main) OMS, by running the following command from its home:

```
$<AGENT_HOME>/bin/emctl stop agent
```

For example,

```
/u01/app/Oracle/agent/core/12.1.0.3.0/bin/emctl stop agent
```

6. Stop the Oracle WebLogic Server so that it does not access the schemas you are going to drop in the next step. For instructions, see the chapter on starting and stopping Oracle Fusion Middleware components in the *Oracle Fusion Middleware Administrator's Guide*.

17.1.2 Prerequisites for Deinstalling the Entire Enterprise Manager System

Before you deinstall Enterprise Manager, meet the following prerequisites:

1. Perform the steps outlined in [Section 17.1.1](#).
2. Drop the Oracle Management Repository (Management Repository):

WARNING: Once the Management Repository is dropped, it CANNOT be retrieved. Therefore, drop the Management Repository ONLY IF you want to deinstall the entire Enterprise Manager system, that is, all your OMS instances, Management Agents, and also the Management Repository. If you want to deinstall only the OMS (or any additional OMS), then do not drop the Management Repository.

WARNING: The RepManager in drop mode puts the database in quiesce mode by "ALTER SYSTEM QUIESCE RESTRICTED;" command.

- a. Ensure that there are no SYSMAN users logged in.
- b. Drop the Enterprise Manager Cloud Control schema (SYSMAN schema) and the Metadata schema (MDS schema) from the Management Repository by running the following command from the OMS home:

```
$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager <database_host>  
<repository_database_port> <repository_database_sid> -action  
dropall -dbUser <repository_database_user> -dbPassword <repository_  
database_password> -dbRole <repository_database_user_role>  
-reposName <repository_name> -mwHome <middleware_home> -mwOraHome  
<middleware_ora_home> -oracleHome <OMS_HOME>
```

For example,

```
/u01/app/Oracle/Middleware/oms/sysman/admin/emdrep/bin/RepManager
```

```
example.com 1234 sid_em -action dropall -dbUser sys -dbPassword letmein  
-dbRole sysdba -reposName SYSMAN -mwHome /u01/app/Oracle/Middleware/  
-mwOraHome /u01/app/Oracle/Middleware/ -oracleHome  
/u01/app/Oracle/Middleware/oms/
```

Note:

- For Microsoft Windows, invoke `RepManager.bat`.
- OMS home or `$(OMS_HOME)` refers to the first (main) OMS where the Admin Server is configured.
- `-mwHome` and `-mwOraHome` refer to the middleware home where the first (main) OMS is configured. The first (main) OMS is the OMS where the Admin Server is configured.
- `-oracleHome` refers to the Oracle home of the first (main) OMS where the Admin Server is configured.
- If you are dropping the schemas that belong to a 10g Release 2 (10.2.x.x) Management Repository, then run the command without these arguments: `-mwHome <middleware_home>`
`-mwOraHome <middleware_ora_home>` `-oracleHome <oracle_home>`

For example,

```
/u01/app/Oracle/Middleware/oms/sysman/admin/emdrep/bin/Re  
pManager example.com 1234 sid_em -action dropall -dbUser  
sys -dbPassword letmein -dbRole sysdba -reposName SYSMAN
```

- RepManager Support:
 - RepManager 12.1 supports `-action dropall` and `-action drop`, which drop SYSMAN, SYSMAN_MDS, SYSMAN_APM, SYSMAN_OPSS, and SYSMAN_RO.
 - RepManager 11.1 supports `-action dropall`, which drops only SYSMAN and SYSMAN_MDS, and `-action drop`, which drops only SYSMAN.
 - RepManager 10.2.0.5 supports `-action drop`, which drops only SYSMAN.
 - The `-action dropall` command drops all the schemas and provides a confirmation message. If the action was unsuccessful, then it lists all the entities that could not be cleaned or dropped. For example, X schema is not cleaned, synonyms are not cleaned, tablespaces are not cleaned. In this case, rerun the command.

If you do not have RepManager, or if you want to manually clean up the leftover entities, then see *My Oracle Support* note 1365820.1.
 - If you want to drop the Enterprise Manager schema completely, then use the RepManager available in the OMS home. Do not use the one in database home because it cannot remove the Enterprise Manager schema completely.
-

- c. Manually delete the data files `mgmt.dbf` and `mgmt_ecm_depot1.dbf` from the database home.

17.1.3 Deinstallation Procedure

This section describes the following:

- [Deinstalling in Graphical Mode](#)
- [Deinstalling in Silent Mode](#)

17.1.3.1 Deinstalling in Graphical Mode

To deinstall Enterprise Manager—single OMS environment or multi-OMS environment with additional OMS instances—in graphical mode, follow these steps:

Note:

- Deinstall the components in the order described in this procedure. Otherwise, the installation wizard displays an error.
 - **For a multi-OMS environment, perform the steps outlined in this section on each of the additional OMS instances.**
-
-

1. Invoke the installer from the OMS home by running the following command:

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall ORACLE_HOME=<absolute_path_
to_oms_home> -jreLoc <path> [-removeallfiles] [-invPtrLoc <absolute_
path_to_orainst.loc>]
```

For example,

```
/u01/app/Oracle/Middleware/oms/oui/bin/runInstaller -deinstall
ORACLE_HOME=/u01/app/Oracle/Middleware/oms/ -jreLoc
/u01/app/Oracle/Middleware/jdk16/jdk -removeallfiles -invPtrLoc
/u01/orainst.loc
```

Note:

- You can invoke the installer even from the directory where you downloaded the software. For example, `<software_location>/.`
 - The `-invPtrLoc` parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
 - When you run `runInstaller -help`, you will see the option `-nowarningonremovefiles` listed. This option is currently not supported and has no effect even if you use it.
-
-

2. On the Inventory screen, select the plug-in homes, and click **Remove**.
3. On the Inventory screen, select the `sbin` home, and click **Remove**.
4. On the Inventory screen, select the Java Development Kit (JDK) home, and click **Remove**.

Note: Deinstall JDK only if it was installed by the installation wizard while installing the Enterprise Manager system. Otherwise, you can skip this step.

Note: After deinstalling JDK, do NOT exit the installer. If you exit the installer inadvertently, then follow these steps:

1. Manually download and install JDK 1.6.0.43.0 on the OMS host. If you already have this supported version, then you can reuse it.
2. Invoke the installer again and pass the absolute path to the location where you have JDK:

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall -jreLoc <JDK_HOME> [-removeallfiles] [-invPtrLoc <absolute_path_to_oraInst.loc>]
```

5. On the Inventory screen, select the Oracle WebTier home, and click **Remove**.
6. On the Inventory screen, select the following, and click **Remove**.
 - OMS home
 - Management Agent home
 - Oracle Common directory
7. On the Inventory screen, click **Close** to exit the wizard.
8. Manually delete the middleware home:

For UNIX platforms:

```
rm -rf <absolute_path_to_middleware_home>
```

For Microsoft Windows platforms:

```
del <absolute_path_to_middleware_home>
```

Note: If you see an error stating that the middleware home could not be deleted because of a long path, then shorten the middleware home name in one of the following ways:

- Rename the middleware home to a short name.

For example, change C:\Oracle\Middleware to C:\OR\MW.

- Mount a drive to the middleware home path.

For example, if C:\Oracle\Middleware\oms\bin is the directory that is causing an issue, then shorten the path in such a way that path length decreases to a reasonable extent (*the file path limits differ from one operating system to another*).

Mount C:\Oracle\Middleware\oms to drive Z.

- Navigate to drive Z, and delete the files:

```
prompt>Z:
```

```
prompt>del bin
```

- Navigate to the middleware home, and delete the leftover files:

```
prompt:>C:
```

```
prompt>del C:\Oracle\Middleware\
```

9. Deinstall the Management Agent as described in [Chapter 18](#).

17.1.3.2 Deinstalling in Silent Mode

To deinstall Enterprise Manager—single OMS environment or multi-OMS environment with additional OMS instances—in silent mode, follow these steps:

Note:

- Deinstall the components in the order described in this procedure. Otherwise, the installation wizard displays an error.
 - **For a multi-OMS environment, perform the steps outlined in this section on each of the additional OMS instances.**
-

1. Deinstall Oracle WebLogic Server 11g Release 1 (10.3.6) following the instructions outlined in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*. See the chapter that describes how you can deinstall the software.

The *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server* is available in the Oracle WebLogic Server documentation library available at:

<http://www.oracle.com/technetwork/indexes/documentation/index.html>

Note: Deinstall Oracle WebLogic Server 11g Release 1 (10.3.6) only if it was installed by the installation wizard while installing the Enterprise Manager system.

2. Deinstall the plug-in homes:

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={absolute_path_to_plug-in_home}" ORACLE_HOME=<absolute_path_to_
oms_home> -jreLoc <JDK_HOME> [-removeallfiles] [-invPtrLoc <absolute_
path_to_oraInst.loc>]
```

For example,

```
/u01/app/Oracle/Middleware/oms/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={/u01/app/Oracle/Middleware/plugins/oracle.sysman.db.oms.plugin_
12.1.0.2.0,/u01/app/Oracle/agent/plugins/oracle.sysman.db.discovery.plugin_
12.1.0.2.0}" ORACLE_HOME=/u01/app/Oracle/Middleware/oms -jreLoc
/u01/app/Oracle/Middleware/jdk16/jdk -removeAllFiles -invPtrLoc
/u01/oraInst.loc
```

Note:

- You can invoke the installer even from the directory where you downloaded the software. If you do so, then do NOT pass `-removeallfiles`.

For example, if you have downloaded the software to `/u01/app/Oracle/Downloads`, then run the following command, skipping the `-removeallfiles` argument.

```
/u01/app/Oracle/Downloads/Disk1/runInstaller -deinstall -silent
"REMOVE_
HOMES={/u01/app/Oracle/Middleware/plugins/oracle.sysman.db.oms.
plugin_
12.1.0.2.0,/u01/app/Oracle/agent/plugins/oracle.sysman.db.disco
very.plugin_12.1.0.2.0}" ORACLE_
HOME=/u01/app/Oracle/Middleware/oms -jreLoc
/u01/app/Oracle/Middleware/jdk16 -invPtrLoc /u01/oraInst.loc
```

- When you run `runInstaller -help`, you will see the option `-nowarningonremovefiles` listed. This option is currently not supported and has no effect even if you use it.
 - To deinstall multiple plug-ins, enter the plug-in homes separated by a comma.
 - The `-invPtrLoc` parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
-

3. Deinstall the sbin home:

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={absolute_path_to_sbin_home}" ORACLE_HOME=<absolute_path_to_oms_
home> -jreLoc <JDK_HOME> [-removeAllFiles] [-invPtrLoc <absolute_path_
to_oraInst.loc>]
```

For example,

```
/u01/app/Oracle/Middleware/oms/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={/u01/app/Oracle/agent/sbin}" ORACLE_HOME=/u01/app/Oracle/Middleware/oms
-jreLoc /u01/app/Oracle/Middleware/jdk16 -removeAllFiles -invPtrLoc
/u01/oraInst.loc
```

4. Deinstall the Java Development Kit (JDK) home:

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={absolute_path_to_jdk_home}" ORACLE_HOME=<absolute_path_to_oms_
```

```
home> -jreLoc <JDK_HOME> [-removeAllFiles] [-invPtrLoc <absolute_path_to_oraInst.loc>]
```

For example,

```
/u01/app/Oracle/Middleware/oms/oui/bin/runInstaller -deinstall -silent "REMOVE_HOMES={/u01/app/Oracle/Middleware/jdk16}" ORACLE_HOME=/u01/app/Oracle/Middleware/oms -jreLoc /u01/app/Oracle/Middleware/jdk16 -removeAllFiles -invPtrLoc /u01/oraInst.loc
```

Note: Deinstall JDK only if it was installed by the installation wizard while installing the Enterprise Manager system. Otherwise, you can skip this step.

5. Manually download and install JDK 1.6.0.43.0 on the OMS host. If you already have this supported version, then you can reuse it.

You must reinstall JDK because the installer has a dependency on it. The new JDK can be installed anywhere on the OMS host, not necessarily in the same location where it existed before. However, ensure that you pass the `-jreLoc` parameter (as described in the following steps) while invoking the installer to indicate the location where you have installed the JDK.

6. Deinstall the Oracle WebTier home:

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_HOMES={absolute_path_to_web_tier}" ORACLE_HOME=<absolute_path_to_oms_home> -jreLoc <JDK_HOME> [-removeAllFiles] [-invPtrLoc <absolute_path_to_oraInst.loc>]
```

For example,

```
/u01/app/Oracle/Middleware/oms/oui/bin/runInstaller -deinstall -silent "REMOVE_HOMES={/u01/app/Oracle/Middleware/Oracle_WT}" ORACLE_HOME=/u01/app/Oracle/Middleware/oms -jreLoc /u01/app/Oracle/Middleware/jdk16 -removeAllFiles -invPtrLoc /u01/oraInst.loc
```

7. Deinstall the OMS, the Management Agent, and the Oracle Common directory:

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_HOMES={absolute_path_to_oracle_homes_and_directories_to_be_deinstalled}" ORACLE_HOME=<absolute_path_to_oms_home> -jreLoc <JDK_HOME> [-removeAllFiles] [-invPtrLoc <absolute_path_to_oraInst.loc>]
```

Note: The argument `REMOVE_HOMES` accepts more than one path separated by a comma.

For example,

```
/u01/app/Oracle/Middleware/oms/oui/bin/runInstaller -deinstall -silent "REMOVE_HOMES={/u01/app/Oracle/Middleware/oms,/u01/app/Oracle/agent/core/12.1.0.3.0,/u01/app/Oracle/Middleware/oracle_common}" ORACLE_HOME=/u01/app/Oracle/Middleware/oms -jreLoc /u01/app/Oracle/Middleware/jdk16 -removeAllFiles -invPtrLoc /u01/oraInst.loc
```

8. Manually delete the middleware home:

For UNIX platforms:

```
rm -rf <absolute_path_to_middleware_home>
```

For Microsoft Windows platforms:

```
del <absolute_path_to_middleware_home>
```

9. Deinstall the Management Agent as described in [Chapter 18](#).

17.1.4 After You Deinstall

After you deinstall, perform these steps:

1. The Oracle homes you deinstalled are deregistered from the central inventory. However, some files might still remain in these Oracle homes. You might also see the OMS instance base directory and the Oracle home for Web Tier. You can manually delete these files and directories.
2. The deinstallation process removes the entry of the `S98gcstartup` script, an auto-start script, from the `/etc/oragchomelist` file, but does not remove the script itself. You can leave this script and the soft links associated with it because when you install Enterprise Manager again on the same host, the installer automatically overwrites the script and re-create the soft links.

However, if you want to clear the host of any Oracle products, then Oracle recommends that you manually delete this script and the soft links associated with it. To do so, navigate to the `/etc/rc.d/` directory, and search for the script `S98gcstartup`. This script is usually present in a subdirectory within the `/etc/rc.d/` directory. Navigate to the subdirectory where the script is found and delete the script. For example, `/etc/rc.d/rc3.d/S98gcstartup` or `/etc/rc.d/init.d/gcstartup/S98gcstartup`.

3. The JDK, which was installed as part of Step (5) of [Section 17.1.3.2](#) to allow complete removal of the Enterprise Manager system, can now be removed manually (by deletion of the installed directory) if it is no longer needed for other purposes and if it did not replace the system-registered JDK.

17.2 Deinstalling or Undeploying Only Plug-ins from the OMS

If you want to deinstall or undeploy only the plug-ins from the OMS, and not the entire Enterprise Manager system, then use the Plug-ins page within the Enterprise Manager Cloud Control Console. For instructions, see the *Oracle Enterprise Manager Cloud Control Administrator's Guide*. **Do NOT use `runInstaller` to undeploy only the plug-ins.**

17.3 Deleting OMS Entries from the Management Repository

If you lose the host where an additional OMS is running, then make sure you manually delete the entry for that OMS from the Management Repository. To do so, follow these steps:

1. Run the following command to deconfigure Oracle WebLogic Server, applications, and so on from the WebLogic Domain; remove all OMS-related entries from the Management Repository; and delete these targets of the OMS: `oracle_oms`, `oracle_oms_pbs`, `oracle_oms_console`.

```
$ORACLE_HOME/bin/omsca delete
```

2. Manually delete the following WebLogic targets of the OMS.
 - `/EMGC_GCDomain/GCDomain/EMGC_OMS2 (weblogic_j2eeserver)`

- /EMGC_GCDomain/instance2/ohs2 (oracle_apache)

Now Enterprise Manager will not have any reference of the deleted additional OMS. If you want to delete the OMS, follow the instructions outlined in [Section 17.1](#).

Deinstalling Oracle Management Agent

This chapter describes how you can deinstall Oracle Management Agent (Management Agent). In particular, this chapter covers the following:

- [Deinstalling Oracle Management Agents](#)
- [Deinstalling or Undeploying Only Plug-ins from the Oracle Management Agent](#)

Note: On a cluster, ensure that you deinstall the Management Agents from all the nodes one by one. To do so, follow the instructions outlined in this chapter.

18.1 Deinstalling Oracle Management Agents

This section covers the following:

- [Prerequisites](#)
- [Deinstallation Procedure](#)
- [After You Deinstall](#)

18.1.1 Prerequisites

Before you deinstall a Management Agent, do the following:

1. Shut down the Management Agent by running the following command from its home. If it is already shut down, then skip this step.
2. Wait for the Management Agent to go to the *unreachable* state in the Cloud Control console. If it is already in the *unreachable* state, then go to the next step.
3. Delete the Management Agent targets and their monitored targets (from any host where EM CLI is installed):

```
emcli delete_target  
-name="example.com:1836"  
-type="oracle_emd"  
-delete_monitored_targets
```

Note: For information on EM CLI and instructions to set it up, see *Oracle Enterprise Manager Command Line Interface Guide*.

18.1.2 Deinstallation Procedure

This section describes the following:

- [Deinstalling Oracle Management Agent in Graphical Mode](#)
- [Deinstalling Oracle Management Agent in Silent Mode](#)
- [Deinstalling Shared Agent](#)
- [Deinstalling Oracle Management Agent Installed Using an RPM File](#)

18.1.2.1 Deinstalling Oracle Management Agent in Graphical Mode

To deinstall a Management Agent in graphical mode, follow these steps:

Note: Deinstall the components in the order described in this procedure. Otherwise, the installation wizard displays an error.

1. Invoke the installer from the Management Agent home by running the following command:

```
$<AGENT_HOME>/oui/bin/runInstaller -deinstall ORACLE_  
HOME=<absolute_path_to_agent_home> [-removeallfiles]  
[-invPtrLoc <absolute_path_to_oraInst.loc>]
```

For example,

```
/u01/app/oracle/agent/core/12.1.0.3.0/oui/bin/runInstaller  
-deinstall ORACLE_HOME=/u01/app/oracle/agent/core/12.1.0.3.0/  
-removeallfiles
```

Note:

- You can invoke the installer even from the directory where you downloaded the software. For example, <software_location>/.
 - When you run `runInstaller -help`, you will see the option `-nowarningonremovefiles` listed. This option is currently not supported and has no effect even if you use it.
 - The `-invPtrLoc` parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
 - For Microsoft Windows, invoke the `setup.exe` file.
-
-

Note: When you invoke `runInstaller` or `setup.exe`, if the Enterprise Manager Cloud Control Installation Wizard does not appear, then it is possible that you do not have access to the `/stage` directory.

There is a classpath variable that the installation wizard computes for OPatch as `../stage/Components/`, and when the `TEMP` variable is set to `/tmp`, the installation wizard tries to look for the `opatch` JAR file in the `/tmp/ ../stage` directory, which is equivalent to `/stage`. However, if you do not have the permission on `/stage`, then the installation wizard can hang. Under such circumstances, verify if you have access to the `/stage` directory. If you do not have access to it, then set the `TEMP` variable to a location where the install user has access to, and then relaunch the installation wizard.

2. In the installation wizard, click **Installed Products**.
3. On the Inventory screen, select the plug-in homes under the required Management Agent home, then click **Remove**.
4. On the Inventory screen, select the `sbin` home, and click **Remove**.
5. On the Inventory screen, select the Management Agent, and click **Remove**.
6. Manually delete the agent base directory. For information on installation base directory, see [Section 2.3.5](#).

For UNIX platforms:

```
rm -rf <absolute_path_to_agent_base_dir>
```

For Microsoft Windows platforms:

```
del <absolute_path_to_agent_base_dir>
```

18.1.2.2 Deinstalling Oracle Management Agent in Silent Mode

This section describes the following methods to deinstall the Management Agent in silent mode:

- [Deinstalling in Silent Mode Using the Installer](#)
- [Deinstalling in Silent Mode Using AgentDeinstall.pl Script](#)

18.1.2.2.1 Deinstalling in Silent Mode Using the Installer To deinstall a Management Agent in silent mode using the installer, follow these steps:

Note: Deinstall the components in the order described in this procedure. Otherwise, the installation wizard displays an error.

1. Deinstall the plug-in homes:

```
$<AGENT_HOME>/oui/bin/runInstaller -deinstall -silent
"REMOVE_HOMES={absolute_path_to_plug-in_home}" ORACLE_
HOME=<absolute_path_to_agent_home> [-removeallfiles]
[-invPtrLoc <absolute_path_to_orainst.loc>]
```

Note:

- When you run `runInstaller -help`, you will see the option `-nowarningonremovefiles` listed. This option is currently not supported and has no effect even if you use it.
 - On Microsoft Windows, invoke the `setup.exe` file.
 - The `-invPtrLoc` parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
 - To deinstall multiple plug-ins, enter the plug-in homes separated by a comma.
-

For example,

```
/home/oracle/agent/core/12.1.0.3.0/oui/bin/runInstaller
-deinstall -silent "REMOVE_
HOMES={/home/oracle/agent/plugins/oracle.sysman.emas.oms.plug
in_
12.1.0.2.0,/home/oracle/agent/plugins/oracle.sysman.emct.oms.
plugin_12.1.0.2.0}" ORACLE_
HOME=/home/oracle/agent/core/12.1.0.3.0 -removeAllFiles
-invPtrLoc /home/oracle/agent/core/12.1.0.3.0/oraInst.loc
```

2. Deinstall the sbin home:

```
$<AGENT_HOME>/oui/bin/runInstaller -deinstall -silent
"REMOVE_HOMES={absolute_path_to_sbin_directory}" ORACLE_
HOME=<absolute_path_to_agent_home> [-removeAllFiles]
[-invPtrLoc <absolute_path_to_oracle_inst.loc>]
```

For example,

```
/home/oracle/agent/core/12.1.0.3.0/oui/bin/runInstaller
-deinstall -silent "REMOVE_HOMES={/home/oracle/agent/sbin}"
ORACLE_HOME=/home/oracle/agent/core/12.1.0.3.0
-removeAllFiles -invPtrLoc
/home/oracle/agent/core/12.1.0.3.0/oraInst.loc
```

3. Deinstall the Management Agent:

```
$<AGENT_HOME>/oui/bin/runInstaller -deinstall -silent
"REMOVE_HOMES={absolute_path_to_agent_oracle_home}" ORACLE_
HOME=<absolute_path_to_agent_home> -removeAllFiles -invPtrLoc
<absolute_path_to_oracle_inst.loc>
```

For example,

```
/home/oracle/agent/core/12.1.0.3.0/oui/bin/runInstaller
-deinstall -silent "REMOVE_
HOMES={/home/oracle/agent/core/12.1.0.3.0}" ORACLE_
HOME=/home/oracle/agent/core/12.1.0.3.0 -removeAllFiles
-invPtrLoc /home/oracle/agent/core/12.1.0.3.0/oraInst.loc
```

4. Manually delete the agent base directory. For information on agent base directory, see [Section 2.3.5](#).

For UNIX platforms:

```
rm -rf <absolute_path_to_install_base_dir>
```

For Microsoft Windows platforms:

```
del <absolute_path_to_install_base_dir>
```

18.1.2.2.2 Deinstalling in Silent Mode Using AgentDeinstall.pl Script To deinstall a Management Agent in silent mode using the AgentDeinstall.pl script, follow these steps:

WARNING: By default, the AgentDeinstall.pl script deinstalls the Management Agent, removes the dependent entries from the inventory, and removes the entire agent base directory. If you want to retain the agent base directory for some reason, then pass the `-skipRemoval` argument to the script. This argument ensures that only the Management Agent home from agent base directory is removed, but the agent base directory and the rest of the subdirectories are retained.

1. Invoke the AgentDeinstall.pl script:

```
$<AGENT_HOME>/perl/bin/perl <AGENT_
HOME>/sysman/install/AgentDeinstall.pl -agentHome <AGENT_
HOME>
```

For example, if you want to deinstall the Management Agent and also remove the agent base directory, then run the following command:

```
$/u01/app/Oracle/core/12.1.0.3.0/perl/bin/perl
/u01/app/Oracle/core/12.1.0.3.0/sysman/install/AgentDeinstall
.pl -agentHome /u01/app/Oracle/core/12.1.0.3.0/
```

For example, if you want to deinstall the Management Agent but NOT remove the agent base directory, then run the following command:

```
$/u01/app/Oracle/core/12.1.0.3.0/perl/bin/perl
/u01/app/Oracle/core/12.1.0.3.0/sysman/install/AgentDeinstall
.pl -agentHome /u01/app/Oracle/core/12.1.0.3.0/ -skipRemoval
```

2. Manually remove the targets, which were being monitored by the Management Agent you deinstalled, from the Enterprise Manager Cloud Control console.
3. Manually delete the agent base directory. For information on agent base directory, see [Section 2.3.5](#).

For UNIX platforms:

```
rm -rf <absolute_path_to_install_base_dir>
```

For Microsoft Windows platforms:

```
del <absolute_path_to_install_base_dir>
```

18.1.2.3 Deinstalling Shared Agent

To deinstall a Shared Agent, run the following command from the *Master Agent* home that is visible on the host where your *Shared Agent* is installed:

```
$<AGENT_HOME>/perl/bin/perl <AGENT_
HOME>/sysman/install/NFSAgentDeInstall.pl AGENT_INSTANCE_
HOME=<absolute_path_to_agent_instance_home> ORACLE_
HOME=<absolute_path_to_agent_home>
```

For example,

```
/home/john/software/oracle/agent/core/12.1.0.3.0/perl/bin/perl  
/home/john/software/oracle/agent/core/12.1.0.3.0/sysman/install/  
NFSAgentDeInstall.pl AGENT_INSTANCE_  
HOME=/home/john/software/oracle/agent/agent_inst ORACLE_  
HOME=/home/john/software/oracle/agent/core/12.1.0.3.0
```

Note: If you encounter an error while deinstalling the *Shared Agent*, then refer to [Section I.4](#).

18.1.2.4 Deinstalling Oracle Management Agent Installed Using an RPM File

To deinstall a Management Agent that was installed using a .rpm file, run the following command as a *root* user:

```
rpm -e <rpm_name>
```

Note: As a prerequisite, ensure that you have Resource Package Manager (RPM) installed on the host.

18.1.3 After You Deinstall

After you deinstall the Management Agent, follow these steps:

1. *(Only for Graphical Mode)* Verify whether the Oracle homes and other directories were successfully deinstalled. To do so, follow these steps:
 - a. Invoke the installation wizard by running the following command from the Management Agent home:

`<DVD>/runInstaller`
2. The Oracle homes you deinstalled are deregistered from the central inventory. However, some files might still remain in these Oracle homes. If they do, you can manually delete them.

You must also manually delete the auto-startup script called `gcstartup` which will be present under `/etc/init.d` directory.

Note: These auto-start scripts are not available on Microsoft Windows.

3. If you deinstalled on a Microsoft Windows platform, then follow these steps. Ensure that you are logged in as a user with Administrator privileges on that host.

Remove Entries from Microsoft Windows Registry

- a. Start the registry editor by selecting **Start** and then **Run**. Type `regedit` and click **OK**.
- b. In the Registry Editor window, in the left pane, expand **HKEY_LOCAL_MACHINE, SOFTWARE**, and then **Oracle**. Under the **Oracle** directory, delete the following:
 - (a) `KEY_agent12g n`
 - (b) `KEY_sbin12g n`

Note: Here, n refers to a numeral indicating the agent instance. For example, `KEY_sbin12g9` for the first agent installation.

- c. Expand **HKEY_LOCAL_MACHINE, SOFTWARE, Oracle**, and then **Sysman**. Under the **Sysman** directory, delete the Management Agent service. For example, `Oracleagent12g9Agent`.
- d. Expand **HKEY_LOCAL_MACHINE, SYSTEM, CurrentControlSet**, and then **Services**. Under the **Services** directory, delete the Management Agent keys.
- e. Expand **HKEY_LOCAL_MACHINE, SYSTEM, ControlSet002**, and then **Services**. Under the **Services** directory, delete the Management Agent service.
- f. Close the registry editor.

Clean Up Environment Settings

1. Open the Environment Variables window.

On Microsoft Windows NT, select **Start, Settings, Control Panel, System**, and then **Environment**.

On Microsoft Windows XP or 2000, select **Start, Settings, Control Panel, System, Advanced**, and then **Environment Variables**.
2. In the System Variables section, click the variable `PATH` and modify the value.
3. Delete Management Agent home.
4. Click **Apply** and then click **OK**.
5. Close the Control Panel window.
6. Restart the host.

18.2 Deinstalling or Undeploying Only Plug-ins from the Oracle Management Agent

If you want to deinstall or undeploy only the plug-ins from the Management Agent, and not the Management Agent itself, then use the Plug-ins page within the Enterprise Manager Cloud Control Console. For instructions, see the *Oracle Enterprise Manager Cloud Control Administrator's Guide*. **Do NOT use `runInstaller` to undeploy only the plug-ins.**

Deinstalling ADP and JVMD

This chapter describes how you can deinstall Application Dependency and Performance (ADP), and Java Virtual Machine Diagnostics (JVMD) in the Enterprise Manager Cloud Control environment.

In particular, this chapter covers the following:

- [Deinstallation Procedure for ADP](#)
- [Deinstallation Procedure for JVMD](#)

19.1 Deinstallation Procedure for ADP

This section consists of the following:

- [Removing ADP Engine](#)
- [Removing ADP Agents](#)

19.1.1 Removing ADP Engine

This section describes the methods to remove ADP Engines. It consists of the following:

- [Removing ADP Engine Using Application Performance Management Page](#)
- [Removing ADP Engine Manually](#)
- [Removing ADP Engine Manually Using ApmEngineSetup.pl](#)

19.1.1.1 Removing ADP Engine Using Application Performance Management Page

To remove the ADP Engine applications running on Managed Servers using the Application Performance Management page, perform the following steps:

1. From the **Setup** menu, select **Middleware Management**, then select **Application Performance Management**.
2. If you want to remove a single ADP Engine, on the Application Performance Management page, select the ADP Engine you want to remove, then click **Remove**.

If you want to remove more than one ADP Engine, on the Application Performance Management page, select the **ADP Engines** node, then click **Remove**.

3. On the Remove ADP Engines page, select the ADP Engines you want to remove.

4. For each ADP Engine you select, select **Remove WebLogic Managed Server**, if you want to remove the WebLogic Managed Server on which the ADP Engine is deployed.
5. Specify values for **Admin WebLogic Host Credentials** and **Admin WebLogic Credentials**.

Admin WebLogic Host Credentials are the host credentials for the host on which the WebLogic Administration Server (for the Enterprise Manager WebLogic domain) is deployed. Admin WebLogic Credentials are the credentials for the Administration Server of the Enterprise Manager WebLogic domain.

6. Click **Remove**.

19.1.1.2 Removing ADP Engine Manually

To remove the ADP Engine application running on a Managed Server manually, perform the following steps:

1. In Cloud Control, from the **Targets** menu, select **Middleware**.
2. On the Middleware page, from the **Middleware Features** menu, select **Application dependency and Performance**.
The Application Dependency and Performance is displayed.
3. From the **Registration** tab, select the ADP Engine application, then click **Remove**.
4. Log in to the WebLogic Administration Console of the Enterprise Manager domain.
5. On the Home Page, click **Servers**.
6. From the Summary of Servers page, click the **Control** tab, then select the ADP Engine Servers.
7. From the **Shutdown** menu, select **Force Shutdown Now** to stop the servers.
8. Click the Lock and Edit button present in the WebLogic Administration console.
9. Click the **Configuration** tab, select **ADP Engine Servers**, then click **Delete**.
10. Undeploy the ADP applications. For example, ADPManager_EMGC_ADPMANAGER1 for ADP.
11. Connect to the host machine where the Managed Server was present, and navigate to the following location to manually delete the Managed Server:

```
$DOMAIN_HOME/<ADP_managed_server>
```

Where \$DOMAIN_HOME is the location of the Enterprise Manager Cloud Control domain.

19.1.1.3 Removing ADP Engine Manually Using ApmEngineSetup.pl

You can remove ADP Engine manually, using the `ApmEngineSetup.pl` script. You can run this script in the following ways:

- In interactive mode, where you are prompted for input details in an interactive manner
- In silent mode, where you specify all the input details using a properties file

Important: You can use the `ApmEngineSetup.pl` script to remove ADP Engine only on a host that is running the OMS, and not on a remote host.

To remove ADP Engine manually using the `ApmEngineSetup.pl` script, follow these steps:

1. Navigate to the following location on the OMS host:

```
$<MIDDLEWARE_HOME>/plugins/oracle.sysman.emas.oms.plugin_
12.1.0.4.0/archives/jvmd/deployment_Scripts/engine/
```

2. View the `README.txt` file, for information on using the `ApmEngineSetup.pl` script.
3. Run the `ApmEngineSetup.pl` script.

If you want to run the `ApmEngineSetup.pl` script in interactive mode, such that you are prompted for the input details, use the following command:

```
perl ApmEngineSetup.pl
```

Ensure that you specify the operation as `remove`, and the Engine Type as `ADP`.

If you want to run the `ApmEngineSetup.pl` script in silent mode, specify all the input details in a properties file, then use the following command:

```
perl ApmEngineSetup.pl -silent -file <properties_file_name> -password
<password>
```

`<properties_file_name>` is the name of the properties file where the ADP Engine and operation details are provided. `<password>` is the WebLogic console password.

To learn how to specify the input details in a properties file, view the sample properties file `SAMPLE_engine.properties`.

19.1.2 Removing ADP Agents

This section describes the methods to remove ADP Agents. It consists of the following:

- [Removing ADP Agents Using Application Performance Management Page](#)
- [Removing ADP Agents Deployed to Targets Manually](#)

19.1.2.1 Removing ADP Agents Using Application Performance Management Page

To remove the ADP Agents (that are deployed on monitored WebLogic domains) using the Application Performance Management page, perform the following steps:

1. From the **Setup** menu, select **Middleware Management**, then select **Application Performance Management**.
2. On the Application Performance Management page, under the Application Performance Management Agents section, click **Manage Diagnostics Agents**.

Note: If no active JVMD or ADP Engines are present, and no JVMD or ADP Agents are deployed, the **Manage Diagnostics Agents** button is disabled.

3. For **Operation**, select **Remove**.

If you select **Expand All** from the **View** menu, you can view the target name, target type, target host, target status, platform, and so on of all the discovered WebLogic Administration Servers and Managed Servers (part of all discovered WebLogic domains).

Select the ADP Agents you want to remove. Click **Next**.

4. On the Target Credentials page, for each WebLogic domain, specify a value for **Oracle WebLogic Administration Server Host Credentials** and **Oracle WebLogic Domain Credentials**, then click **Apply**.

Oracle WebLogic Administration Server Host Credentials are the host credentials for the host on which the Management Agent that is monitoring the selected WebLogic domain is running. Oracle WebLogic Domain Credentials are the credentials for the Administration Server of the selected WebLogic domain.

Click **Next**.

5. On the ADP Agents Configurations page, specify values for the **WebLogic Home** and **Middleware Home** fields.

These fields are displayed only if their values could not be obtained internally. If the application is able to obtain the values for WebLogic Home and Middleware Home internally, the ADP Agents Configurations page is skipped and you are directly taken to the Enterprise Manager OMS Credentials page from the Target Credentials page.

6. On the Enterprise Manager OMS Credentials page, specify a value for **Oracle Enterprise Manager WebLogic Administration Server Host Credentials**, and **Oracle Enterprise Manager WebLogic Domain Credentials**.

Oracle Enterprise Manager WebLogic Administration Server Host Credentials are the host credentials of the OMS host. The Oracle Enterprise Manager WebLogic Domain Credentials are the domain credentials of the Enterprise Manager WebLogic domain.

Click **Next**.

7. On the Review page, review all the information, then click **Remove**.

19.1.2.2 Removing ADP Agents Deployed to Targets Manually

To manually remove the ADP Agent deployed to a target, perform the following steps:

1. In Cloud Control, from the **Targets** menu, select **Middleware**.
2. On the Middleware page, from the **Middleware Features** menu, select **Application dependency and Performance**.
The Application Dependency and Performance is displayed.
3. From the **Configuration** tab, select the desired ADP Engine application on which the ADP Agents have been deployed.
4. Expand the **ADP Engine** menu, then select **Resource Configuration**.
5. From the Resource table, select the ADP Agent name, click **Edit Resource**, then click **Deploy**.
6. From the Deploy Parameters table, select the servers from which you want to undeploy the ADP Agents. Change the default menu selection from **Deploy** to:
 - **Remove**, to erase all the ADP Agent files from the Managed Servers.

- **Disable**, to remove the ADP Agent startup arguments from the Managed Servers.

Note: Select the **Server Started by Node Manager** option only when the node manager is used.

19.2 Deinstallation Procedure for JVM D

This section consists of the following:

- [Removing JVM D Engine](#)
- [Removing JVM D Agents](#)

19.2.1 Removing JVM D Engine

This section describes the methods to remove JVM D Engines. It consists of the following:

- [Removing JVM D Engine Using Application Performance Management Page](#)
- [Removing JVM D Engine Manually](#)
- [Removing JVM D Engine Manually Using ApmEngineSetup.pl](#)

19.2.1.1 Removing JVM D Engine Using Application Performance Management Page

To remove the JVM D Engine applications running on Managed Servers using the Application Performance Management page, perform the following steps:

1. From the **Setup** menu, select **Middleware Management**, then select **Application Performance Management**.
2. If you want to remove a single JVM D Engine, on the Application Performance Management page, select the JVM D Engine you want to remove, then click **Remove**.

If you want to remove more than one JVM D Engine, on the Application Performance Management page, select the **JVM Diagnostics Engines** node, then click **Remove**.

3. On the Remove JVM D Engines page, select the JVM D Engines you want to remove.
4. For each JVM D Engine you select, select **Remove WebLogic Managed Server**, if you want to remove the WebLogic Managed Server on which the JVM D Engine is deployed.
5. Specify values for **Admin WebLogic Host Credentials** and **Admin WebLogic Credentials**.

Admin WebLogic Host Credentials are the host credentials for the host on which the WebLogic Administration Server (for the Enterprise Manager WebLogic domain) is deployed. Admin WebLogic Credentials are the credentials for the Administration Server of the Enterprise Manager WebLogic domain.

6. Click **Remove**.

19.2.1.2 Removing JVMD Engine Manually

To remove the JVMD Engine application running on a Managed Server manually, perform the following steps:

1. Log in to the WebLogic Administration console of the Enterprise Manager Cloud Control domain.
2. On the Home Page, click **Deployments**.
3. Select the JVMD applications (for example, jammanagerEMGC_JVMDMANAGER1, jammanagerEMGC_JVMDMANAGER2). From the **Stop** menu, select **Force Stop Now**.
4. Click the Lock and Edit button present in the WebLogic Administration console.
5. After the applications are stopped, select the same applications, then click **Delete**.
6. Click **Home** to go back to the WebLogic Administration home page. From the Environment table, select **Servers**.
7. On the Summary of Servers page, select the **Control** tab, then select the JVMD Engine servers that need to be shut down.
8. From the **Shutdown** menu, select **Force Shutdown Now** to stop the servers.
9. Click the Lock and Edit button present in the WebLogic Administration console.
10. Click the **Configuration** tab, select the JVMD Engine servers, then click **Delete**.

19.2.1.3 Removing JVMD Engine Manually Using ApmEngineSetup.pl

You can remove JVMD Engine manually, using the ApmEngineSetup.pl script. You can run this script in the following ways:

- In interactive mode, where you are prompted for input details in an interactive manner
- In silent mode, where you specify all the input details using a properties file

Important: You can use the ApmEngineSetup.pl script to remove JVMD Engine only on a host that is running the OMS, and not on a remote host.

To remove JVMD Engine manually using the ApmEngineSetup.pl script, follow these steps:

1. Navigate to the following location on the OMS host:
`<MIDDLEWARE_HOME>/plugins/oracle.sysman.emas.oms.plugin_12.1.0.4.0/archives/jvmd/deployment_Scripts/engine/`
2. View the README.txt file, for information on using the ApmEngineSetup.pl script.
3. Run the ApmEngineSetup.pl script.

If you want to run the ApmEngineSetup.pl script in interactive mode, such that you are prompted for the input details, use the following command:

```
perl ApmEngineSetup.pl
```

Ensure that you specify the operation as `remove`, and the Engine Type as `JVMD`.

If you want to run the ApmEngineSetup.pl script in silent mode, specify all the input details in a properties file, then use the following command:

```
perl ApmEngineSetup.pl -silent -file <properties_file_name> -password
<password>
```

<properties_file_name> is the name of the properties file where the JVMD Engine and operation details are provided. <password> is the WebLogic console password.

To learn how to specify the input details in a properties file, view the sample properties file `SAMPLE_engine.properties`.

19.2.2 Removing JVMD Agents

This section describes the methods to remove JVMD Agents. It consists of the following:

- [Removing JVMD Agents Using Application Performance Management Page](#)
- [Removing JVMD Agents Deployed to Targets Manually](#)

19.2.2.1 Removing JVMD Agents Using Application Performance Management Page

To remove the JVMD Agents (that are deployed on monitored WebLogic domains) using the Application Performance Management page, perform the following steps:

1. From the **Setup** menu, select **Middleware Management**, then select **Application Performance Management**.
2. On the Application Performance Management page, under the Application Performance Management Agents section, click **Manage Diagnostics Agents**.

Note: If no active JVMD or ADP Engines are present, and no JVMD or ADP Agents are deployed, the **Manage Diagnostics Agents** button is disabled.

3. For **Operation**, select **Remove**.

If you select **Expand All** from the **View** menu, you can view the target name, target type, target host, target status, platform, and so on of all the discovered WebLogic Administration Servers and Managed Servers (part of all discovered WebLogic domains).

Select the JVMD Agents you want to remove. Click **Next**.

4. On the Target Credentials page, for each WebLogic domain, specify a value for **Oracle WebLogic Administration Server Host Credentials** and **Oracle WebLogic Domain Credentials**, then click **Apply**.

Oracle WebLogic Administration Server Host Credentials are the host credentials for the host on which the Management Agent that is monitoring the selected WebLogic domain is running. Oracle WebLogic Domain Credentials are the credentials for the Administration Server of the selected WebLogic domain.

Click **Next**.

5. On the JVMD Agents Configurations page, specify values for the **WebLogic Home** and **Middleware Home** fields.

These fields are displayed only if their values could not be obtained internally. If the application is able to obtain the values for WebLogic Home and Middleware Home internally, the JVMD Agents Configurations page is skipped and you are directly taken to the Review page from the Target Credentials page.

6. On the Review page, review all the information, then click **Remove**.

19.2.2.2 Removing JVMD Agents Deployed to Targets Manually

To manually remove the JVMD Agent deployed to a target, perform the following steps:

1. Log in to the Administration Console of the target server.
2. On the Home Page, click **Deployments**.
3. Select the JVMD Agent application (`javadiagnosticagent.ear` or `jamagent.war`). From the **Stop** menu, select **Force Stop Now**.
4. After the applications are stopped, select the same applications, then click **Delete**.
5. Log in to Enterprise Manager Cloud Control.
6. In Cloud Control, from the **Targets** menu, select **Middleware**.
7. On the Middleware page, in the Search table, search for targets of type **Java Virtual Machine**, select the target corresponding to the server, then click **Remove**.

Removing Standby Oracle Management Services

This chapter describes how to remove standby Oracle Management Services (OMS) from a Level 4 High Availability (HA) configuration. The following OMS removal scenarios are covered:

- [Removing Additional Standby OMS Instances](#)
- [Removing the First Standby OMS](#)

20.1 Removing Additional Standby OMS Instances

1. Deconfigure and delete an additional standby OMS instance by running the following command from the OMS home:

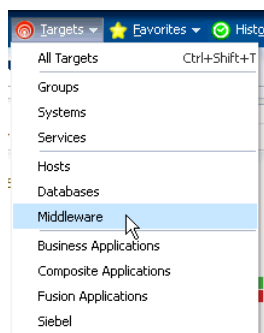
```
$<OMS_HOME>/bin/omsca delete -OMSNAME <oms_name>
```

When prompted, enter the repository login credentials.

Note: Run this command on each of the additional standby OMS instances.

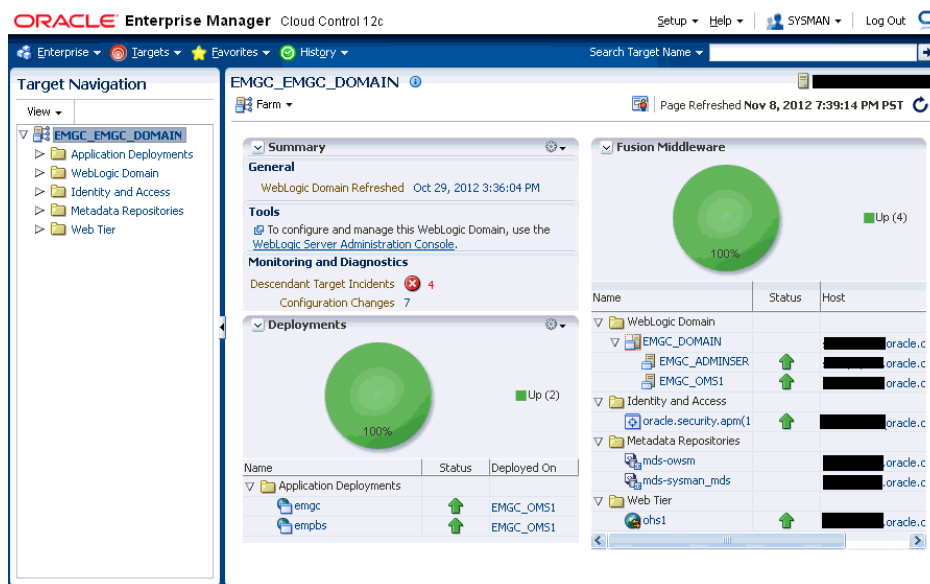
2. From the Enterprise Manager console, refresh the Weblogic domain.
 1. From the **Targets** menu, select **Middleware**.

Figure 20–1 *Middleware Menu*



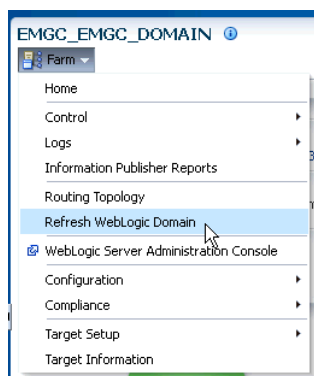
2. Click the **WebLogic Domain** you want to refresh. The domain home page displays.

Figure 20–2 Domain Home Page

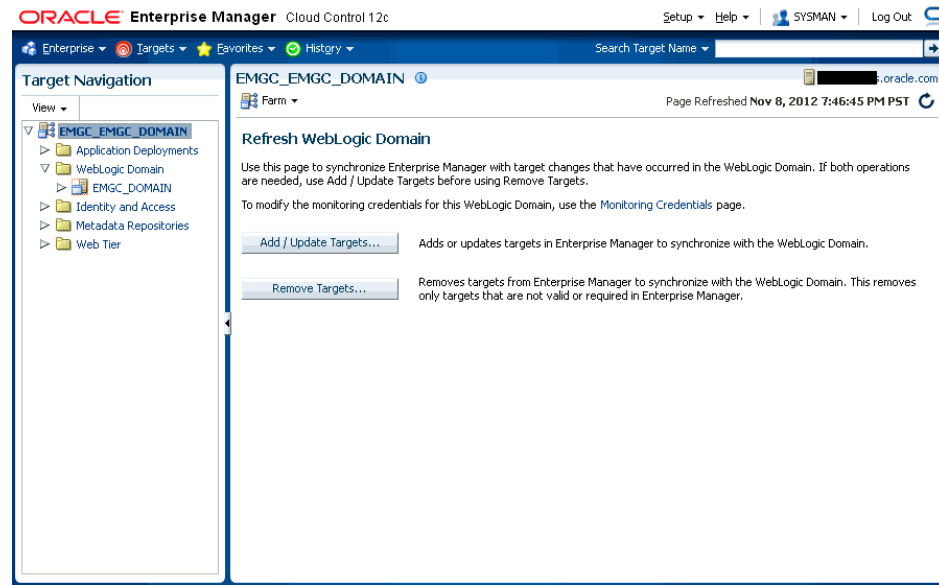


3. From either the **Farm** or **WebLogic Domain** menu, select **Refresh WebLogic Domain**.

Figure 20–3 Refresh WebLogic Domain



Enterprise Manager displays available **Refresh WebLogic Domain** options.

Figure 20–4 Refresh WebLogic Domain

4. Click **Add/Update Targets**. The Management Agent refreshes by connecting to the Administration Server. The Administration Server must be up for the refresh to occur.
Click **Close** on the Confirmation page. Cloud Control will search the domain for new and modified targets.
3. Delete the OMS target associated with the OMS.
 1. From the **Target Navigation** area, click the target associated with the additional standby OMS you deconfigured earlier.
 2. From the **WebLogic** menu, select **Target Setup** and then **Remove Target**. Enterprise Manager displays a Warning dialog asking if you wish to continue. Click **Yes**.
4. Repeat this deinstallation procedure for all remaining additional standby OMSs.

20.2 Removing the First Standby OMS

Important: DO NOT attempt to deinstall the first standby OMS if there are any remaining additional standby OMSs within your environment. See ["Removing Additional Standby OMS Instances"](#) on page 20-1 for instructions on removing additional standby OMSs.

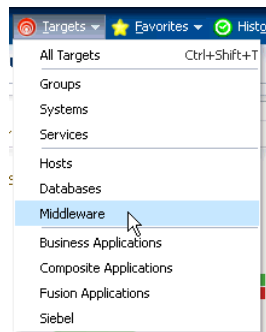
1. Deconfigure and delete the first standby OMS instance by running the following command from the OMS home:

```
$<OMS_HOME>/bin/omsca -delete -full
```

Note: You are prompted to confirm your action, and furnish the AdminServer credentials and the repository database details such as the database host name, listener port, SID, and password. Once you provide the required details, the command automatically stops the OMS, Oracle WebLogic Server, and also Oracle WebTier.

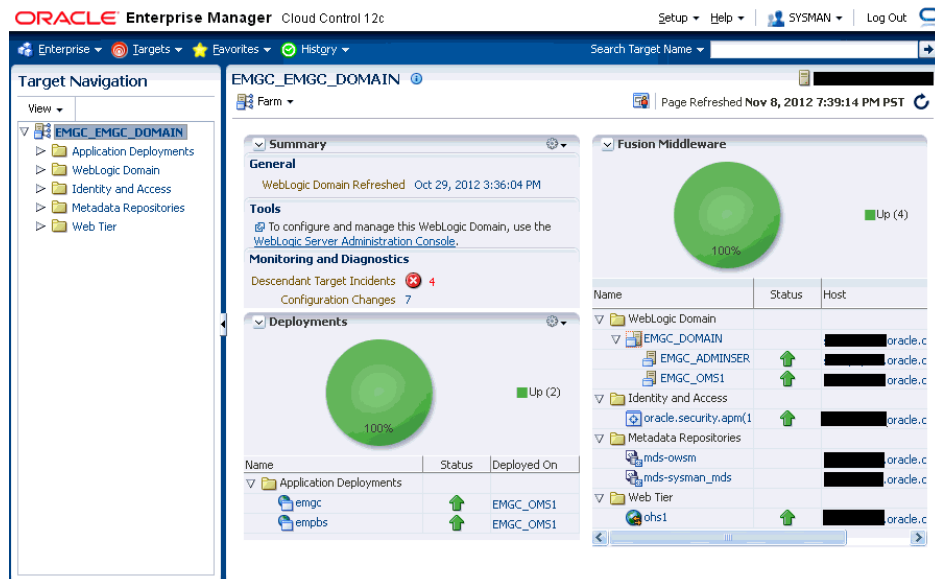
2. From the Enterprise Manager console, refresh the Weblogic domain.
 1. From the **Targets** menu, select **Middleware**.

Figure 20–5 Middleware Menu

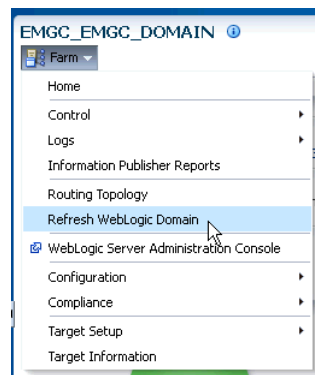


2. Click the **WebLogic Domain** you want to refresh. The domain home page displays.

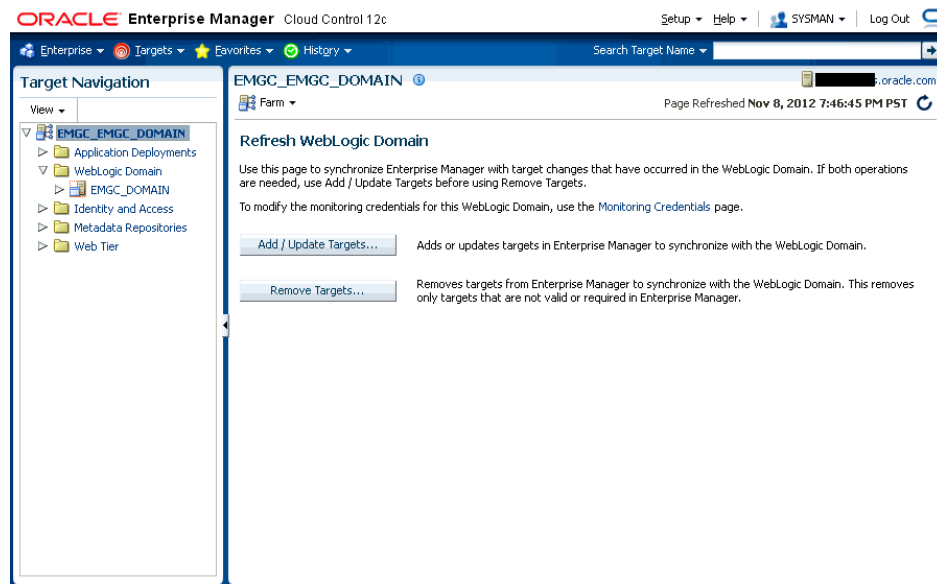
Figure 20–6 Domain Home Page



3. From either the **Farm** or **WebLogic Domain** menu, select **Refresh WebLogic Domain**.

Figure 20–7 Refresh WebLogic Domain

Enterprise Manager displays available **Refresh WebLogic Domain** options.

Figure 20–8 Refresh WebLogic Domain

4. Click **Add/Update Targets**. The Management Agent refreshes by connecting to the Administration Server. The Administration Server must be up for the refresh to occur.
Click **Close** on the Confirmation page. Enterprise Manager will search the domain for new and modified targets.
3. Delete the OMS target associated with the OMS.
 1. From the **Target Navigation** area, click the target associated with the first standby OMS you deconfigured earlier.
 2. From the **WebLogic** menu, select **Target Setup** and then **Remove Target**. Enterprise Manager displays a Warning dialog asking if you wish to continue. Click **Yes**.

Part VII

Appendixes

This part contains the following appendixes:

- [Appendix A, "Understanding the Enterprise Manager Directory Structure"](#)
- [Appendix B, "Installation and Configuration Log Files"](#)
- [Appendix E, "Using RepManager Utility"](#)
- [Appendix F, "Collecting OCM Data Using Oracle Harvester"](#)
- [Appendix G, "Enabling Enterprise Manager Accessibility Features"](#)
- [Appendix H, "Configuring Targets for Failover in Active/Passive Environments"](#)
- [Appendix I, "Troubleshooting"](#)

Understanding the Enterprise Manager Directory Structure

Before you perform maintenance and advanced configuration tasks, you must be familiar with the directories and files that are copied to disk when you install Enterprise Manager. Understanding where specific files are located can help you if you need to troubleshoot installation or configuration problems.

When installing Enterprise Manager, if you select a location that does not contain WebLogic Server, then JDK will be installed in the `jdk16` directory before installation of WebLogic Server.

Use the following sections to become familiar with the directories that are created on your disk when you install Enterprise Manager:

- Understanding the Enterprise Manager Directories Installed with Oracle Enterprise Manager Cloud Control 12c
- Understanding the Enterprise Manager Directories Installed with an Oracle Management Service
- Understanding the Enterprise Manager Directories Installed with Management Agent

A.1 Understanding the Enterprise Manager Directories Installed with Oracle Enterprise Manager Cloud Control 12c

When you install Oracle Enterprise Manager Cloud Control 12c, you install the Oracle Management Service. With the Oracle Management Service, you install the following Oracle home directories:

- Oracle Management Service home directory
- Middleware WebTier home directory
- Middleware Common home directory
- Oracle Management Service Instance home directory
- Oracle Management Agent home directory
- Oracle Management Agent Instance home directory
- Oracle Management Service Plug-in homes
- Oracle Management Agent Plug-in homes
- Oracle Business Intelligence Publisher home (Optional)

A.1.1 About the Oracle Management Service Home Directory

The Oracle Management Service is a J2EE application that is installed and deployed using the Oracle WebLogic Server.

The installation procedure installs the Enterprise Manager components within the Cloud Control Home, including the Oracle Management Service.

Information about the directories that are specific to the Fusion Middleware installation can be found in the Fusion Middleware documentation.

A.1.2 About the Oracle Management Agent Home (AGENT_HOME) Directory

The Oracle Management Agent Home (AGENT_HOME) directory contains all the binaries required to configure and run the Oracle Management Agent on the host.

This directory serves as the Oracle Home for the Oracle Management Agent.

Information about the directories that are specific to the Fusion Middleware installation can be found in the Fusion Middleware documentation.

A.1.3 About Business Intelligence Publisher Home Directory

The Business Intelligence Publisher is a J2EE application that is installed and configured as described in [Chapter 15](#).

A.1.4 Summary of the Important Directories in the Oracle Management Service Home

[Figure A–1](#) shows some of the important directories you should be familiar with in a typical Cloud Control installation. You can use this information as you begin to maintain, troubleshoot, and configure the Oracle Management Service installation.

Figure A–1

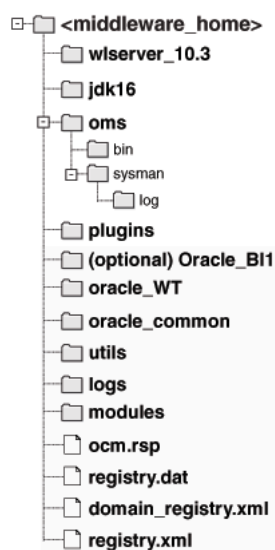


Table A–1 Directories Installed with Enterprise Manager

Directory	Description
wlsrserver_10.3, logs, utils, modules	These directories contain Fusion Middleware files.

Table A–1 (Cont.) Directories Installed with Enterprise Manager

Directory	Description
jdk16	This directory contains JDK configuration files.
oms	This directory contains OMS configuration files. For more information, see Section 10.2.2.
plugins	This directory contains metadata plug-ins configuration files installed on the OMS.
agent	This directory contains agent configuration files. For more details, see Section 10.2.3.
[optional] Oracle_BI1	This directory contains the Oracle Business Intelligence Publisher configuration files.
oracle_WT	This directory contains Oracle WebTier configuration files.
oracle_common	This directory contains common files used by OMS, Oracle WebTier, and WebLogic Server directories.

A.2 Understanding the Enterprise Manager Directories Installed with Management Service

Table A–2 describes in detail the Oracle Management Service directories installed with Oracle Management Service. In the table, ORACLE_HOME refers to the Oracle Management Service home directory in which the Oracle Management Service is installed and deployed.

Table A–2 Important Directories in the Management Service Oracle Home

Directory	Description
ORACLE_HOME/bin	The bin directory in the Management Service home contains commands used to control the components of the Cloud Control installation.
OMS_INSTANCE_HOME/WebTierIH1	This directory contains WebTier instance Oracle Home corresponding to EMGC_OMS#.
OMS_INSTANCE_HOME/NodeManager	This directory contains WebLogic Node Manager properties, logs, and domain information.
OMS_INSTANCE_HOME/em	This is the OMS instance directory and contains emgc.properties and Enterprise Manager log files.
OMS_INSTANCE_HOME/user_projects	This directory contains EMGC_ADMINSERVER and EMGC_OMS# domains and their logs.
ORACLE_HOME/sysman/log	This directory contains schema log files. The repository log files are under sysman/log/schemamanager. The install logs are under ORACLE_HOME/cfgtoollogs. The operation logs are under OMS_INSTANCE_HOME/em/EMGC_OMS1/sysman/log.

A.3 Understanding the Enterprise Manager Directories Installed with Management Agent

The Oracle Management Agent is installed automatically when you install Oracle Management Service. This local instance of the Oracle Management Agent gathers management information about the targets on the Oracle Management Service host. You can then manage those targets, such as the host itself, from the Cloud Control Console.

You can install additional Oracle Management Agents using different installation methods. This enables you to install the Oracle Management Agent on the hosts throughout your enterprise. The Oracle Management Agent can then gather management data about the targets on each host so those targets can be managed from the Cloud Control Console.

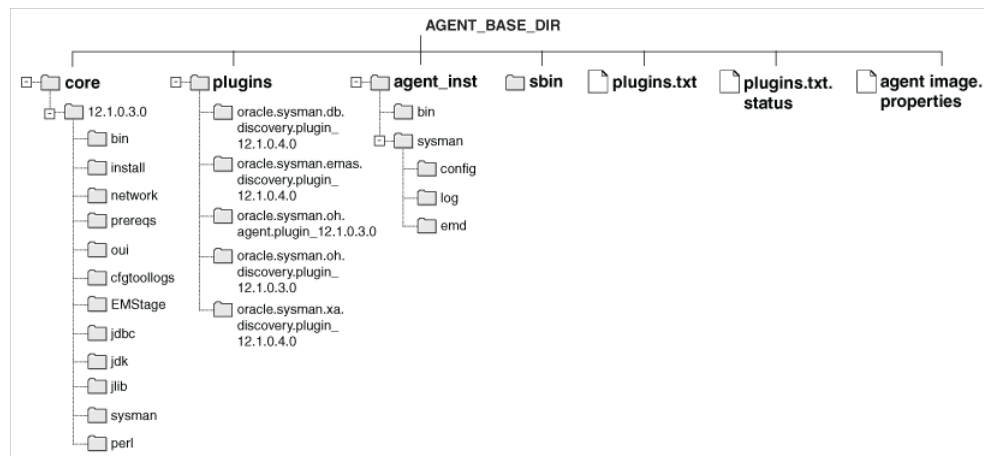
Specifically, the Oracle Management Agent files are installed into the same directory structure shown in the agent directory when you install the Oracle Management Service ([Figure A-1](#)).

The agent directory structure, when you install a standalone agent or install the OMS is the same. The AGENT_BASE_DIR is the directory where agent is installed and contains the following main directories:

- AGENT_HOME
- AGENT_INSTANCE_HOME
- SBIN_HOME
- PLUGIN_HOME

The directory that contains the files required to run the Oracle Management Agent is referred to as the AGENT_INSTANCE_HOME directory. For example, to start or stop an Oracle Management Agent, you use the emctl command located in the bin directory of the AGENT_INSTANCE_HOME. Similarly, to configure files for the Oracle Management Agent, you modify the configuration files in the sysman/config directory of the AGENT_INSTANCE_HOME. See [Figure A-2](#) for the agent directory structure.

Figure A-2 Agent Directory Structure



A.3.1 Summary of the Important Directories in the Oracle Management Agent Home

[Table A-3](#) describes some of the important agent directories.

Table A-3 Important Directories in Oracle Management Agent Home

Directory	Description
AGENT_HOME	<p>The AGENT_HOME directory contains all the binaries required to configure and run the Oracle Management Agent on this host.</p> <p>The default AGENT_HOME location is AGENT_BASE_DIR/core/12.1.0.2.0.</p> <p>This directory serves as the Oracle Home for the Oracle Management Agent.</p>
AGENT_HOME/bin	This directory contains binaries for the Oracle Management Agent.
AGENT_HOME/install	This directory contains installation-related files for deploying the agent.
AGENT_HOME/prereqs	This directory contains prerequisite files for EMPrereqKit.
AGENT_HOME/oui	This directory contains files related to the installer framework.
AGENT_HOME/cfgtoollogs	This directory contains agent deployment and configuration log files.
AGENT_HOME/EMStage	This directory is used by the provisioning framework for provisioning activities.
AGENT_HOME/sysman/admin	This directory contains the files used by the Oracle Management Agent to define agent core target types (such as databases, hosts, and so on), to run configuration scripts, and other administrative tasks.
AGENT_INSTANCE_HOME	<p>The AGENT_INSTANCE_HOME directory contains agent-related configuration files after agent is installed and configured.</p> <p>The default AGENT_INSTANCE_HOME location is AGENT_BASE_DIR/agent_inst.</p>
AGENT_INSTANCE_HOME/bin	<p>The AGENT_INSTANCE_HOME/bin directory in the Cloud Control Home contains the emctl command that controls the Oracle Management Agent for this host.</p> <p>You use the following emctl commands in this directory to start and stop the Oracle Management Agent on this host:</p> <pre><AGENT_INSTANCE_HOME>/bin/emctl start agent</pre> <pre><AGENT_INSTANCE_HOME>/bin/emctl stop agent</pre>
AGENT_INSTANCE_HOME/sysman/config	This directory contains the configuration files for the Oracle Management Agent. For example, this is where Enterprise Manager stores the emd.properties file. The emd.properties file defines settings such as the Oracle Management Service upload URL for this particular agent.
AGENT_INSTANCE_HOME/sysman/log	This directory contains the log files for the Oracle Management Agent.
AGENT_INSTANCE_HOME/sysman/emd	The emd directory contains information about targets discovered on hosts.
SBIN_HOME	This directory contains set UIDs for the agent. The default location is AGENT_BASE_DIR/sbin.
PLUGIN_HOME	<p>This directory contains all the discovery and monitoring plug-ins required for the agent.</p> <p>The default location is AGENT_BASE_DIR/plugins.</p>

A.3.2 Understanding the Oracle Management Agent Directory Structure in Windows

When you install the Oracle Management Agent on a Windows system, the directory structure of the `AGENT_HOME` directory is the same as the directory structure for installations on a UNIX system.

A.4 Identifying the Agent Instance Home When Using the emctl Command

When you install Cloud Control, the resulting directory structure can often include multiple subdirectories with the same name. For example, you can have a `bin` directory within the `agent_instance_home` directory. Use the `emctl` command within the `agent_instance_home/bin` directory to control the Oracle Management Agent.

In addition, you can have a `bin` directory within the Oracle Management Service Oracle home. Use the `emctl` command in this directory to control the Oracle Management Service.

To quickly identify the Agent Instance home that is controlled by the files in a particular `bin` directory, use the following command:

```
$PROMPT> emctl getemhome
```

This command displays the path to the current Agent Instance home that will be affected by commands executed by this instance of the `emctl` command.

Installation and Configuration Log Files

This appendix lists the locations of the various log files that are created during the prerequisites check, installation, and configuration phases of Enterprise Manager Cloud Control components.

In particular, this appendix covers the following:

- [Enterprise Manager Cloud Control Installation Logs](#)
- [Add Host Log Files](#)
- [Manual Management Agent Installation Logs](#)
- [Additional OMS Installation Logs](#)

B.1 Enterprise Manager Cloud Control Installation Logs

This section describes the following log files that are created while installing Enterprise Manager Cloud Control:

- [Installation Logs](#)
- [Configuration Logs](#)

B.1.1 Installation Logs

The following are the installation logs, which provide complete information on the installation status:

- `<ORACLE_INVENTORY_HOME>/logs/installActions<timestamp>.log`
- `<ORACLE_HOME>/cfgtoollogs/oui/installActions<timestamp>.log`

Note: The `installActions` log file is located in the `<ORACLE_INVENTORY_HOME>` directory by default. This log file will be copied on to the above-mentioned Oracle home location after the installation is complete.

B.1.2 Configuration Logs

This section describes the following configuration logs:

- [General Configuration Logs](#)
- [Repository Configuration Logs](#)
- [Secure Logs](#)

B.1.2.1 General Configuration Logs

The Oracle Management Service (OMS) configuration logs are located in the following location of the Oracle home of the OMS.

```
<ORACLE_HOME>/cfgtoollogs/omsca
```

Table B–1 lists the configuration logs for different installation types.

Table B–1 General Configuration Logs

Installation Type	Location
Install a new or Upgrade Enterprise Manager system	<ul style="list-style-type: none"> ▪ <ORACLE_HOME>/cfgtoollogs/cfgfw/CfmLogger<timestamp>.log ▪ <ORACLE_HOME>/cfgtoollogs/cfgfw/oracle.sysman.top.oms.<timestamp>.log <p>Note: <ORACLE_HOME> refers to the Oracle home of the OMS.</p>
Add an additional Management Service	<ul style="list-style-type: none"> ▪ <ORACLE_HOME>/cfgtoollogs/omsca/logs/omsca<timestamp>.log ▪ <ORACLE_HOME>/cfgtoollogs/cfgfw/oracle.sysman.top.oms.<timestamp>.log <p>Note: <ORACLE_HOME> refers to the Oracle home of the OMS.</p>
Install Oracle Management Agent	<ul style="list-style-type: none"> ▪ <ORACLE_HOME>/cfgtoollogs/cfgfw/CfmLogger ▪ <ORACLE_HOME>/cfgtoollogs/cfgfw/oracle.sysman.top.agent.<timestamp>.log <p>Note: <ORACLE_HOME> refers to the Oracle home of the Management Agent.</p>

B.1.2.2 Repository Configuration Logs

This section describes the following repository configuration logs:

- [SYSMAN Schema Operation Logs](#)
- [MDS Schema Operation Logs](#)

B.1.2.2.1 SYSMAN Schema Operation Logs

The SYSMAN schema operation logs are available in the following location of the Oracle home of the OMS. Listed in this directory is an overall log file, `emschema.log`, which logs all the actions performed by all the instances of RepManager run.

```
$<ORACLE_HOME>/sysman/log/schemanager/
```

In this location, for each run of RepManager, a new subdirectory is created based on the time at which the RepManager was run.

For example, if the RepManager was run and an instance was created at 09/29/2007 12:50PM, then the following subdirectory is created.

```
$<ORACLE_HOME>/sysman/log/schemanager/m_092907_1250_PM/
```

An instance of RepManager (or equivalently RepManager) can have schema actions, mainly CREATE, DROP, UPGRADE, TRANSX, and RESUME_RETRY. For each action, a subdirectory is created.

For example, if a CREATE action is performed by a RepManager instance at 09/29/2006 12:51PM, then the following subdirectory is created. Listed under this subdirectory are RCU-related log files and emschema.log.CREATE log file that logs the CREATE action-specific messages.

```
$<ORACLE_HOME>/sysman/log/schemamanager/m_092907_1250_PM/m_092907_1251PM.CREATE/
```

In general, in \$<ORACLE_HOME>/sysman/log/schemamanager/m_<time-stamp>/m_<time-stamp>.<schema-action>, the following files are created:

- RCU per component (i.e. init, common, modify, drop, config, outofbox, preupgrade log)
- RCU log
- Schema action-specific RCU logs
- TransX action-specific log (emrep_config.log)

If the any of the schema operations (CREATE/UPGRADE/PREUPGRADE/DROP) fail in SQL execution, and if you retry the operation by clicking **Retry**, then a separate subdirectory titled m_<time-stamp>.RESUME_RETRY is created.

The following shows the overall directory structure of repository operation logs for different schema actions:

```
$<ORACLE_HOME>/sysman/log/schemamanager
    emschema.log
    m_030210_0349_AM
        m_030210_0325_AM.TRANSX
            emrep_config.log
            emschema.log.TRANSX
    m_030210_0438_AM
        m_030210_0438_AM.DROP (Same structure for Drop and Dropall actions)
            rcu.log
            emschema.log.DROP
            em_repos_drop.log
    m_030210_0450_AM
        m_030210_0450_AM.CREATE
            custom_comp_create_tbs.log
            em_repos_common.log
            em_repos_init.log
            emrep_config.log.3
            emrep_config.log.2
            emrep_config.log.1
            emrep_config.log
            emschema.log
            rcu.log
            emschema.log.CREATE
            em_repos_config.log
    m_030210_1006_PM
        m_030210_1006_PM.RESUME_RETRY
            emrep_config.log.3
            emrep_config.log.2
            emrep_config.log.1
            emrep_config.log
            emschema.log
            rcu.log
            emschema.log.RESUME_RETRY
            em_repos_modify.log
    m_030210_1021_PM
        m_030210_1021_PM.UPGRADE
```

```
em_repos_init.log
emrep_config.log.3
emrep_config.log.2
emrep_config.log.1
emrep_config.log
emschema.log
rcu.log
emschema.log.UPGRADE
em_repos_modify.log
m_030210_1100_PM
  m_030210_1100_PM.PREUPGRADE
    em_repos_preupgrade.log
    emschema.log.PREUPGRADE
    rcu.log
    em_repos_init.log
    emrep_config.log.3
    emrep_config.log.2
    emrep_config.log.1
    emrep_config.log
    em_repos_common.log
m_030210_1125_PM
  m_030210_1125_PM.MY_ORACLE_SUPPORT
    emschema.log.MY_ORACLE_SUPPORTm_030210_1135_PM
  m_030210_1135_PM.PLUGINPURGE
    emschema.log.PLUGINPURGE
em_repos_pluginpurge.log
rcu.log
```

B.1.2.2.2 EMPrereqKit Logs

For EMPrereqKit, the logs are available at the <oraInventoryLoc>/logs/ location.

The details of execution of the prerequisites per prerequisite components location is available at:

```
<oraInventoryLoc>/logs/emdbprereqs/LATEST/repository.log or
emprereqkit.log
```

The details of execution of the EMPrereqkit is available at:

```
<oraInventoryLoc>/logs/emdbprereqs/LATEST/emprereqkit.log
```

The errors are located at

```
<oraInventoryLoc>/logs/emdbprereqs/LATEST/emprereqkit.err.log
```

B.1.2.2.3 MDS Schema Operation Logs

MDS Schema Creation Log

For MDS schema creation operation, the following log is available in the Oracle home of the OMS:

```
$<ORACLE_HOME>/cfgtoollogs/cfgfw/emmdscreate_<timestamp>.log
```

For more information, review the following logs from the Oracle home of the OMS:

```
$<ORACLE_HOME>/sysman/log/schemamanager/m_<timestamp>/m_
<timestamp>.CREATE/mds.log
```

```
$<ORACLE_HOME>/sysman/log/schemamanager/m_<timestamp>/m_
<timestamp>.CREATE/rcu.log
```

MDS Schema Drop Logs

For MDS schema drop operation, the following logs are available in the location you specified by using the `-logDir` argument while invoking the MDS schema drop command:

```
$<user_specified_location>/mds.log
```

```
$<user_specified_location>/emmdsdrops_<timestamp>.log
```

However, if you did not specify any custom location while invoking the MDS schema drop command, then the logs are created in the Oracle home of the OMS. For example, `/scratch/OracleHomes/oms12c/mds.log` and `/scratch/OracleHomes/oms12c/emmdsdrops_<timestamp>.log`.

B.1.2.3 Secure Logs

For OMS, the following secure log is available in the OMS Instance Base location. Here, `<oms_name>`, for example, can be `EMGC_OMS1`.

```
<OMS_INSTANCE_HOME>/em/<oms_name>/sysman/log/secure.log
```

For Management Agents, the following secure log is available in the Oracle home of the Management Agent.

```
<Agent_Instance_Home>/sysman/log/secure.log
```

B.1.2.4 Oracle Management Service Logs

The following log files that provide information about the running OMS are available in the OMS Instance Base location. Here, `<oms_name>`, for example, can be `EMGC_OMS1`.

```
<OMS_INSTANCE_HOME>/em/<oms_name>/sysman/log/emoms.trc
```

```
<OMS_INSTANCE_HOME>/em/<oms_name>/sysman/log/emoms.log
```

B.2 Add Host Log Files

This section describes the locations for the following Add Host log files:

- [Initialization Logs](#)
- [Application Prerequisite Logs](#)
- [System Prerequisite Logs](#)
- [Agent Installation Logs](#)
- [Other Add Host Logs](#)

B.2.1 Initialization Logs

[Table B–2](#) lists the initialization logs of the remote host and their locations. Note that `<OMS_INSTANCE_HOME>` mentioned in this table refers to the OMS instance base directory (by default, it is `gc_inst`).

Table B–2 Initialization Logs

Log File	Location
<code><hostname>_deploy.log</code>	<code><OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/applogs</code>

B.2.2 Application Prerequisite Logs

Table B–3 lists the application prerequisite logs and their locations. Note that <ORACLE_HOME> mentioned in this table refer to the Oracle home of the OMS, and the <install_type> mentioned in this table refer to one of the installation types mentioned in Table B–4.

Table B–3 Prerequisite Logs

Log File	Location
prereq<time_stamp>.log	<OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/prereqlogs/<install_type>_logs/<hostname>/
prereq<time_stamp>.out	<OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/prereqlogs/<install_type>_logs/<hostname>/
prereq<time_stamp>.err	<OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/prereqlogs/<install_type>_logs/<hostname>/

Table B–4 Install Types

Install Type	Description	Target Operating System Type
emagent_install	New Agent Installation	UNIX
emagent_clone	Agent Cloning	UNIX
nfs_install	Shared Agent Installation	UNIX

B.2.3 System Prerequisite Logs

Table B–5 lists the system prerequisite logs and their locations. Note that <ORACLE_HOME> mentioned in this table refer to the Oracle home of the OMS.

Table B–5 System Prerequisite Logs

Log File	Location
prereq<time_stamp>.log	<OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/prereqlogs/productprereq_logs/<hostname>/
prereq<time_stamp>.out	<OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/prereqlogs/productprereq_logs/<hostname>/
prereq<time_stamp>.err	<OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/prereqlogs/productprereq_logs/<hostname>/

B.2.4 Agent Installation Logs

Table B–6 lists the agent installation logs and their locations. Note that <ORACLE_HOME> mentioned in this table refer to the Oracle home of the OMS.

Table B–6 Agent Installation Logs

Log File	Location	Description
install.log/.err	<OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/logs/<hostname>	Fresh and Cloned Agent install logs
nfs_install.log/.err	<OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/logs/<hostname>	Shared Agent installation logs
cfgfw/*.log	<OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/cfgtoollogs/<hostname>	Agent Configuration logs

B.2.5 Other Add Host Logs

Table B–7 lists all the other installation logs that are created during an agent installation using the Add Host wizard. Note that <ORACLE_HOME> mentioned in this table refer to the Oracle home of the OMS.

Table B–7 Other Add Host Logs

Logs	Location	Description
EMAgentPushLogger<TIMESTAMP>.log	<OMS_INSTANCE_HOME>/sysman/agentpush/logs/	Agent Deploy application logs.
remoteInterfaces<TIMESTAMP>.log	<OMS_INSTANCE_HOME>/sysman/agentpush/logs/	Logs of the remote interfaces layer.
deployfwk.log	<OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/applogs/	Add Host Deployment Framework logs
ui.log	<OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/applogs/	Add Host User Interface logs.

B.3 Manual Management Agent Installation Logs

Table B–8 lists the installation logs that are created when a Management Agent is installed manually, that is, in silent mode. Note that <ORACLE_HOME> mentioned in this table refers to the target Management Agent Oracle Home, that is, <AGENT_BASE_DIR>/core/12.1.0.3.0/.

Table B–8 Manual Management Agent Installation Logs

Logs	Location	Description
agentDeploy<TIMESTAMP>.log	<ORACLE_HOME>/cfgtoollogs/agentDeploy/	Installation logs
prereq<TIMESTAMP>.log	<ORACLE_HOME>/cfgtoollogs/agentDeploy/	Installation prerequisite logs
CfmLogger<TIMESTAMP>.log	<ORACLE_HOME>/cfgtoollogs/cfgfw/	Configuration logs
AttachHome<TIMESTAMP>.log	<ORACLE_HOME>/cfgtoollogs/agentDeploy/	Attach home logs
UpdateHomeDeps<TIMESTAMP>.log	<ORACLE_HOME>/cfgtoollogs/agentDeploy/	Update home logs

Table B–8 (Cont.) Manual Management Agent Installation Logs

Logs	Location	Description
cloneActions<TIMESTAMP>.log	<ORACLE_HOME>/cfgtoollogs/agentDeploy/	Clone action logs

B.4 Additional OMS Installation Logs

Table lists the installation logs that you can view when adding an OMS fails:

Note: ORACLE_HOME is the home for new additional OMS. However, for admin logs, the home is the primary OMS.

Table B–9 Additional OMS Installation Logs

Logs	Location
omsca failure	\$ORACLE_HOME/cfgtoollogs/omsca
Plug-in failure	\$ORACLE_HOME/cfgtoollogs/pluginca
Managed server logs	\$ORACLE_HOME/cfgtoollogs/omsca/log_<timestamp>/
<ul style="list-style-type: none"> ■ emLogs (emoms logs) ■ msLogs (Managed server logs, if server fails to start) ■ nmLogs 	
Admin logs	\$INSTANCE_HOME/user_projects/domains/GCDomain/servers/EMGC_ADMINSERVER/logs (If out of memory error or space issue occurs, this logs on the primary OMS)
Deployment procedure output	Deployment procedure screenshots
Clone logs	\$ORACLE_HOME/cfgtoollogs/clone

Redirecting Oracle Management Agent to Another Oracle Management Service

This appendix explains how to redirect or repoint your Oracle Management Agent (Management Agent), that is already communicating with an Oracle Management Service (OMS), to communicate and upload data to another OMS that is part of a different Enterprise Manager Cloud Control (Cloud Control) deployment.

Note: When you repoint a Management Agent to another OMS that is part of a different Cloud Control deployment, you lose all the changes made to the agent instance home, such as user defined metric collections, changes made to the `emd.properties` file, and so on.

In particular, this appendix covers the following:

- [Prerequisites](#)
- [Procedure](#)

C.1 Prerequisites

Before redirecting or repointing a Management Agent, ensure that you meet the following prerequisites:

- Ensure that the new OMS that you want to point the Management Agent to is of the same version as the Management Agent, or of a higher version.

To view the version of the Management Agent you want to repoint, from the **Setup** menu, select **Manage Cloud Control**, then select **Agents**. Click the name of the Management Agent. The Management Agent version is displayed in the Summary section.

To view the version of the new OMS, from the **Setup** menu, select **Manage Cloud Control**, then select **Management Services**. Click the name of the new OMS. The OMS version is displayed in the Summary section.

You can repoint the Management Agent only if the new OMS is compatible with the Management Agent. Using the Enterprise Manager certification matrix, you can view the compatibility between an OMS version and a Management Agent version. For information on accessing this matrix, refer *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

- Ensure that the previous OMS that the Management Agent was pointing to, and the new OMS that you want to point the Management Agent to have the same set of plug-ins deployed on them, and that all the plug-ins configured on the

Management Agent are deployed on the new OMS. Also, ensure that all these plug-ins deployed on the new OMS are of the same version, (that is, the version configured on the Management Agent or the previous OMS) or a higher version.

To view the list of plug-ins deployed on a particular OMS, log in to the Enterprise Manager system, from the **Setup** menu, select **Extensibility**, then select **Plug-ins**.

To view the list of plug-ins configured on a particular Management Agent, run the following command:

```
$<AGENT_INSTANCE_HOME>/bin/emctl listplugins agent -type all
```

- Ensure that you check the contents of `<AGENT_BASE_DIR>/plugins.txt`. Only the plug-ins mentioned in `plugins.txt` will be configured on the Management Agent after you repoint it to the new OMS.
- Ensure that all the patches applied on the Management Agent that change the target type or collection metadata are also applied on the new OMS that you want to point the Management Agent to.

To view all the patches applied on the Management Agent, from the **Targets** menu, select **All Targets**. Click the name of the Management Agent Oracle Home target. All the patches applied on the Management Agent are displayed in the Applied Patches section.

From the displayed list of patches, apply the required patches (the patches that change the target type or collection metadata) on the new OMS. For information on how to apply a patch on an OMS, refer the Patching Enterprise Manager chapter present in *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

- If you have applied any one-off patches on the Management Agent you want to repoint, ensure that you apply the fix for Bug 15904425 on the Management Agent and the new OMS.

C.2 Procedure

To redirect or repoint a Management Agent, follow these steps:

1. Run the following command to stop the Management Agent:

```
$<AGENT_INSTANCE_HOME>/bin/emctl stop agent
```

2. Run the following EMCLI command to delete the Management Agent target on the old OMS:

```
$<OMS_HOME>/bin/emcli delete_target -delete_monitored_targets  
-name=<name_of_agent_target> -type="oracle_emd"
```

For more information about the `delete_target` EMCLI command, refer *Oracle Enterprise Manager Command Line Interface Guide*.

3. Run the following command to remove the Management Agent instance home:

```
rm -rf <absolute_path_to_agent_instance_home>
```

If the agent base directory and the agent instance home point to the same physical location, do not run this command. Instead, remove the `<AGENT_INSTANCE_HOME>/bin`, `<AGENT_INSTANCE_HOME>/sysman`, `<AGENT_INSTANCE_HOME>/diag`, and `<AGENT_INSTANCE_HOME>/install` directories.

4. Run the `agentDeploy.sh` (`agentDeploy.bat` for Microsoft Windows hosts) script with the `-configOnly` option to create a new instance home for the Management Agent and redirect it to the new OMS:

```
$<AGENT_BASE_DIR>/core/12.1.0.2.0/sysman/install/agentDeploy.sh AGENT_BASE_DIR=<absolute_path_to_agent_base_dir> RESPONSE_FILE=<absolute_path_to_responsefile> -configOnly
```

Ensure that you pass a response file when you run the `agentDeploy.sh` or `agentDeploy.bat` scripts. The response file must contain the `OMS_HOST`, `EM_UPLOAD_PORT`, and `AGENT_REGISTRATION_PASSWORD` parameters. The `OMS_HOST` parameter must specify the new OMS host name, the `EM_UPLOAD_PORT` parameter must specify the upload port to be used to connect to the new OMS, and the `AGENT_REGISTRATION_PASSWORD` parameter must specify the password to be used for registering new Management Agents that join the Enterprise Manager system.

For more information about the parameters you can specify in the response file, refer [Table 6-3](#). For more information about the `-configOnly` option, refer [Table 6-6](#).

Note: The specified agent base directory location and the new agent instance home location map to locations on the same host, where the Management Agent was already configured. The OMS host name, of course, maps to the other host where the new OMS is configured, that is, the OMS with which you want the Management Agent to communicate now.

Applying One-Off Patches to Oracle Management Agents

In Enterprise Manager Cloud Control 12c Release 3 (12.1.0.3.0), you can combine Management Agent binaries with Management Agent patches and plug-in patches, so that you do not have to apply these patches every time you deploy or upgrade a Management Agent. You can save the Management Agent one-off patches that you want to apply on a particular version of the Management Agent software, such that these patches are automatically applied on the software whenever a new Management Agent of the same version is deployed, or an old Management Agent is upgraded to that version. This is a one-time operation, that is, you do not have to perform this action every time you deploy or upgrade a Management Agent.

If you save the Management Agent one-off patches on the OMS host as described in this appendix, any Management Agent deployment or upgrade activity will automatically pick up these patches for the respective Management Agent versions and platforms. Hence, this feature saves you a considerable amount of time and effort.

For information on applying patches on a plug-in and ensuring that the patched plug-in is deployed on all the new Management Agents that you deploy, and all the old Management Agents that you upgrade, see *Oracle Enterprise Manager Cloud Control Administration Guide*.

Ensure that you follow the steps mentioned in this appendix and the section referenced in the previous para before scheduling a Management Agent deployment or upgrade session, so that the patches that you want to apply on the Management Agent and plug-ins are applied automatically after the Management Agent deployment or upgrade.

This appendix contains the following sections:

- [Saving Management Agent Patches to an OMS Host](#)
- [Verifying Patch Application After Management Agent Deployment or Upgrade](#)

D.1 Saving Management Agent Patches to an OMS Host

To save Management Agent one-off patches to your OMS host, such that they are applied whenever a new Management Agent is deployed, or a Management Agent is upgraded, follow these steps:

1. Download the required Management Agent one-off patches from My Oracle Support, available at the following URL:

<https://support.oracle.com/>

Ensure that the size of the patch zip file you downloaded is the same as what is displayed on the My Oracle Support page.

For information on how to download a patch from My Oracle Support, see *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*.

2. Create the following directory on the OMS host, and transfer all the generic Management Agent one-off patches to it:

```
$<OMS_HOME>/install/oneoffs/<agent_version>/Generic/
```

Here, <agent_version> is the version of the Management Agent that the patch is for. Ensure that you use the five-digit Management Agent version while creating this directory.

For example, if you want to apply Patch 11180406, a generic Management Agent one-off patch for a 12.1.0.3.0 Management Agent, whenever a 12.1.0.3.0 Management Agent is deployed, or an old Management Agent is upgraded to 12.1.0.3.0, download this patch from My Oracle Support, create the following directory, then transfer the patch to it:

```
$<OMS_HOME>/install/oneoffs/12.1.0.3.0/Generic/
```

3. Create the following directories on the OMS host, and transfer all the platform-specific Management Agent one-off patches to them:

```
$<OMS_HOME>/install/oneoffs/<agent_version>/<platform>/
```

Here, <agent_version> is the version of the Management Agent that the patch is for. Ensure that you use the five-digit Management Agent version while creating these directories.

<platform> is the platform directory name, which is different for different patch platforms. [Table D–1](#) lists the platform directories that you must create for various patch platforms.

Table D–1 Platform Directory Names for Transferring Platform-Specific Management Agent Patches

Patch Platform	Platform Directory Name
Linux x86	linux
Linux x86-64	linux_x64
Oracle Solaris on SPARC (64-bit)	solaris
Oracle Solaris on x86-64 (64-bit)	solaris_x64
HP-UX PA-RISC (64-bit)	hpunix
HP-UX Itanium	hpi
IBM S/390 Based Linux (31-bit)	linux_zseries64
IBM AIX on POWER Systems (64-bit)	aix
IBM: Linux on POWER Systems	linux_ppc64
Microsoft Windows x64 (64-bit)	windows_x64
Microsoft Windows (32-bit)	win32

Note: If you have a multi-OMS environment, ensure that you perform these steps on all the OMS hosts. Ensure that you download and transfer the same patches to the same directories on all the OMS hosts. Failing to do so may result in inconsistency and unexpected errors.

For example, if you want to apply Patch 11878907 (which is for a 12.1.0.3.0 Linux x86-64 Management Agent), and Patch 11993577 (which is for a 12.1.0.3.0 Microsoft Windows x64 Management Agent), whenever these Management Agents are deployed, or older versions of these Management Agents are upgraded to 12.1.0.3.0, download these patches from My Oracle Support, create the following directories, then transfer the patches to them:

For Patch 11878907:

```
$<OMS_HOME>/install/oneoffs/12.1.0.3.0/linux_x64/
```

For Patch 11993577:

```
$<OMS_HOME>/install/oneoffs/12.1.0.3.0/windows_x64/
```

D.2 Verifying Patch Application After Management Agent Deployment or Upgrade

You can use these methods to verify whether the Management Agent one-off patches that you saved to your OMS host (described in [Section D.1](#)) have been applied on a Management Agent that you deployed or upgraded:

- Run the following command from the Management Agent home:

```
$<AGENT_HOME>/OPatch/opatch lsinventory -oh <AGENT_HOME> -invPtrLoc  
<AGENT_HOME>/oraInst.loc
```

This command displays all the patches applied on the Management Agent.

- In the Cloud Control console, from the **Setup** menu, select **Manage Cloud Control**, then select **Agents**. Click the name of the required Management Agent to navigate to its home page. In the Configuration section, click **Oracle Home and Patch Details**. The patches applied on the Management Agent are displayed in the Patches Applied section.

Using RepManager Utility

This appendix describes the RepManager utility. In particular, this appendix covers the following:

- [Overview](#)
- [Supported Actions and Commands](#)

E.1 Overview

RepManager is a utility that enables you to upgrade and drop Oracle Management Repository, selectively purge plug-ins, and load dlf messages to Oracle Management Repository. This utility is available in the Oracle Management Service (OMS) home:

For UNIX operating systems:

```
$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager
```

For Microsoft Windows operating systems:

```
$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager.bat
```

This utility is invoked by Repository Configuration Assistant while installing a complete Enterprise Manager system, and by Repository Upgrade Configuration Assistant while upgrading to Enterprise Manager Cloud Control.

Note: If you want to drop the Enterprise Manager schema completely, then use the RepManager available in the OMS home. Do not use the one in database home because it cannot remove the Enterprise Manager schema completely.

E.2 Supported Actions and Commands

[Table E-1](#) shows the list of actions and their associated commands supported by the RepManager utility.

WARNING: The RepManager in drop mode puts the database in quiesce mode by "ALTER SYSTEM QUIESCE RESTRICTED;" command.

Table E–1 Actions and Commands Supported by RepManager

Action	Command	Description	Example
preupgrade	<pre>\$<OMS_ HOME>/sysman/admin/emdrep/bin/RepManager -action preupgrade <repository_database_ host> <repository_ database_port> <repository_database_ sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman [-mwHome <Middleware home>] -pluginDepList "<pluginid1>=<plugini d1 home>, <pluginid2>=<pl uginid2 home>" -runAsReposUser <TRUE/FALSE> -dlfSources "<oms home>, <plugin1 home>, <plugin2home>"</pre>	<p>Use this action to perform steps before upgrading an Oracle Management Repository with the following parameters:</p> <ul style="list-style-type: none"> Specify the host, port, and SID to connect to Oracle RDBMS where Oracle Management Repository is to be upgraded. Specify the database user and password, repository name (SYSMAN) and password for SYSMAN user, and Middleware home to upgrade the Oracle Management Repository. Specify a comma-separated list of plug-ins to be deployed according to the dependency. You can pass a file with this option, the contents being a comma-separated list of plug-in IDs. If the <code>-pluginDepList</code> parameter is not set, or is left with an empty list (for example, "{}"), then the following is read, by default, to retrieve the plug-in dependency list: <pre>\$<OMS_ HOME>/sysman/admin/emdrep/plugin info/pluginDepList</pre> Depending on how the plug-ins can be deployed, specify whether they must be deployed as SYS or SYSMAN, which is the repository user. To deploy them as SYSMAN, set the <code>-runAsReposUser</code> parameter to TRUE. If you do not pass this parameter, by default, the plug-ins will be deployed as SYS user. Specify a comma-separated locations for DLF files from platform/plugins. You can pass a file with this option, the contents being comma-separated locations for DLF files from platform/plugins. If the <code>-dlfSources</code> parameter is not set, or is left with an empty list (for example, "{}"), then the following is read, by default, to retrieve the dlf resource locations: <pre>\$<OMS_ HOME>/sysman/admin/emdrep/plugin info/dlfSources</pre> <p>If this option is missing and default dlfSources file is not present, only dlf files for platform will be picked. If this is present, only the DLFs under these sources will be picked up.</p> 	<pre>\$<OMS_ HOME>/sysma n/admin/emd rep/bin/Rep Manager -action preupgrade example.com 1521 db3 -dbUser sys -dbRole sysdba -reposName sysman -mwHome /scratch/we blogic/midd leware -pluginDepL ist <pluginid1> =<pluginid1 home>, <plug inid2>=<plu ginid2 home></pre>

Table E-1 (Cont.) Actions and Commands Supported by RepManager

Action	Command	Description	Example
upgrade	<pre>\$<OMS_ HOME>/sysman/admin/emdrep/bin/RepManager -action upgrade <repository_database_ host> <repository_ database_port> <repository_database_ sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman [-mwHome <Middleware home>]-pluginDepList "<pluginid1>=<plugini d1 home>,<pluginid2>=<pl uginid2 home>" -runAsReposUser <TRUE/FALSE> -dlfSources "<oms home>,<plugin1 home>,<plugin2home>"</pre> <p>Note: Run preupgrade before performing upgrade action.</p>	<p>Use this action to upgrade an Oracle Management Repository with the following parameters:</p> <ul style="list-style-type: none"> Specify the host, port, and SID to connect to Oracle RDBMS where Oracle Management Repository is to be upgraded. Specify the database user and password, repository name (SYSMAN) and password for SYSMAN user, and Middleware home to upgrade the Oracle Management Repository. Specify a comma-separated list of plug-ins to be deployed according to the dependency. You can pass a file with this option, the contents being a comma-separated list of plug-in IDs. If the <code>-pluginDepList</code> parameter is not set, or is left with an empty list (for example, "{}"), then the following is read, by default, to retrieve the plug-in dependency list: <pre>\$<OMS_ HOME>/sysman/admin/emdrep/plugin info/pluginDepList</pre> Depending on how the plug-ins can be deployed, specify whether they must be deployed as SYS or SYSMAN, which is the repository user. To deploy them as SYSMAN, set the <code>-runAsReposUser</code> parameter to TRUE. If you do not pass this parameter, by default, the plug-ins will be deployed as SYS user Specify a comma-separated locations for DLF files from platform/plugins. You can pass a file with this option, the contents being comma-separated locations for DLF files from platform/plugins. If the <code>-dlfSources</code> parameter is not set, or is left with an empty list (for example, "{}"), then the following is read, by default, to retrieve the dlf resource locations: <pre>\$<OMS_ HOME>/sysman/admin/emdrep/plugin info/dlfSources</pre> <p>If this option is missing and default dlfSources file is not present, only dlf files for platform will be picked. If this is present, only the DLFs under these sources will be picked up.</p> 	<pre>\$<OMS_ HOME>/sysma n/admin/emd rep/bin/Rep Manager -action upgrade example.com 1521 db3 -dbUser sys -dbRole sysdba -reposName sysman -mwHome /scratch/we blogic/midd leware -pluginDepL ist <pluginid1> =<pluginid1 home>,<plug inid2>=<plu ginid2 home></pre>

Table E-1 (Cont.) Actions and Commands Supported by RepManager

Action	Command	Description	Example
transX	<pre>\$<OMS_ HOME>/sysman/admin/emdrep/bin/RepManager -action transx <repository_database_ host> <repository_ database_port> <repository_database_ sid> -reposName sysman [-mwHome <Middleware home>] -dlfSources "<oms home>,<plugin1 home>,<plugin2home>"</pre> <p>Note: You can also run -doTransX. By default, it is set to true. If you set the value to false, no translation bundles are loaded. This is applicable for -dlfSources for preupgrade and upgrade actions.</p>	<p>Use this action to load the translation resources to the Oracle Management Repository with the following parameters:</p> <ul style="list-style-type: none"> Specify the host, port, and SID to connect to Oracle RDBMS to load translation resources to Oracle Management Repository. Specify the database user and password, repository name (SYSMAN) and password for SYSMAN user, and Middleware home to load translation resources to Oracle Management Repository. Specify a comma-separated locations for DLF files from platform/plugins. You can pass a file with this option, the contents being comma-separated locations for DLF files from platform/plugins. If the -dlfSources parameter is not set, or is left with an empty list (for example, "{}"), then the following is read, by default, to retrieve the dlf resource locations: <pre>\$<OMS_ HOME>/sysman/admin/emdrep/plugin info/dlfSources</pre> <p>If this option is missing and default dlfSources file is not present, only dlf files for platform will be picked. If this is present, only the DLFs under these sources will be picked up.</p> 	<pre>\$<OMS_ HOME>/sysma n/admin/emd rep/bin/Rep Manager -action transx example.com 1521 db3 -reposName sysman -mwHome /scratch/WL S/middlewar e</pre>
resume	<pre>\$<OMS_ HOME>/sysman/admin/emdrep/bin/RepManager -resume retry <repository_database_ host> <repository_ database_port> <repository_database_ sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman [-mwHome <Middleware home>] -checkpointLocation <directory where schemamanager stores checkpoints></pre>	<p>Use this action to resume the last failed action, for example, upgrade.</p> <ul style="list-style-type: none"> Specify the host, port, and SID to connect to Oracle RDBMS where the action is to be resumed. Specify the database user and password, repository name (SYSMAN) and password for SYSMAN user, and Middleware home where the action is to be resumed. Specify the location at which to resume the step. The checkpoint location is \$<OMS_ HOME>/sysman/log/schemamanag er. 	<pre>\$<OMS_ HOME>/sysma n/admin/emd rep/bin/Rep Manager example.com 1521 db3 -dbUser sys -dbRole sysdba -reposName sysman -resume retry -checkpoint Location /scratch/we blogic/midd leware/oms/ sysman/log/ schemamanag er -mwHome /scratch/we blogic/midd leware</pre>

Table E-1 (Cont.) Actions and Commands Supported by RepManager

Action	Command	Description	Example
drop OR dropall	<pre>\$<OMS_ HOME>/sysman/admin/em drop/bin/RepManager -action drop <repository_database_ host> <repository_ database_port> <repository_database_ sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman [-mwHome <Middleware home>] [-mwOraHome <Oracle Home>]</pre> <p>OR</p> <pre>\$<OMS_ HOME>/sysman/admin/em drop/bin/RepManager -action dropall <repository_database_ host> <repository_ database_port> <repository_database_ sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman [-mwHome <Middleware home>] [-mwOraHome <Oracle Home>]</pre> <p>Ensure that there are no active sessions, scheduler jobs, and dbms_jobs running for SYSMAN, SYSMAN_MDS SYSMAN_OPSS, and SYSMAN_APM. Ensure that none of these users are logged in. To ensure this, stop the OMS using the command <code>emctl stop oms -all</code> on all OMS instances.</p> <p>Note: If BI Pubilsher (BIP) had been installed and configured, then BIP should be stopped using the Admin Server before running this command.</p>	<p>Use this action to remove all Enterprise Manager repository schemas as follows:</p> <ul style="list-style-type: none"> Specify the host, port, and SID to connect to Oracle RDBMS from which all schemas are to be dropped. Specify the database user and password, repository name (SYSMAN) and password for SYSMAN user, and Middleware home. <p>At the end, a confirmation message appears to confirm the status of this operation. If all the schemas were successfully dropped, then a message confirming the same appears. Otherwise, a message providing details on each of the schemas appears.</p> <p>For example,</p> <p>SYSMAN_OPSS schema is not cleaned. EM_X synonyms are not dropped.</p>	<pre>\$<OMS_ HOME>/sysma n/admin/emd rep/bin/Rep Manager example.com 1521 db3 -dbUser sys -dbRole sysdba -reposName sysman -action drop -mwHome /scratch/we blogic/midd leware</pre> <p>OR</p> <pre>\$<OMS_ HOME>/sysma n/admin/emd rep/bin/Rep Manager example.com 1521 db3 -dbUser sys -dbRole sysdba -reposName sysman -action dropall -mwHome /scratch/we blogic/midd leware -mwOraHome /scratch/we blogic/midd leware</pre>

Table E-1 (Cont.) Actions and Commands Supported by RepManager

Action	Command	Description	Example
pluginpurge	<pre>\$<OMS_ HOME>/sysman/admin/em drep/bin/RepManager -action pluginpurge <repository_database_ host> <repository_ database_port> <repository_database_ sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman -pluginPurgeList "<plugin_ name>=<plugin_ location>" [-mwHome <Middleware home>] -mwOraHome <Oracle Home></pre> <p>Note: To purge multiple plug-ins, for the -pluginPurgeList argument, enter the plug-ins separated by a command. For example, <pluginid1>=<pluginid1 home>, <pluginid2>=<pluginid2 home></p>	<p>Use this action to deinstall a plug-in from the repository as follows:</p> <ul style="list-style-type: none"> Specify the host, port, and SID to connect to Oracle RDBMS from which the plug-in is to be deinstalled. Specify a comma-separated list of plug-ins to be purged from Enterprise Manager Repository with EM-EXT model. 	<pre>\$<OMS_ HOME>/sysma n/admin/emd rep/bin/Rep Manager example.com 1521 db3 -dbUser sys -dbRole sysdba -reposName sysman -action pluginpurge -pluginPurg eList "oracle.sys man.myyempw pax.oms.plu gin_ 12.1.0.2.0= /scratch/we blogic/midd leware/plug ins/oracle. sysman.myye mpwpax.oms. plugin_ 12.1.0.2.0" -mwHome /scratch/we blogic/midd leware</pre>

Note: RepManager 12.1 supports -action dropall and -action drop, which drop SYSMAN, SYSMAN_MDS, SYSMAN_APM, SYSMAN_OPSS, and SYSMAN_RO. RepManager 11.1 supports -action dropall, which drops only SYSMAN and SYSMAN_MDS, and -action drop, which drops only SYSMAN. RepManager 10.2.0.5 supports -action drop, which drops only SYSMAN.

Note: If you do not specify passwords during RepManager actions, you will be prompted to do so.

Collecting OCM Data Using Oracle Harvester

My Oracle Support provides a key set of features and functionality that greatly enhance the customer's interaction with Oracle Support. My Oracle Support streamlines the Service Request submission process by providing in-context information specific to a customer's configurations, as well as proactive support. To enable these features within My Oracle Support, the customer's configuration information must be uploaded to Oracle. When the configuration data is uploaded on a regular basis, customer support representatives can analyze this data and provide better service to customers.

The following mechanisms are provided to customers for collecting and uploading configuration data to Oracle.

- Oracle Enterprise Manager Harvester (Oracle Harvester)
- Oracle Configuration Manager (OCM)

In particular:

- Oracle Configuration Manager is installed and configured automatically when you install an Oracle product.

When installing any product, the first screen asks for My Oracle Support credentials. THIS IS A PIVOTAL SCREEN in the installation. The user name and password that you provide are the credentials against which the configuration data is uploaded to Oracle.

- Configuration collections run and the configuration data is uploaded to Oracle every 24 hours.
- Once the data is uploaded, it can be viewed by logging into My Oracle Support (<https://support.oracle.com>) using the same credentials supplied during product installation.

Note: If you use Enterprise Manager to manage your applications, we recommend that you use Oracle Harvester to upload your configurations to Oracle. Otherwise, use OCM.

F.1 Oracle Harvester

Oracle Harvester only harvests data for targets that are managed by Enterprise Manager. Because Oracle Harvester has the same OCM dependencies, Oracle Harvester enables the gathering of target configuration data by leveraging Enterprise Manager collection methods thus precluding the need to install OCM on target homes managed by Oracle Harvester.

Highlights of Oracle Harvester

The following are highlights of Oracle Harvester:

- Data is uploaded by default for all targets against the same credentials with which OCM in the Oracle Management Service (OMS) home is configured. From Enterprise Manager Cloud Control 12c, you can change this default value for a target by assigning a CSI from the CSI Assignment page. Click **Setup**, then **My Oracle Support** to get started.
- Requires OCM to be configured and running in the OMS home for Enterprise Manager.
- Gathers target configuration data from the Management Repository
- Automatically runs periodically so no user intervention is required

Oracle Harvester and OCM

When you install Enterprise Manager, Oracle Harvester and Oracle Configuration Manager are automatically installed as are all the necessary subcomponents. The Oracle Harvester will run as long as the OCM in the OMS home is configured and running.

OCM *must* be enabled in the Oracle Home of the OMS and configured (and running in connected mode) in the Instance Home of the OMS. The reason is that the Oracle OMS target will *not* be discovered by the OCM collector if ORACLE_CONFIG_HOME is not set.

Perform the following steps to ensure the Oracle OMS target is discovered:

1. Locate the OMS instance home.

In the \$ORACLE_HOME/sysman/config/emInstanceMapping.properties file (where ORACLE_HOME is the Oracle Home of the OMS), there is an entry referencing a file called emgc.properties.

The directory in which the emgc.properties file is located is the "instance home" of the OMS. In the following example, /u01/app/oracle/product/gc_inst/em/EMGC_OMS1 is the instance home of the OMS:

```
EMGC_OMS1=/u01/app/oracle/product/gc_inst/em/EMGC_OMS1/emgc.properties
```

2. Set the environment variable ORACLE_CONFIG_HOME to the directory of this emgc.properties file.

Example:

```
$export ORACLE_CONFIG_HOME=/u01/app/oracle/product/gc_inst/em/EMGC_OMS1
```

3. Configure OCM.

Support For Enterprise Manager Release 12.1

By default, all targets are uploaded using the credentials used to register Oracle Configuration Manager in the OMS Home. In Enterprise Manager release 12.1, you have the option of assigning a Customer Support Identifier (CSI) to each target home.

The Oracle Harvester supports uploading configuration data to different CSIs for each different Oracle Home.

The steps include:

1. Ensuring that the Oracle Harvester has run. This job runs automatically. The status of the run can be monitored from the Support Identifier Assignment page.

To access this page from the Enterprise Manager home page, select **Setup**, then select **My Oracle Support**. From the menu, select **Support Identifier Assignment**.

2. Setting My Oracle Support preferred credentials. From the Enterprise Manager home page, select **Setup**, then select **My Oracle Support**. From the menu, select **Set credentials** and supply any valid My Oracle Support credentials.
3. Assigning the Support Identifier.
 - a. From the Enterprise Manager home page, select **Setup**, then select **My Oracle Support**. Select **Support Identifier Assignment** and provide the correct user name and password. Select **Set credentials**.
 - b. Select **Home**. Click **Assign** button. Select CSI and click **OK**.
4. Ensuring the message displays indicating the assignment was successful. The message reads:

Support Identifier has been assigned for 1 Oracle homes. The changes in the Customer Support Identifiers will be reflected in My Oracle Support after the next Harvester run.

Viewing CSIs in Enterprise Manager

You can see the CSI associated with a target by viewing the target property or by doing a configuration search with CSI set as the search criteria. Any user with operator privilege on all targets for a given Oracle Home can assign a CSI for that Oracle Home.

Refer to the help in the Enterprise Manager interface on how to access this information.

Harvester Target Lifecycle Properties from Enterprise Manager

Oracle Harvester provides the target lifecycle property to enable you to identify the purpose of a target, for example, development, testing, and so on.

Once defined, the Oracle Harvester collects the target lifecycle property for all the targets and uploads the property to Oracle Configuration Manager server.

You can assign target lifecycle property to any target from either the Enterprise Manager UI or the My Oracle Support UI.

The possible values of a target's lifecycle property are:

- Mission Critical
- Production
- Stage
- Test
- Development

Harvester Job Status Metric

From Enterprise Manager Release 12.1 Patch Set 2 (PS2) and OCM 10.3.8.1.0, a *Harvester Job Status* metric has been added to the OMS and Repository target. This metric will provide information related to the Harvester Job. The following information is collected as part of this metric:

- **Harvester Status:** Provides the status of the last harvester job run. Possible values include:
 - SUCCESS: indicates the job ran successfully.

- ERROR: returned if job failed.
- NOT CONFIGURED: indicates that OCM is not configured.
- NOT AUTHENTICATE: shows that OCM is configured, but it is not in Authenticated mode.
- **Harvester Error:** Shows an error message in case the harvester job fails to run.
- **Last Harvester Job Run:** Shows the time the last harvester job ran.
- **Next Harvester Job Run:** Shows the time of the next harvester job run.
- **Total Targets Processed:** Shows the number of targets processed by the harvester job during its last run.
- **Total Targets Successful:** Total number of targets successfully uploaded to MOS from Total Targets Processed.
- **Total Targets Failed:** Shows the total number of target that failed to upload to MOS out of the Total Targets Processed in the Last Harvester Job Run.
- **OCM Version:** Shows the version of OCM configured with Enterprise Manager.

The Harvester Job Status metric data is available from the OMS and Repository target metrics page. An ERROR threshold has been defined for the Harvester Status field. If the value of this field shows ERROR, then an incident will be created, which will appear on both the OMS and Repository home page and the Incident Manager Page.

F.1.1 Supported Targets in Oracle Harvester

Oracle Harvester collects configuration data from Enterprise Manager releases 10.2.0.5, 11.1, and 12.1. Depending on the version of Enterprise Manager that Oracle Harvester is running on, Oracle collects the configuration data from a different set of target types. Only configuration data from the target types represented in the following tables are collected by Oracle Harvester.

[Table F-1](#) shows the supported targets for Enterprise Manager Release 12.1. [Table F-2](#) shows the supported targets for Enterprise Manager Release 10.2.0.5 and 11.1, respectively.

Table F-1 Supported Targets in Enterprise Manager 12.1 Releases

Target	Plug-in Release	Enterprise Manager Release		
		12.1	12.1 PS1	12.1 PS2
BI	12.1.0.3	No	Yes	Yes
Host	not applicable	Yes	Yes	Yes
Management Agent	not applicable	Yes	Yes	Yes
Management Repository	not applicable	Yes	Yes	Yes
Oracle Application Server	all versions	Yes	Yes	Yes
Oracle Database	all versions	Yes	Yes	Yes
Oracle Database Machine	all versions	Yes	Yes	Yes
Oracle Exadata Storage Server	all versions	Yes	Yes	Yes
Oracle Exalogic	12.1.0.2	No	Yes	Yes
	12.1.0.3	No	No	Yes
Oracle Fusion Applications	all versions	Yes	Yes	Yes
Oracle Fusion Middleware	all versions	Yes	Yes	Yes
Oracle Home	not applicable	Yes	Yes	Yes

Table F–1 (Cont.) Supported Targets in Enterprise Manager 12.1 Releases

Target	Plug-in Release	Enterprise Manager Release		
		12.1	12.1 PS1	12.1 PS2
Oracle Identity Manager for configurations: OIF, OID, OVD and DIP		No	Yes	Yes
Oracle Identity Manager for configurations: OIM, OAM and OAAM	all versions	Yes	Yes	Yes
Oracle Management Service	not applicable	Yes	Yes	Yes
Oracle SOA Suite	all versions	Yes	Yes	Yes
Oracle Virtual Manager	all versions	Yes	Yes	Yes
Oracle WebLogic Server	all versions	Yes	Yes	Yes
Siebel	12.1.0.3	No	No	Yes

Table F–2 Supported Targets in Enterprise Manager Release 10.2.0.5 and 11.1

Target	Plug-in Release	Enterprise Manager Release	
		10.2.0.5	11.1
Host	not applicable	Yes	Yes
Oracle Application Server	all versions	Yes	Yes
Oracle Database	all versions	Yes	Yes
Oracle Exadata Storage Server	all versions	No	Yes
Oracle Home	not applicable	Yes	Yes
Oracle Virtual Manager	all versions	No	Yes
Oracle WebLogic Server	all versions	No	Yes

F.1.2 Configuration Data Not Available in My Oracle Support

In previous versions of Enterprise Manager, Oracle Harvester configuration data was only uploaded to My Oracle Support when 30 days had passed since the last upload of data by a standalone OCM Collector if such data already existed in My Oracle Support.

This restriction has been lifted in Enterprise Manager 12c. Configuration data for targets collected from Oracle Harvester running in Enterprise Manager release 12c displays in My Oracle Support immediately, regardless of how recently data was uploaded by a standalone OCM Collector.

F.2 Oracle Configuration Manager

Oracle Configuration Manager is installed and configured automatically when you install an Oracle product. It is installed in the product Home and collects configuration data for all targets installed in that Home.

The OCM setup requires specifying the My Oracle Support account and password, or My Oracle Support account and Customer Support Identifier (CSI). Configuration data will be uploaded using this information and can be viewed by logging in to My Oracle Support using the same credentials.

OCM must be installed in every Oracle Home from which you want to upload configuration data to Oracle. In addition to being part of the product installation, OCM can also be downloaded from My Oracle Support. The Mass Deployment tool is available to help with deploying OCM across data centers. The OCM kit is available from the Collector tab on My Oracle Support.

Once OCM is installed, no additional work is required. By default, automatic updates are enabled and you are encouraged to use this feature to ensure you are always running the latest version of OCM. This feature can be disabled if required, for example, for security reasons. If you disable the feature, you can turn it on by executing the following command:

```
<ocm_install_root>/ccr/bin/emCCR automatic_update on
```

Note: If you use Enterprise Manager or Ops Center to manage your applications, we recommend that you use Oracle Harvester or Ops Center Harvester respectively to upload your configurations to Oracle. Otherwise, use OCM.

F.3 Additional Information

To find additional information about My Oracle Support, see:

<https://support.oracle.com>

To find more information about OCM, perform the following steps:

1. Log into My Oracle Support at <https://support.oracle.com>
2. To access the **Collector** tab, click **More** and select **Collector** from the drop-down menu. The Collector page contains useful information.

F.4 Troubleshooting Configuration Data Collection Tools

The following sections describe how to resolve issues with the configuration data collections.

In Enterprise Manager release 12.1.0.2, ensure that collection data is uploaded to Oracle by using the `emCCR status` command. Look at the last uploaded date and time.

Note: This `emCCR status` command shows that collected data was uploaded, but does not ensure the Oracle Harvester collections were successful and uploaded.

Location of error logs:

- Oracle Harvester error logs:
 - For Harvester Job errors, look at:
`INSTANCE_HOME/sysman/log/emoms_pbs.trc`
 - UI errors, for example CSI Assignment errors, look at:
`INSTANCE_HOME/sysman/log/emoms.trc`

For example:

```
/gc_inst/user_projects/domains/GCDomain/servers/EMGC_  
OMS1/sysman/log/emoms.trc
```

- Oracle Configuration Manager log is located at:
`ccr/hosts/<hostname>/log/collector.log`

F.4.1 Oracle Harvester Collection Fails If the state/upload/external Directory Is Missing

If the Oracle Harvester collection fails with the following error, the required directory named *external* is missing.

```
[JobWorker 75210:Thread-61] ERROR gcharvester.GcCollectionMgr initOcm.? - GC OCM
Harvester: Caught GC Harvester exception from GCInit.init(): The installed version
of Oracle Configuration Manager in the ORACLE_HOME
(/scratch/aime/work/midlwre8937/oms11g) is prior to 10.3.1. The Grid Control
Configuration harvesting requires at a minimum, 10.3.1
```

To resolve this issue, create the *external* directory:

```
$ORACLE_INSTANCE_HOME/ccr/state/upload/external
(Bug 12795503)
```

F.4.2 Oracle Configuration Manager Is Not Running

When OCM is not running, you may see the following error:

```
2012-08-29 16:34:20,709 [JobWorker 97285:Thread-60] WARN
gcharvester.HarvesterJobUtils performOCMCollections.? - GC OCM Harvester: OCM was
stopped and is not running
```

To resolve this issue, verify that the OCM was installed and configured in the appropriate directories (execute `emCCR status`).

In particular, OCM must be installed in the OMS Oracle Home and configured (and running in connected mode) in the OMS Instance Home.

F.4.3 Configuration Data Not Available in My Oracle Support

When you look at My Oracle Support and do not find configuration data, it could be that the Oracle Harvester collection did not run.

To resolve this issue, verify that the OCM was installed and configured in the appropriate directories (execute `emCCR status`). In particular, OCM must be installed in the OMS Oracle Home and configured (and running in connected mode) in the OMS Instance Home.

To verify that OCM is running, perform the following steps:

1. Set `ORACLE_CONFIG_HOME` to the INSTANCE HOME
2. Execute `$ORACLE_HOME/ccr/bin/emCCR status`

F.4.4 Only a Subset of the Targets Is Collected by the Oracle Harvester

If many targets are uploaded to the Management Repository but only a subset of the targets is collected by the Oracle Harvester, it could be because the same error was encountered 10 times during a collection, causing the Oracle Harvester to stop collecting. Look at the appropriate log file to verify that this error has occurred.

Resolve the issue by running the following SQL script against the Management Repository. This script forces the Oracle Harvester to ignore this collection error and continue collecting the remaining target information.

```
sql> insert into mgmt_ocm_upl_props (name,str_value) values('ignore_
errors','true');
sql> commit;
```

Bounce the OMS after executing the SQL script.

(Bug 11734389)

Enabling Enterprise Manager Accessibility Features

As part of the effort to make Oracle products, services, and supporting documentation accessible and usable to the disabled community, Enterprise Manager offers several features that make management data available to users of assistive technology. Enterprise Manager provides the following accessibility features:

- Support for Screen Reader
- Support for High Contrast
- Support for Large Fonts

This appendix consists of the following configuration settings you must modify to enable Screen Reader support:

- [Enabling Enterprise Manager Accessibility Mode](#)
- [Setting uix-config.xml Flag](#)
- [Configuring web.xml File](#)
- [Verifying That Screen Reader Support Is Enabled](#)

Note: If Screen Reader support is enabled, then all pages related to *Refresh Process Status* are not refreshed automatically because PPR is turned off. This is an expected behavior.

G.1 Enabling Enterprise Manager Accessibility Mode

To enable screen reader mode, do the following:

1. On the Cloud Control home page, from the <user_name> menu, select **My Preferences** and then select **Accessibility**.
2. In the Accessibility Preference page, select **I use a screen reader**. Click **Apply**.

ADF accessibility mode is a session based setting which takes place immediately and does not require you to restart the Enterprise Manager Management Service.

For ADF pages, you will see an Accessibility Preferences dialog after logging into Cloud Control for the first time. The settings in this dialog are the same as those in the Accessibility Preference page mentioned above.

G.2 Setting uix-config.xml Flag

To enable screen reader mode for UIX pages, do the following:

1. Locate the uix-config.xml configuration file.

To locate the uix-config.xml file in a Cloud Control installation, change directory to the following location in the Oracle Management Service home:

```
./oms/sysman/archives/emgc/deployments/EMGC_  
DOMAIN/emgc.ear/em.war/WEB-INF/uix-config.xml
```

2. Open the uix-config.xml file using a text editor and set the following entry:

```
<!-- An alternate configuration that disables accessibility features -->  
<default-configuration>  
<accessibility-mode>screenReader</accessibility-mode>  
</default-configuration>
```

3. Save and close the file.
4. Restart the Oracle Management Service.

Note: UIX accessibility mode is a product-wide setting. You will have to restart the Enterprise Manager Management Service for this setting to take effect.

Note: In the uix-config.xml file, enable-auto-table-ctrl-labels is set to true. This enables tool tip boxes containing labels to appear when you hover your cursor over UI elements such as checkboxes and radio buttons in tables. To disable this function, change the setting to false.

G.3 Configuring web.xml File

To configure web.xml file, follow these steps:

1. Locate the web.xml configuration file.

To locate the web.xml file in a Cloud Control installation, change directory to the following location in the Oracle Management Service home:

```
./oms/sysman/archives/emgc/deployments/EMGC_  
DOMAIN/emgc.ear/em.war/WEB-INF/web.xml
```

2. Open the web.xml file with your favorite text editor and locate the following six lines of the file:

```
<!-- Uncomment this to enable textual chart descriptions  
<context-param>  
<param-name>enableChartDescription</param-name>  
<param-value>true</param-value>  
</context-param>  
-->
```

3. Remove comments from this section by deleting the first line and the last line of this section so that the section consists of only these 4 lines:

```
<context-param>
```

```
<param-name>enableChartDescription</param-name>
<param-value>true</param-value>
</context-param>
```

4. Save and exit the file.
5. Restart the Oracle Management Service.

G.4 Verifying That Screen Reader Support Is Enabled

Throughout Enterprise Manager, charts are used to display performance data. For most users, these charts provide a valuable graphical view of the data that can reveal trends and help identify minimum and maximum values for performance metrics.

However, charts do not convey information in a manner that can be read by a screen reader. To remedy this problem, you can configure Enterprise Manager to provide a complete textual representation of each performance chart. By default, support for the textual representation of charts is disabled. When textual description for charts is enabled, Enterprise Manager displays a small icon for each chart that can be used as a drill-down link to the textual representation.

To verify whether Screen Reader support has been enabled for ADF pages, follow these steps:

1. On the Cloud Control home page, click **Help** and then select **About Enterprise Manager**.
2. In the About Enterprise Manager dialog box, ensure that **Accessibility Preference - Screen Reader Support** is set to **Enabled**.
3. If **Accessibility Preference - Screen Reader Support** is set to **Disabled**, follow the steps listed in [Enabling Enterprise Manager Accessibility Features](#).

To verify whether Screen Reader support has been enabled for UIX pages, follow these steps:

1. On the Cloud Control home page, from the **Enterprise** menu, select **Reports** and then select **Information Publisher Reports**.
2. In the Information Publisher Reports page, click **Hardware Summary**. The Hardware Summary page is displayed. If accessibility setting has been enabled, you will see the icon shown in [Figure G-1](#):

Figure G–1 *Icon Representing Textual Representation of Charts*



Configuring Targets for Failover in Active/Passive Environments

This section provides a general reference for Cloud Control administrators who want to relocate Cold Failover Cluster (CFC) targets from one existing Management Agent to another. Although the targets are capable of running on multiple nodes, these targets run only on the active node in a CFC environment.

CFC environments commonly use a combination of cluster software to provide a virtual host name and IP address along with interconnected host and storage systems to share information and provide high availability (HA) for applications. Automating failover of the virtual host name and IP, in combination with relocating the Enterprise Manager targets and restarting the applications on the passive node, requires the use of the Oracle Enterprise Manager command-line interface (EM CLI) and Oracle or third-party cluster software. Several Oracle partner vendors offer clusterware solutions in this area.

This chapter covers the following topics:

- [Target Relocation in Active/Passive Environments](#)
- [Installation and Configuration](#)
- [Failover Procedure](#)
- [Failback Procedure](#)
- [EM CLI relocate_targets Parameters](#)
- [Relocation Script](#)

H.1 Target Relocation in Active/Passive Environments

With Oracle Enterprise Manager 12c, a single Oracle Management Agent running on each node in the cluster can monitor targets configured for active/passive high availability. Only one Management Agent is required on each of the physical nodes of the CFC cluster because, in case of a failover to the passive node, Enterprise Manager can move the HA monitored targets from the Management Agent on the failed node to another Management Agent on the newly activated node using a series of EMCLI commands. See the *Oracle® Enterprise Manager Command Line Interface* manual for more information.

If your application is running in an active/passive environment, the clusterware brings up the applications on the passive node in the event that the active node fails. For Enterprise Manager to continue monitoring the targets in this type of configuration, the existing Management Agent needs additional configuration.

The following sections describe how to prepare the environment to automate and restart targets on the new active node. Failover and failback procedures are also provided.

H.2 Installation and Configuration

The following sections describe how to configure Enterprise Manager to support a CFC configuration using the existing Management Agents communicating with the Oracle Management Service processes:

- [Prerequisites](#)
- [Configuration Steps](#)

H.2.1 Prerequisites

The following steps assume that the monitored targets have already been installed and configured for failover in a CFC.

Prepare the Active/Passive environments as follows:

- Ensure the operating system clock is synchronized across all nodes of the cluster. (Consider using Network Time Protocol (NTP) or another network synchronization method.)
- Install management agents on each node in the cluster using the physical hostname. Install the Management Agent on a local disk volume on each node in the cluster. Once installed, the Management Agents are visible in the Cloud Control console.
- Install and configure EMCLI on each node in the CFC cluster. See the *Oracle® Enterprise Manager Command Line Interface Guide* for more information.

H.2.2 Configuration Steps

The following steps show how to configure Enterprise Manager to support a CFC configuration using the existing Management Agents that are communicating with the OMS processes. The example that follows is based on a configuration with a two-node cluster that has one failover group.

Configuration involves two steps:

- [Discovering Targets](#)
- [Deploying Plug-ins](#)

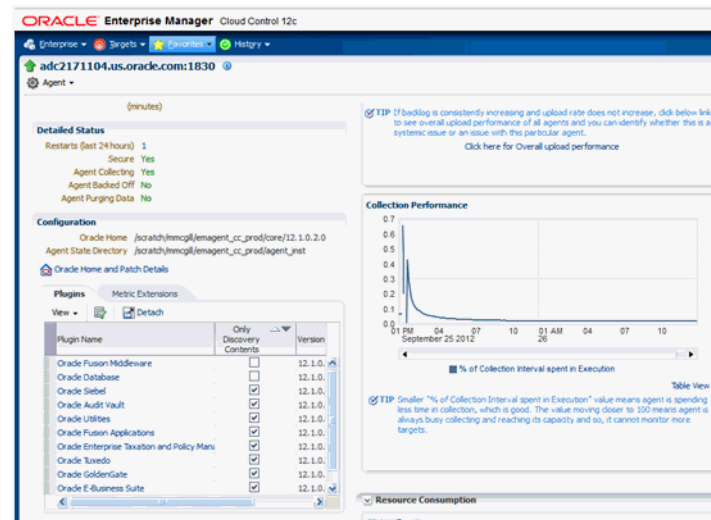
H.2.2.1 Discovering Targets

After the Active / Passive targets have been configured, use the Add Targets Manually screens in the Cloud Control console to add the targets (such as database, listener, application server, and so on). This screen can be accessed by navigating to Setup | Add Target | Add Targets Manually. You should perform this step specifying the active node (the node that is currently hosting the target to be added).

H.2.2.2 Deploying Plug-ins

After the target has been added determine which plug-ins have been deployed on the agent for the active host. This can be found by navigating to the agent homepage and viewing the plug-ins tab in the Configuration region.

Figure H-1 Agent Home Page



Make a note of the Plug-ins that do not have the Only Discovery Contents box checked. These plug-ins need to be deployed on the agent of the passive node.

After determining which plug-ins are missing by looking at the Agent homepage of the passive node, deploy any missing plug-ins by navigating to Setup | Extensibility | Plug-ins, selecting the relevant plug-in and using the Deploy on Management Agent menu to deploy the plug-in.

H.3 Failover Procedure

To speed relocation of targets after a node failover, configure the following steps using a script that contains the commands necessary to automatically initiate a failover of a target. Typically, the clusterware software has a mechanism with which you can automatically execute the script to relocate the targets in Enterprise Manager. Also, see "Relocation Script" on page H-5 for a sample script.

1. Shut down the target services on the failed active node.

On the active node where the targets are running, shut down the target services running on the virtual IP.

2. If required, disconnect the storage for this target on the active node.

Shut down all the applications running on the virtual IP and shared storage.

3. Enable the target's IP address on the new active node.

4. If required, connect storage for the target on the currently active node.

5. Relocate the targets in Cloud Control using EM CLI.

To relocate the targets to the Management Agent on the new active node, run the EM CLI *relocate_targets* verb for each target type (such as a listener or application servers) that you must relocate after the failover operation.

Example:

```
emcli relocate_targets
-src_agent=<node 1>:3872
-dest_agent=<node 2>:3872
-target_name=<database_name>
```

```
-target_type=oracle_database
-copy_from_src
-force=yes
```

In this example, port 3872 is the default port for the Management Agent. To find the appropriate port number for your configuration, use the value for the Agent URL parameter. You can determine this parameter by running the following command for the Management Agent:

```
emctl status agent
```

Note: In case of a failover event, the source Agent may not be running. However, there is no need to have the source Management Agent running to accomplish the relocate operation. EM CLI is an OMS client that performs its relocate operations directly against the Management Repository.

6. Bring up all targets on the new active node.
7. From the Enterprise Manager console, ensure all relocated targets are up and running .

H.4 Failback Procedure

To return the HA targets to the original active node, or to any other cluster member node:

1. Repeat the steps in ["Failover Procedure"](#) on page H-3 to return the HA targets to the active node.
2. Verify the target status in the Enterprise Manager console.

H.5 EM CLI relocate_targets Parameters

As shown in [Section H.3, "Failover Procedure"](#), you run the EM CLI `relocate_targets` verb for each target type that will be failed over to (or be switched over) during relocation operations. [Table H-1, "relocate_targets Verb Parameters"](#) documents the verb parameters associated with this EM CLI verb.

Table H-1 *relocate_targets Verb Parameters*

EM CLI Parameter	Description
-src_agent	Management Agent on which the target was running before the failover occurred.
-dest_agent	Management Agent that will be monitoring the target after the failover.
-target_name	Name of the target to be failed over.
-target_type	Type of target to be failed over (internal Enterprise Manager target type). For example, the Oracle database (for a standalone database or an Oracle RAC instance), the Oracle listener for a database listener, and so on.

Table H-1 (Cont.) relocate_targets Verb Parameters

EM CLI Parameter	Description
-copy_from_src	Use the same type of properties from the source Management Agent to identify the target. This is a MANDATORY parameter. Not supplying this parameter may result in the corruption of the target definition.
-force	Force dependencies (if needed) to failover as well.

H.6 Relocation Script

The following example shows a relocation script that can be executed from a clusterware configuration when a failover operation occurs.

Before running the script:

- Set up the *Default Normal Host Credential* with *Normal Host Credential*.
- Set up the *Target Preferred Credential* of the database instance with the *Normal Database Credential*, *SYSDBA Database Credential*, and *Database Host Credential*.

H.6.1 Relocation Script Example

```
#!/bin/ksh
#get the status of the targets

emcli get_targets
-targets="db1:oracle_database;listener_db1:oracle_listener"
-noheader

if [[ $? != 0 ]]; then exit 1; fi

# blackout the targets to stop false errors. This blackout is set to expire in 30
minutes.

emcli create_blackout
-name="relocating active passive test targets"
-add_targets="db1:oracle_database;listener_db1:oracle_listener"
-reason="testing failover"
-schedule="frequency:once;duration:0:30"

if [[ $? != 0 ]]; then exit 1; fi

# relocate the targets to the new host

emcli relocate_targets
-src_agent=host1.us.oracle.com:3872
-dest_agent=host2.us.oracle.com:3872
-target_name=db1 -target_type=oracle_database
-copy_from_src -force=yes

if [[ $? != 0 ]]; then exit 1; fi

emcli relocate_targets
-src_agent=host1.us.oracle.com:3872
-dest_agent=host2.us.oracle.com:3872
-target_name=listener_db1
-target_type=oracle_listener
-copy_from_src -force=yes
```

```
if [[ $? != 0 ]]; then exit 1; fi

# End the blackout and let the targets become visible

emcli stop_blackout
-name="relocating active passive test targets"

if [[ $? != 0 ]]; then exit 1; fi

# Recheck the status of the targets

emcli get_targets
-targets="db1:oracle_database;listener_db1:oracle_listener"
-noheader

if [[ $? != 0 ]]; then exit 1; fi
```

Troubleshooting

This appendix describes how to troubleshoot issues that you might encounter while working with Enterprise Manager Cloud Control.

- [Troubleshooting Configuration Assistant Failures](#)
- [Troubleshooting ADP and JVM D Failures](#)
- [Troubleshooting Package-Related Issues](#)
- [Troubleshooting Deinstallation Failures](#)

I.1 Troubleshooting Configuration Assistant Failures

This section describes the log files you must review and the actions you must take when the following configuration assistants fail:

- [Plugins Prerequisite Check Configuration Assistant](#)
- [Repository Configuration Assistant](#)
- [Repository Out Of Box Configuration Assistant](#)
- [MDS Schema Configuration Assistant](#)
- [OMS Configuration Assistant](#)
- [Plugins Deployment and Configuration Configuration Assistant](#)
- [Start Oracle Management Service Configuration Assistant](#)
- [Plugins Inventory Migration Configuration Assistant](#)
- [Oracle Configuration Manager Repeater Configuration Assistant](#)
- [OCM Configuration for OMS Configuration Assistant](#)
- [Agent Configuration Assistant](#)
- [Agent Upgrade Configuration Assistant](#)
- [Repository Upgrade Configuration Assistant](#)
- [Stopping APM Engines Configuration Assistant](#)
- [Stop Admin Server Configuration Assistant](#)

I.1.1 Plugins Prerequisite Check Configuration Assistant

Log Files

Review the following log files:

- `$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log`
- `$<OMS_HOME>/cfgtoollogs/pluginca/configplugin_prereq_check_<timestamp>.log`

Workaround Steps

Run the following command:

```
$<OMS_HOME>/oms/bin/pluginca -action prereqCheck -oracleHome <oms_home_path> -middlewareHome <middleware_home_path> -plugins <plugin_id>=<plugin_version>
```

Note: For multiple plug-ins, separate the plug-in details with a comma. For example, `-plugins <plugin_id>=<plugin_version>, <plugin_id>=<plugin_version>`

I.1.2 Repository Configuration Assistant

Log Files

Review the following log files:

- `$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log`
- `$<OMS_HOME>/sysman/log/schemamanager/m_<timestamp>/m_<timestamp>.<ACTION>/`

Note: `<ACTION>` refers to any of the schema actions, for example, `CREATE`, `TRANSX`, `MY_ORACLE_SUPPORT`, and so on.

Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.
2. Clean up the Management Repository by running the following command:

```
$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager <repository_database_host> <repository_database_port> <repository_database_sid> -action dropall -dbUser <repository_database_user> -dbPassword <repository_database_password> -dbRole <repository_database_user_role> -mwHome <middleware_home> -mwOraHome <oms_oracle_home> -oracleHome <oms_oracle_home>
```

Note:

- For Microsoft Windows, invoke `RepManager.bat`.
 - RepManager 12.1 supports `-action dropall` and `-action drop`, which drop SYSMAN, SYSMAN_MDS, SYSMAN_APM, SYSMAN_OPSS, and SYSMAN_RO. RepManager 11.1 supports `-action dropall`, which drops only SYSMAN and SYSMAN_MDS, and `-action drop`, which drops only SYSMAN. RepManager 10.2.0.5 supports `-action drop`, which drops only SYSMAN.
-

3. Rerun the configuration assistant.

If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

If you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.sh` script (`runConfig.bat` on Microsoft Windows) from OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

If you are installing in silent mode, then rerun the `runConfig.sh` script from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

If the `runConfig.sh` script fails, then clean up your environment and redo the installation.

Note: For Microsoft Windows, run `runConfig.bat`.

I.1.3 Repository Out Of Box Configuration Assistant

Log Files

Review the following log file:

```
$<OMS_HOME>/sysman/log/schemamanager/m_<timestamp>/m_<timestamp>.<ACTION>/
```

Workaround Steps

1. Resolve the cause of the issue.

Caution: Do NOT clean up or drop the Management Repository.

2. Rerun the configuration assistant.

If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

If you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.sh` script (`runConfig.bat` on Microsoft Windows) from OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

If you are installing in silent mode, then rerun the `runConfig.sh` script from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

If the `runConfig.sh` script fails, then clean up your environment and redo the installation.

Note: For Microsoft Windows, run `runConfig.bat`.

I.1.4 MDS Schema Configuration Assistant

Log Files

Review the following log file:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/emmdscreate_<timestamp>.log
```

For more information, review the following log files:

- <OMS_HOME>/sysman/log/schemamanager/m_<timestamp>/m_<timestamp>.CREATE/mds.log
- \$<OMS_HOME>/sysman/log/schemamanager/m_<timestamp>/m_<timestamp>.CREATE/rcu.log

Workaround Steps

Follow these steps:

1. Drop the MDS schema by running the following command from the OMS home:

```
$<OMS_HOME>/sysman/admin/emdrep/bin/mdsschemamanager.pl
-action=-dropRepository -connectString=<database_connect_string>
-dbUser= <database_user> -dbPassword=<database_password>
-oracleHome=<OMS_oracle_home> -mwHome=<middleware_home>
```

Where <database_connect_string> must be in the following format:<database_host>:<database_port>:<database_sid>

2. Rerun the Configuration Assistant.

If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

If you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the runConfig.sh script (runConfig.bat on Microsoft Windows) from OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

If you are installing in silent mode, then rerun the runConfig.sh script (runConfig.bat on Microsoft Windows) from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

If the runConfig.sh script fails, then clean up your environment and redo the installation.

Note: For Microsoft Windows, run runConfig.bat.

I.1.5 OMS Configuration Assistant

Log Files

Review the following log files:

- If the installer fails BEFORE the OMS configuration assistant starts running, then review the following log file:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
```

- If the installer fails AFTER the OMS configuration assistant starts running, then review the following log file:

```
$<OMS_HOME>/cfgtoollogs/omsca/omsca_<timestamp>.log
```

Workaround Steps

Follow these steps:

1. Check whether any Java processes are running from the Middleware home. To do so, run the following command from the host where the OMS is running:

```
ps -ef | grep java | grep <Oracle_Middleware_Home>
```

2. Kill all the running processes, except for installer-related Java processes, by running the following command. The installer-related Java processes run from the temp directory, so you can ignore the processes from that directory.

```
kill -9 <process_id>
```

3. Remove the Oracle Management Service Instance Base by running the following command:

```
rm -rf <OMS_Instance_Home>
```

4. Rerun the Configuration Assistant.

If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

If you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the runConfig.sh script (runConfig.bat on Microsoft Windows) from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>  
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

If you are installing in silent mode, then rerun the runConfig.sh script (runConfig.bat on Microsoft Windows) from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>  
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

If the runConfig.sh script fails, then clean up your environment and redo the installation.

Note: For Microsoft Windows, run runConfig.bat.

I.1.6 Plugins Deployment and Configuration Configuration Assistant

Log Files

Review the following log files:

- \$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
- \$<OMS_HOME>/cfgtoollogs/pluginca/configplugin_deploy_<timestamp>.log

Workaround Steps

Run the following command:

```
$<OMS_HOME>/oms/bin/pluginca -action deploy -oracleHome <oms_home_path>
-middlewreHome <middleware_home_path> -plugins <plugin_id>=<plugin_
version>
```

Note: For multiple plug-ins, separate the plug-in details with a comma. For example, -plugins <plugin_id>=<plugin_version>, <plugin_id>=<plugin_version>

I.1.7 Start Oracle Management Service Configuration Assistant

Log Files

Review the following log file:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
```

Workaround Steps

Run the following command:

```
$<OMS_HOME>/bin/emctl start oms
```

I.1.8 Plugins Inventory Migration Configuration Assistant

Log Files

Review the following log file:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
```

Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.
2. Rerun the configuration assistant.

If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

If you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the runConfig.sh script (runConfig.bat on Microsoft Windows) from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

If you are installing in silent mode, then rerun the runConfig.sh script from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

If the runConfig.sh script fails, then clean up your environment and redo the installation.

Note: For Microsoft Windows, run runConfig.bat.

I.1.9 Oracle Configuration Manager Repeater Configuration Assistant

Log Files

Review the following log file:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
```

Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.
2. Rerun the configuration assistant.

If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

If you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.sh` script (`runConfig.bat` on Microsoft Windows) from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>  
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

If you are installing in silent mode, then rerun the `runConfig.sh` script (`runConfig.bat` on Microsoft Windows) from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>  
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

If the `runConfig.sh` script fails, then clean up your environment and redo the installation.

Note: For Microsoft Windows, run `runConfig.bat`.

I.1.10 OCM Configuration for OMS Configuration Assistant

Log Files

Review the following log file:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
```

Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.
2. Rerun the configuration assistant.

If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

If you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.sh` script (`runConfig.bat` on Microsoft Windows) from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>  
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

If you are installing in silent mode, then rerun the `runConfig.sh` script (`runConfig.bat` on Microsoft Windows) from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

If the `runConfig.sh` script fails, then clean up your environment and redo the installation.

Note: For Microsoft Windows, run `runConfig.bat`.

I.1.11 Agent Configuration Assistant

Log Files

Review the following log files:

- `$<AGENT_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log`
- If secure fails, then review the following log file:

```
$<AGENT_INSTANCE_HOME>/sysman/log/secure.log
```

- In the log file, search for the following statement:

```
SEVERE:Plugin configuration has failed.
```

If you find this statement, then review the following log file:

```
$<AGENT_INSTANCE_HOME>/install/logs/agentplugindeploy_<timestamp>.log
```

Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.
2. Rerun the configuration assistant.

If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

If you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.sh` script (`runConfig.bat` on Microsoft Windows) from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

If the `runConfig.sh` script fails, then clean up your environment and redo the installation.

Note: For Microsoft Windows, run `runConfig.bat`.

If you are installing in silent mode, then run the following command from the Management Agent home:

```
$<AGENT_HOME>/sysman/install/agentDeploy.sh AGENT_BASE_DIR=<agent_base_dir_path>
OMS_HOST=<oms_host_name> EM_UPLOAD_PORT=<oms_upload_https_port>
AGENT_REGISTRATION_PASSWORD=<agent_reg_password> -configOnly
```

Note: Enter the HTTPS port (secure port) for the EM_UPLOAD_PORT argument.

I.1.12 Agent Upgrade Configuration Assistant

Log Files

If the agent upgrade configuration assistant fails, then review the following log file:

```
$<AGENT_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
```

Workaround Steps

Resolve the cause of the issue, and rerun the configuration assistant from the Jobs page of the Enterprise Manager Cloud Control console.

Note: The Jobs page referred to here is the page within the earlier release of the Enterprise Manager Cloud Control console.

I.1.13 Repository Upgrade Configuration Assistant

Log Files

Review the following log files:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/emmdscreate_<timestamp>.log
```

```
$<OMS_HOME>/sysman/log/schemamanager/m_<timestamp>/m_<timestamp>.<ACTION>/
```

Note: (<ACTION> refers to any of the schema actions, for example, PREUPGRADE, UPGRADE, TRANSX, and so on.)

Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.
2. Rerun the configuration assistant.

If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

If you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the runConfig.sh script (runConfig.bat on Microsoft Windows) from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>  
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0.xml}
```

If you are installing in silent mode, then rerun the runConfig.sh script (runConfig.bat on Microsoft Windows) from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>  
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0.xml}
```

If the runConfig.sh script fails, then clean up your environment and redo the installation.

Note: For Microsoft Windows, run `runConfig.bat`.

I.1.14 Stopping APM Engines Configuration Assistant

Log Files

Review the following log file:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
```

Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.
2. Rerun the configuration assistant.

If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

If you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.sh` script (`runConfig.bat` on Microsoft Windows) from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>  
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

If you are installing in silent mode, then rerun the `runConfig.sh` script (`runConfig.bat` on Microsoft Windows) from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>  
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

If the `runConfig.sh` script fails, then clean up your environment and redo the installation.

Note: For Microsoft Windows, run `runConfig.bat`.

I.1.15 Stop Admin Server Configuration Assistant

Log Files

Review the following log file:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
```

Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.
2. Rerun the configuration assistant.

If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

If you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.sh` script (`runConfig.bat` on Microsoft Windows) from the OMS home:


```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0.xml}
```

If you are installing in silent mode, then rerun the runConfig.sh script (runConfig.bat on Microsoft Windows) from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0.xml}
```

If the runConfig.sh script fails, then clean up your environment and redo the installation.

Note: For Microsoft Windows, run runConfig.bat.

I.2 Troubleshooting ADP and JVM D Failures

This section describes how to troubleshoot the errors encountered while deploying ADP/JVM D Engines, and ADP/JVM D Agents:

- [ADP Engine Name Conflict](#)
- [Failure to Deploy ADP Agent On a Target](#)
- [SSL Handshake Failure Agent Deployment Errors](#)
- [Copying ADP Agent Zip or Javadiagnosticagent.ear Failure](#)

I.2.1 ADP Engine Name Conflict

Error

When you deploy ADP Engine to an existing managed server whose instance (for example: EMGC_ADPEENGINE2) has not been completely removed, then the new deployment of ADP Engine with the same name fails on the unzip step with the following error:

```
@ Are you sure you haven't deployed adp engine to a managed server with name
@ <ADP_managed_server> already?
```

Workaround Steps

To remove the existing managed server completely, perform the following steps:

1. Follow the steps listed in [Chapter 19](#) to remove the ADP Engine application and the managed server to which the ADP application is deployed.
2. Connect to the host machine where the managed server was present, and navigate to the following location to manually delete the managed server (EMGC_ENGINE2):

```
$DOMAIN_HOME/<ADP_managed_server>
```

Where, \$DOMAIN_HOME is the location of the Cloud Control domain

I.2.2 Failure to Deploy ADP Agent On a Target

Error

While deploying the ADP Agent, the deployment job may fail on the Deploy ADP Agent On Target step, with the following error:

Failed to connect to
https://<host>:<port>/HttpDeployer/HttpDeployerServlet

Also, if you check the output of the Deploy HttpDeployer OnTarget (the previous step), then you will see a message as follows:

Operation is pending and will be activated or cancelled when the ongoing edit session is activated or cancelled.

Workaround Steps

To correct this error, perform the following steps:

1. Log into WebLogic Administration Console of the domain where the ADP Agent was to be deployed.
2. On the Administration home page, click **Save Changes** or **Discard Changes**, and start deploying the ADP agent afresh.

I.2.3 Failure to Deploy JVM D Agent On a Target

Error

While deploying a JVM D Agent on a target, the *Deploy HTTPDeployer On Target* job step fails due to an SSL handshake failure. This error may occur if the appropriate patch is not applied on the WebLogic Server software.

Workaround Steps

Apply the appropriate patch on your Oracle WebLogic Server software, then retry the deployment. The appropriate patches for different versions of Oracle WebLogic Server are mentioned in [Table I-1](#). Note that if you are deploying a JVM D Agent on Oracle WebLogic Server 9.2.4 or higher, or Oracle WebLogic Server 10.3.2 or higher, you do not need to apply a patch, as the fix is already present in these versions.

Table I-1 Oracle WebLogic Server Patches to be Applied

Oracle WebLogic Server Version	Patch to be Applied
9.1.0	Patch 8422724
9.2.0	Patch 9384535
9.2.1	Patch 9032735
9.2.2	Patch 9309512
9.2.3	Patch 8849418
10.0.0	Patch 8422724
10.0.1	Patch 8895699
10.0.2	Patch 8896127
10.3.0	Patch 8715553
10.3.1	Patch 9003716

I.2.4 SSL Handshake Failure Agent Deployment Errors

Error

If the WebLogic Domain is SSL enabled using a demo certificate, then the agent deployment may fail due to an SSL Handshake Failure. The following error normally occurs because the demo certificate is not present in `AgentTrust.jks`:

```
Certificate chain received from myhost.acme.com - 123.34.11.11 was not
trusted causing SSL handshake failure. Check the certificate chain to
determine if it should be trusted or not. If it should be trusted, then
update the client trusted CA configuration to trust the CA certificate
that signed the peer certificate chain. If you are connecting to a WLS
server that is using demo certificates (the default WLS server behavior),
and you want this client to trust demo certificates, then specify
-Dweblogic.security.TrustKeyStore=DemoTrust on the command line for this
client.
```

Note: If the WebLogic Domain is using a production certificate, then this issue will not occur as `AgentTrust.jks` has trusted certificates from all well known CA's.

Workaround Steps

To correct the error, import WebLogic demo certificate to Management Agent keystore as follows:

1. Export WebLogic Demo certificate from `cacerts` file. This file is present under the WebLogic home of the Middleware installation at the following location:

```
keytool -export -keystore $WEBLOGIC_HOME/server/lib/cacerts -alias
certgencab -file mycert.cer
```

Press **Enter** when prompted for a password.

2. Import WebLogic Demo certificate to TrustStore of Oracle Management Agent as follows:

```
keytool -import -keystore $ORACLE_
HOME/core/12.1.0.0.0/stage/sysman/config/montrust/AgentTrust.jks -alias
wlscertgencab -file mycert.cer
```

Enter the password **welcome** when prompted, and press **Enter**.

To check if the certificate has been imported correctly, run the following command:

```
keytool -list -keystore $ORACLE_
HOME/core/12.1.0.0.0/stage/sysman/config/montrust/AgentTrust.jks
```

Where, `$ORACLE_HOME` is Oracle Management Agent home.

Press **Enter** when prompted for password, a certificate with the name `wlscertgencab` is generated with the current date.

I.2.5 Copying ADP Agent Zip or Javadiagnosticagent.ear Failure

Error

If the users who installed the OMS, and the Management Agent are not in the same group, then the job fail on Copying ADP Agent Zip step for an ADP agent, and Copy Javadiagnosticagent Ear step for a JVM D agent, with the following error:

```
oracle.sysman.emSDK.emd.comm.RemoteOperationException: Error while streaming
JobReader:java.io.IOException: Broken pipe
```

Workaround Steps

To correct the error, either install the Enterprise Manager Agent using OMS host user credentials.

OR

Enable `sudo` or `Powerbroker` settings for the agent host, so that the job runs as if run by an OMS host user.

To set the `sudo`, or `Powerbroker` settings, do the following:

1. In Cloud Control, from the **Setup** menu, select **Security**, and then click **Privilege Delegation**.
2. On the Manage Privilege Delegation Settings page, do the following:
 - a. Select the **Sudo** or **PowerBroker** from the type menu.
 - b. Enter the host name, or alternatively select the name from the list of host targets. Ensure that the host selected corresponds to the Management Agent; this agent must be the one monitoring the WebLogic Domain where the ADP/JVMD agents have to be deployed.
 - c. Click **Go**.

I.3 Troubleshooting Package-Related Issues

While installing Enterprise Manager Cloud Control, you might see the following error message:

```
Lin.X64 SUSE 10 : Backup fails with the given below error
install_driver(Oracle) failed: Attempt to reload DBD/Oracle.pm aborted.
Compilation failed in require at (eval 15) line 3.
```

If you see this error, then install the following packages, and try again.

- libaio-32bit-0.3.104-14.2
- libaio-devel-32bit-0.3.104-14.2

I.4 Troubleshooting Deinstallation Failures

While deinstalling the *Shared Agent* as described in [Section 18.1.2.3](#), you might see the following error:

```
SEVERE:The home <AGENT_HOME> cannot be deinstalled. Please deinstall all
referenced home(s) <REFERENCE_HOME>
```

For example,

```
SEVERE:The home /tmp/agt_install/core/12.1.0.1.0 cannot be deinstalled. Please
deinstall all referenced home(s) /tmp/agt_install/plugins
```

If you see the error, then deinstall the *Shared Agent* following these steps:

1. Identify the dependent plug-ins and the `sbin` home to be detached from the Central Inventory:
 - a. On the host where the *Shared Agent* is installed, open the following file from the Central Inventory:


```
<absolute_path>/oraInventory/ContentsXML/inventory.xml
```

- b. Make a note of the dependent plug-ins listed within the <REFHOMELIST> and </REFHOMELIST> tags.

For example,

```
<HOME NAME="nfs5515" LOC="/home/john/software/oracle/agent/core/12.1.0.0.0"
TYPE="O" IDX="1">
<REFHOMELIST>
<REFHOME
LOC="/home/john/software/oracle/agent/plugins/oracle.sysman.oh.discovery.pl
ugin_12.1.0.0.0"/>
<REFHOME
LOC="/home/john/software/oracle/agent/plugins/oracle.sysman.db.discovery.pl
ugin_12.1.0.0.0"/>
<REFHOME
LOC="/home/john/software/oracle/agent/plugins/oracle.sysman.emas.discovery.
plugin_12.1.0.0.0"/>
<REFHOME
LOC="/home/john/software/oracle/agent/plugins/oracle.sysman.oh.agent.plugin
_12.1.0.0.0"/>
</REFHOMELIST>
</HOME>
```

- c. Make a note of the sbin directory listed within the <REFHOMELIST> and </REFHOMELIST> tags.

For example,

```
<HOME NAME="nfs5515" LOC="/home/john/software/oracle/agent/core/12.1.0.0.0"
TYPE="O" IDX="1">
<REFHOMELIST>
<REFHOME LOC="home/john/software/oracle/agent/sbin"/>
</REFHOMELIST>
```

- d. Detach the dependent plug-ins you identified in Step 1 (b) from the Central Inventory. To do so, run the following command from the *Master Agent* home that is visible on the host where your *Shared Agent* is installed:

```
$<AGENT_HOME>/oui/bin/runInstaller -detachHome -silent
-waitForCompletion -invPtrLoc <absolute_path>/oraInst.loc ORACLE_
HOME=<plug-in_home> -nogenerateGUID
```

For example,

```
/home/john/software/oracle/agent/core/12.1.0.3.0/oui/bin/runInstall
er -detachHome -silent -waitForCompletion -invPtrLoc
/home/john/software/oracle/agent/core/12.1.0.3.0/oraInst.loc
ORACLE_
HOME=/home/john/software/oracle/agent/plugins/oracle.sysman.emas.di
scovery.plugin_12.1.0.3.0 -nogenerateGUID
```

Note: This step detaches only one plug-in at a time. Therefore, if you have multiple plug-ins, repeat this step to detach every other dependent plug-in.

- e. Detach the sbin home you identified in Step 1 (c) from the Central Inventory. To do so, run the following command from the *Master Agent* home that is visible on the host where your *Shared Agent* is installed:

```
$<AGENT_HOME>/oui/bin/runInstaller -detachHome -silent
-waitForCompletion -invPtrLoc <absolute_path>/oraInst.loc ORACLE_
HOME=<sbin_home> -nogenerateGUID
```

For example,

```
/home/john/software/oracle/agent/core/12.1.0.3.0/oui/bin/runInstall
er -detachHome -silent -waitForCompletion -invPtrLoc
/home/john/software/oracle/agent/core/12.1.0.3.0/oraInst.loc
ORACLE_HOME=/home/john/software/oracle/agent/sbin -nogenerateGUID
```

2. **Deinstall the *Shared Agent*.** To do so, run the following command from the *Master Agent* home that is visible on the host where your *Shared Agent* is installed:

```
$<AGENT_HOME>/perl/bin/perl <AGENT_
HOME>/sysman/install/NFSAgentDeInstall.pl AGENT_INSTANCE_
HOME=<absolute_path_to_agent_instance_home> ORACLE_HOME=<absolute_path_
to_agent_home>
```

For example,

```
/home/john/software/oracle/agent/core/12.1.0.3.0/perl/bin/perl
/home/john/software/oracle/agent/core/12.1.0.3.0/sysman/install/NFSAgen
tDeInstall.pl AGENT_INSTANCE_
HOME=/home/john/software/oracle/agent/agent_inst ORACLE_
HOME=/home/john/software/oracle/agent/core/12.1.0.3.0
```

I.5 Troubleshooting Management Agent Installation Failures

If the installation of a Management Agent fails, and the Management Agent deployment logs available at <ORACLE_HOME>/cfgtoollogs/agentDeploy/agentDeploy<TIMESTAMP>.log mention that the port check failed, then run the agentDeploy.sh script again, using the -ignorePrereqs option.

Also, if the port check failed for a host that has an IPv6 address listed as part of the host DNS setup, then ensure that the IPv6 address is enabled on the host.

Index

A

- accessibility, G-1
 - accessibility mode, G-1
 - configuring web.xml file, G-2
 - enabling accessibility mode, G-1
 - screen reader, G-3
 - screen reader support, G-3
 - uix-config.xml, G-2
 - web.xml File, G-2
- add host log files, B-5
- Add Host Status page, 7-18
- Add Host Target Wizard
 - overview, 2-10
- Add Host Targets Wizard, 1-8
 - best practice, 2-11
 - install types offered, 2-10
- Add Management Service deployment
 - procedure, 2-11
- Additional Standby OMS, removing, 20-1
- ADP, 13-1
- ADP agents, 13-2
- ADP architecture, 13-2
- ADP managers, 13-2
- agent base directory, 2-22
 - requirements, 6-6, 7-11
- agent home, 2-21
- agent installation logs, B-6
- agent instance directory, 2-22
- agent instance home, A-6
 - permissions, 6-6
 - requirements, 6-6
- agent plug-in home, 2-22
- AGENT_
 - HOME/sysman/admin/scripts/db/config/resp
onse.pl, 10-5
- agent_inst, 2-22
- agentDeploy.sh script
 - limitation, 6-3
 - location, 6-3
 - purpose, 6-1
 - software-only install, 9-1
- agentDeploy.sh script supported options, 6-23
- AgentNFS.pl script
 - alternate way, 8-17
 - purpose, 8-1

- response file, 8-17
- AgentPull.sh script, 6-1
 - response file, 6-18
- AgentPull.sh script supported options, 6-23
- allroot.sh script, 2-29, 4-16, 4-32
- Application Dependency and Performance, 13-1
 - advanced installation
 - architecture
 - advanced installation
 - facts, 13-2
 - postinstallation, 13-8
 - prerequisites, 13-2
 - procedure, 13-3
 - advanced installation options, 13-1
 - deinstallation
 - ADP Agents, 19-3
 - ADP Manager, 19-1
 - see* ADP
- Application Performance Management, 11-11
- application prerequisite logs, B-6
- assistive technology, G-1
- asynchronous I/O, 12-15

B

- Bad SQL
 - configuring the database to show Bad SQL, 10-4
- baselines, 12-9
- Beacons, 12-16
 - configuring firewalls to allow ICMP traffic, 11-11
- BI Publisher, 15-1
 - Administration, 15-19
 - Allowing Access, 15-10
 - Repository Access, 15-22
 - Troubleshooting, 15-22
 - Verifying Integration, 15-9
- BI Publisher Installation, 15-3
- BI Publisher Inventory, 15-3
- BI Publisher Security Model, 15-12
- BI Publisher, SSL, 15-17
- buffer cache, 12-13
- business intelligence publisher, A-2

C

- capacity

- predicting, 12-8
- central inventory, 6-7
- cksum command, 1-6
- Cloud Control
 - architecture overview, 12-1
 - components, 12-1
 - sizing, 12-8
- Cold Failover Cluster configuration, H-1
- Cold Failover Cluster, HA, H-1
- commands
 - data file commands
 - deleting data files, 17-5
 - deleting data files, 2-16
 - Enterprise Manager commands
 - deinstalling in GUI mode, 17-5, 17-6
 - deinstalling in silent mode, 17-9
 - management agent commands
 - deinstalling from all nodes in GUI mode, 18-2
 - deinstalling from all nodes in silent mode, 18-3, 18-4
 - shutting down management agent, 17-3
 - OMS commands
 - deleting OMS, 17-2
 - verifying file size, 1-6
- configuration assistants
 - overview, 2-23
 - resolving failures, 2-26
 - run by default, 2-23
- configuration logs, B-1
 - general, B-2
 - repository, B-2
 - sysman schema operation logs, B-2
- configureBIP script, 15-5
- Console Only Mode, 16-1
- console port, 2-12

D

- data collections
 - how Enterprise Manager stores, 10-1
 - understanding default and custom, 10-1
- data files, 2-16
 - deleting, 2-16
 - overview, 2-16
- database templates
 - handling errors, 3-7, 4-34
 - overview, 3-4, 4-5
 - providing details in installer, 4-20
 - providing details in response file, 3-13
 - resetting user account passwords, 3-13, 3-15, 4-21, 4-23, 4-36, 4-37
- DBSNMP user, 10-5
- default_collection directory, 10-1
- defaults assigned, 11-2
- deinstallation
 - deinstalling in GUI mode
 - deinstalling Enterprise Manager system, 17-1
 - deinstalling management agent, 18-1, 19-1
 - deinstalling management agent installed with RPM file, 18-6

- deinstalling in silent mode
 - deinstalling shared agent, 18-5
- Deinstalling ADP, 19-1
- Deinstalling JVMD, 19-5
- deploying JVMD agents, 14-10
- deployment procedure, 2-11
- deployment size
 - changing deployment size, 2-10
 - handling errors, 3-4, 3-7
 - overview, 2-9
 - running prerequisite checks, 2-10
 - selecting in installer, 4-21
 - small, medium, large, 2-9, 4-22
 - target count, agent count, session count, 2-9, 4-22
- DHCP, 2-28
- directories, A-1, A-2
 - Middleware Common home directory, A-1
 - Middleware WebTier home directory, A-1
 - Oracle Business Intelligence Publisher home, A-1
 - Oracle Management Agent home directory, A-1
 - Oracle Management Agent Plug-in home, A-1
 - Oracle Management Service home directory, A-1
 - Oracle Management Service Instance home directory, A-1
 - Oracle Management Service Plug-ins home, A-1
- directory structure, A-1
 - Oracle Management Agent, A-3
 - Oracle Management Service, A-3
 - Oracle Management Service home, A-2
- dontProxyFor
 - description of property, 11-10

E

- E2E monitoring, 12-16
- EMBIP* Roles
 - folder/catalog object access, 15-21
- EMBIPAdministrator, 15-12
- EMBIPAuthor, 15-12
- EMBIPScheduler, 15-12
- EMBIPViewer, 15-12
- EMCLI, 6-10, 6-14, 6-17
- emctl command, A-6
- Enterprise Manager
 - See* Oracle Enterprise Manager
- Enterprise Manager Cloud Control
 - configuration assistants, 2-23
 - deinstallation
 - dropping MDS schema, 17-3
 - dropping SYSMAN schema, 17-3
 - graphical mode, 17-5
 - overview, 17-1
 - prerequisites, 17-1, 17-3
 - silent mode, 17-7
 - deleting data files, 2-16
 - installation
 - software-only installation, 2-4
 - installation modes, 2-2
 - installation types, 2-3
 - installation wizard, 2-2

- ports
 - console port, 2-12
 - customizing ports, 2-13, 2-15
 - default ports, 2-12
 - HTTP port, 2-13
 - HTTPS port, 2-13
 - overview, 2-12
 - upload port, 2-12
- prerequisite checks, 2-26
- procuring from OTN
 - extracting contents, 1-6
 - verifying file size, 1-6
 - verifying platform information, 1-7
- silent installation
 - advanced installer options, 3-8
 - editing response file, 3-9
 - facts, 3-2
 - postinstall steps, 3-17
 - prerequisites, 3-5
 - procedure, 3-5
- software-only installation
 - configuration phase, 4-2
 - facts, 4-3
 - graphical mode, 4-7
 - installation phase, 4-1
 - overview, 4-1
 - prerequisites, 4-7
 - silent mode, 4-28
- upgrade
 - overview, 2-3
- Enterprise Manager Framework Security
 - in a firewall environment, 11-1
- Enterprise Manager Prerequisite Kit, B-4
- /etc/hosts file, 6-4

F

- Failover, active/passive environment, H-1
- Failover, Enterprise Manager, H-3
- Failover, relocate_targets verb, H-4
- files
 - RepManager.bat, 17-4
- firewalls
 - between browser and the Cloud Control, 11-5
 - between Cloud Control and a managed database target, 11-10
 - between Management Service and Management Agents, 11-11
 - between Management Service and Management Repository, 11-10
 - configuring for ICMP traffic, 11-11
 - configuring for UDP traffic, 11-11
 - configuring the Management Agent for, 11-5
 - configuring the Management Service for, 11-7
 - configuring to allow incoming data from Management Service, 11-9
 - configuring to allow incoming traffic to Management Agent, 11-7
 - considerations when using with multiple Management Services, 11-11

- First Standby OMS, removing, 20-3

G

- gc_inst, 2-21
- graphical mode, 2-2

H

- host list file, 2-29
- HTTP port, 2-13
- HTTPS port, 2-13
- Hyper-Threading, 12-12

I

- ICMP, 11-11
- ICMP echo request default port, 11-2
- initialization logs, B-5
- install logs, B-1
 - installActions, B-1
- installation base directory
 - permission, 7-10
 - requirements, 7-11
- installation types, 2-3
- installation wizard, 2-2
- installing JVMMD, 14-1
 - see also* remote deployment
 - separate host from the OMS, 14-3
- installing jvmd agents, 14-10
- instance directory
 - permission, 7-10
 - requirements, 8-10
- Integrating BI Publisher, 15-5
- Internet Control Message Protocol, 11-11
- invPtrLoc parameter, 2-20
- I/O Channels
 - monitoring, 12-15

J

- Java Development Kit
 - default version installed, 3-2
 - supported version, 2-17
- job_queue_processes, 10-6
- JROCKIT, 3-3
- JVM Diagnostics
 - advanced installation
 - architecture
 - postinstallation steps, 14-18
 - prerequisites, 14-3
 - procedure, 14-3
 - see* JVMMD
- JVM diagnostics, 14-1
- JVMD
 - architecture
- JVMD advanced install options, 14-1
- JVMD agents, 14-2
- JVMD Architecture, 14-1
- JVMD managers, 14-2

L

- licenses, 2-28
- Listener port
 - obtaining, 11-10
- Loader, 12-12
- loader threads, 12-12
- locked user account, 7-3
- Login Timeout Value
 - modifying the default, 10-6
- logs
 - application prerequisite logs, B-6
 - cfgfw/*.log, B-7
 - configuration logs, B-2
 - deployfwk.log, B-7
 - initialization logs, B-5
 - installation logs, B-1
 - install.log/.err, B-7
 - MDS schema operation logs, B-4
 - nfs_install.log/.err, B-7
 - Oracle Management Service log files, B-5
 - secure logs, B-5
 - sysman schema operation logs, B-2
 - system prerequisite logs, B-6
 - ui.log, B-7

M

- Management Agent, 12-1, 12-3, 12-9
 - configuring to allow incoming communication from the Management Service, 11-7
 - configuring to use a proxy server, 11-6
- management agent
 - deinstallation in GUI mode
 - overview, 18-1, 19-1
 - postdeinstall tasks, 18-6
 - installation
 - verifying, 6-26, 8-21
 - installation using response file
 - creating response file, 6-19, 6-22
 - prerequisites, 6-3
- management agent home, 2-21
- Management Servers
 - adding, 12-15
- Management Service, 12-1, 12-3
 - See* Oracle Management Service
- master agents, 8-1, 8-2
- MDS schema, 2-16
- MDS schema creation log, B-4
- MDS schema drop logs, B-4
- mgmt.dbf data file, 2-16
- middleware home
 - NFS-mounted drive, 3-4, 3-12, 4-6
- My Oracle Support
 - enabling OMS access, 11-9

N

- Named Credentials, 7-3
- new_install.rsp response file, 3-9
- nmosudo, 10-27

- node manager, 2-18
- node manager credentials, 2-18

O

- OEM_MONITOR, 10-5
- OMS home, 2-21
- OMS instance base location, 2-21
- OMS plug-in home, 2-22
- OpenSSH, 7-3, 8-2
- operating system groups, 6-4, 7-6, 8-5
- operating system requirements, 8-5
- operating system users, 6-4, 7-6, 8-5
- operating systems supported, 6-4
- Oracle Advanced Security, 11-10
- Oracle BI Publisher, downloading, 15-2
- Oracle BI Publisher, integration, 15-2
- Oracle Business Intelligence, 15-1
- Oracle Configuration Manager
 - enabling, 2-5
 - manually collecting, uploading, 2-5
 - overview, 2-4
- Oracle Enterprise Manager
 - directory structure, A-1
 - rollup process, 12-13
- Oracle Enterprise Manger
 - tuning, 12-11
- Oracle home, 2-21
- Oracle Inventory Directory, 2-20
- Oracle Management Agent
 - cloning
 - facts, 7-2
 - in graphical mode, 7-13
 - in silent mode, 7-20
 - overview, 7-1
 - postclone steps, 7-22
 - prerequisites, 7-5
 - supported additional parameters, 7-18, 8-16
 - configuring when protected by a firewall, 11-5
 - deinstallation
 - deinstalling shared Agent, 18-5
 - graphical mode, 18-2
 - overview, 18-1
 - prerequisites, 18-1
 - silent mode, 18-3
 - installation
 - packages, 6-4
 - silent, 6-1, 6-2, 6-3, 6-7, 6-25
 - installing shared agents
 - facts, 8-2
 - in graphical mode, 8-12
 - in silent mode, 8-17
 - postinstall steps, 8-20
 - prerequisites, 8-4
 - ports, 2-13
 - software, 1-8
 - software-only installation
 - configuring, 9-2
 - facts, 9-2
 - installing, 9-2

- overview, 9-1
 - postinstall steps, 9-3
 - prerequisites, 9-2
- Oracle Management Repository, 12-2
- Oracle Management Service, B-2
 - configuring for use with a proxy server, 11-8
 - configuring to allow incoming data from Management Agent, 11-9
 - configuring when protected by a firewall, 11-7
- Oracle Management Service home directory, A-2
- Oracle Management Service logs, B-5
- Oracle Middleware home, 2-20
- Oracle Net firewall proxy access, 11-10
- Oracle WebLogic Server, 2-17
 - admin server
 - admin server port, 2-19
 - existing admin server, 2-18
 - starting admin server, 2-19
 - verifying admin server, 2-19
 - cluster support, 2-18
 - credentials, 2-18
 - default version installed, 3-2
 - domain, 2-18
 - log file output, 2-17
 - manual installation, 3-3
 - node manager, 2-18
 - verifying, 2-17
 - verifying installation, 2-17
- Oracle WebLogic Server Cluster, 2-18
- Oracle9i
 - configuring for monitoring, 10-4
- oraInst.loc file, 4-15, 4-32
- oraInstRoot.sh script, 2-29
- oraInstroot.sh script, 4-15, 4-32
- oraInventory, 2-20
- other installation logs, B-7
- OUIinventories.add, 10-2
- Overview, 3-1

P

- packages, 6-4, 8-5
- PERFSTAT, 10-5
- permissions, 6-6, 6-7
- plug-ins
 - selecting plug-ins, 4-18, 5-2
 - verifying installation, 6-26
- ports, 2-12
 - 4888, 11-7, 11-9
 - 4889, 11-9
 - Admin Server port, 2-13, 2-19
 - admin server port, 2-19
 - console ports, 2-12
 - custom EM ports, 2-13
 - customize ports, 2-13
 - default ports, 2-12
 - HTTP port, 2-13
 - HTTPS port, 2-13
 - managed server port, 2-13
 - node manager port, 2-13

- upload ports, 2-12
 - viewing a summary of ports assigned during installation, 11-2
- postinstallation scripts, 7-13, 8-11
- PowerBroker, 10-24
- preinstallation scripts, 7-13, 8-11
- prerequisite checks
 - default checks, 2-26
 - overview, 2-26
 - run by default, 2-26
 - run in standalone mode, 2-27
 - running in standalone mode, 2-27
- Privilege Delegation Providers, 10-23
- privilege delegation setting
 - applying, 10-26
 - creating, 10-24
 - disabling, 10-27
- privileged delegation setting, 7-9, 7-17, 8-8, 8-15
- proxy server
 - configuring Management Agent for, 11-6
 - configuring the Management Service for, 11-8

R

- remote deployment
 - JVMD agents, 14-10
 - JVMD managers
- RepManager, 2-17
- RepManager Utility, E-1
 - supported actions, E-1
 - drop, E-5
 - dropall, E-5
 - pluginpurge, E-6
 - preupgrade, E-2
 - resume, E-4
 - transX, E-4
 - upgrade, E-3
- response file, 3-1
- rollup process, 12-13
- root.sh script, 2-29
- RPM File, 18-6

S

- schemanager, B-2
- secure logs, B-5
- Secure Socket Layer, BI Publisher, 15-17
- self update console, 1-8
- session timeout
 - modifying, 10-6
- setNMProps.sh script, 13-5, 14-5
- shared agents
 - auto-discovery of targets, 8-2
 - configuring instance directory, 8-2
 - overview, 8-1
- shared oracle home, 8-10
- silent mode, 2-2
- software
 - Enterprise Manager Cloud Control, 1-3
 - Oracle Management Agent, 1-8

- software updates
 - overview, 2-5
- software-only installation, 2-4
- SSH, 7-3, 7-11, 8-2, 8-11
- SSH public key Authentication, 7-4, 8-3
- SSH1, 7-3, 8-2
- SSH2, 7-3, 8-2
- startScriptEnabled property, 13-5, 14-5
- startWebLogic.sh script, 13-5, 14-5
- staticports.ini file, 2-13, 2-15, 2-16
- Statspack, 10-4
- SUDO, 7-9, 7-10, 8-9, 8-10
- Sudo, 10-24
- SYSMAN schema, 2-16
- system prerequisite logs, B-6

T

- Target Relocation, active/passive, H-1
- temporary directory
 - permissions, 6-6
 - space, 6-5, 7-11, 8-10
- thresholds, 12-9, 12-10
- Top SQL Report
 - configuring the database to show the Top SQL Report, 10-4
- troubleshooting
 - ADP manager name conflict, I-11
 - Copying ADP Agent Zip or Javadiagnosticagent Ear Step, I-13
 - deploy ADP agent failure, I-11
 - SSL Handshake error, I-13
- troubleshooting ADP and JVMD, I-11

U

- UDP, 11-11
- uix-config.xml, G-2
- uix-config.xml Flag, G-2
- upload port, 2-12
- User Datagram Protocol, 11-11

W

- web.xml, G-2