Oracle® Enterprise Manager

Grid Control Installation and Basic Configuration

10*g* Release 3 (10.2.0.3.0)

B40103-01

January 2007

ORACLE®

Oracle Enterprise Manager Grid Control Installation and Basic Configuration, 10*g* Release 3 (10.2.0.3.0)

B40103-01

Copyright © 2003, 2007, Oracle. All rights reserved.

Primary Author: Aparna Kamath

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software—Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Contents

Preface xiii

Intended Audience xiii
Documentation Accessibility xiii
Related Documents xiv
Conventions xiv

What's New xvii

Multiple Oracle Home Installations xviii
Resuming an Enterprise Manager Grid Control Installation xix
Out-of-Box Secure Grid Environment xix
Automated Startup Scripts (UNIX Only) xix
Automated Secure Shell (SSH) Setup During Push Install xix
Oracle Configuration Manager xx
Enhanced Installer Screens xx

Part I Preinstallation

1 Preinstallation Requirements

1.1 Planning Your Installation 1-1
1.2 Enterprise Manager Components Overview 1-2
1.2.1 Enterprise Manager - Topology 1-3
1.3 Preinstallation Considerations for Enterprise Manager 1-3
1.3.1 Licensing Information 1-3
1.3.2 Oracle Directory 1-3
1.3.3 Multiple Oracle Home Support 1-4
1.4 Preinstallation Requirements for Enterprise Manager 1-4
1.4.1 Enterprise Manager Hardware Requirements 1-4
1.4.1.1 Recommended CPU and Memory Allocation 1-4
1.4.1.2 Temporary Disk Space Requirements on HP-UX 1-5
1.4.1.3 Temporary Disk Space Requirements on IBM AIX 1-5
1.4.1.4 Considering Resource Allocation 1-6
1.4.2 Enterprise Manager Platform and Target Certification Requirements 1-6
1.4.2.1 Operating System Certifications 1-6
1.4.2.2 Required Packages and Kernel Parameters 1-7
1.4.2.3 Browser Certifications for the Enterprise Manager Console 1-7

1.4.2.4 Certified Enterprise Manager Targets 1-8
1.4.3 Enterprise Manager Software Requirements 1-9
1.4.3.1 Management Repository Software Requirements 1-9
1.4.3.2 Management Service Software Requirements 1-9
1.4.4 Network Requirements 1-10
1.4.5 Prerequisite Checks 1-10
1.5 Running the Prerequisite Check in Standalone Mode 1-11

2 Things to Know Before Installation

2.1 Obtaining Software from the Oracle Technology Network 2-1
2.1.1 Extracting Software from the Zip Files 2-1
2.2 Oracle Directory 2-2
2.3 Installing in an Existing Oracle Home 2-2
2.4 First-Time Installation of Oracle Enterprise Manager Grid Control 2-2
2.4.1 Installing Additional Languages 2-3
2.5 Passwords and Restrictions 2-3
2.6 Why Must I Log In as Root During Installation (UNIX Only)? 2-3
2.6.1 Running root.sh During Installation (UNIX Only) 2-4
2.7 Starting Oracle Universal Installer (OUI) 2-4
2.8 Enterprise Manager Configuration Plug-in (EMCP) 2-4

Part II Enterprise Manager Installation

3 Installing Enterprise Manager

3.1 Accessing the Installation Software 3-1
3.1.1 Installing from a Remote DVD Drive (UNIX Only) 3-1
3.1.1.1 Setting the Mount Point for the DVD-ROM on Linux 3-1
3.1.2 Setting the Mount Point for the DVD-ROM on AIX 3-2
3.1.3 Installing on Remote Computers Using Remote Access Software 3-2
3.1.3.1 Installing from a Hard Drive 3-3
3.1.3.2 Installing from a Remote DVD Drive 3-3
3.2 Using Oracle Universal Installer 3-3
3.2.1 Specifying a Temporary Directory 3-3
3.2.2 Starting the Installer 3-4
3.3 Enterprise Manager Installation Types 3-5
3.3.1 Installing Enterprise Manager 10*g* Grid Control Using a New Database 3-6
3.3.1.1 Permissions and Prerequisites 3-7
3.3.1.2 To Install Enterprise Manager Using a New Database 3-7
3.3.2 Installing Enterprise Manager 10*g* Grid Control Using an Existing Database 3-21
3.3.2.1 Prerequisites 3-21
3.3.2.1.1 Check Database Initialization Parameters 3-22
3.3.2.1.2 NLS_LANG Environment Variable 3-23
3.3.2.2 To Install Enterprise Manager Using Existing Database 3-24
3.3.2.2.1 Configuration Assistant 3-31
3.3.3 Installing an Additional Management Service 3-31
3.3.3.1 Prerequisites 3-31

3.3.3.2 To Install an Additional Management Service ... 3-32
3.3.4 Installing a Management Agent ... 3-37
3.3.4.1 Prerequisites ... 3-38
3.3.4.2 To Install an Additional Management Agent Using OUI ... 3-38
3.4 Executing the runConfig Tool from the Command Line ... 3-43
3.4.1 Options You Can Specify to Execute runConfig ... 3-43
3.4.1.1 ORACLE_HOME ... 3-43
3.4.1.2 ACTION ... 3-43
3.4.1.3 MODE ... 3-43
3.4.1.4 COMPONENT_XML ... 3-44
3.4.1.5 RESPONSE_FILE ... 3-44
3.4.1.6 INV_PTR_LOC ... 3-44
3.4.1.7 RERUN ... 3-44
3.4.1.8 Typical Usage of the runConfig.sh ... 3-45
3.4.1.9 runConfig Log Files ... 3-45
3.4.2 Executing the configToolFailedCommands Script (UNIX Only) ... 3-45
3.5 Deinstallation of Enterprise Manager Grid Control ... 3-45
3.5.1 Additional Deinstallation Steps for Windows Operating Systems ... 3-46
3.5.1.1 Remove Entries in Windows Registry ... 3-46
3.5.1.2 Clean Up Environment Settings ... 3-46
3.5.1.3 Delete Software and Start Menu Icons ... 3-47

4 Enterprise Manager Silent Installations

4.1 Performing Silent Installations ... 4-1
4.1.1 Silent Installation of Enterprise Manager Using a New Database ... 4-3
4.1.2 Silent Installation of Enterprise Manager Using an Existing Database ... 4-3
4.1.3 Silent Installation of an Additional Management Service ... 4-4
4.1.4 Silent Installation of an Additional Management Agent ... 4-4
4.1.4.1 Setting Up Proxy Configuration for the Management Agent ... 4-5
4.2 Assigning Custom Ports (Static Ports Feature) ... 4-5
4.3 Formats for the Staticports.ini File ... 4-7
4.4 Error Conditions that Cause the Installer to Resort to Default Ports ... 4-7

5 Prerequisites for Installing Enterprise Manager on Oracle RAC

5.1 Preinstallation Requirements ... 5-1
5.1.1 Configure Oracle Cluster Synchronization Services (CSS) ... 5-1
5.1.2 Certification for Agents on Oracle Real Application Clusters (Oracle RAC) ... 5-2
5.1.3 Additional Software Requirements for Agent Installation on Clusters ... 5-2
5.1.3.1 Oracle Clusterware/Vendor Clusterware ... 5-2
5.1.4 Preinstallation Tasks for Oracle Real Application Clusters ... 5-2

6 Deploying the Management Agent

6.1 Management Agent Installation/Deployment Options ... 6-1
6.2 Installing the Management Agent Using Agent Deploy ... 6-2
6.2.1 Agent Deploy Installation Prerequisites ... 6-3
6.2.2 Accessing the Agent Deploy Application ... 6-3

6.2.3 Agent Deploy Installation Types ... 6-3
6.2.3.1 Fresh Installation of the Management Agent ... 6-4
6.2.3.1.1 Scenarios to Consider While Performing a Cluster Agent Install ... 6-10
6.2.3.2 Installation Using a Shared Agent Home ... 6-11
6.2.3.3 Concepts and Prerequisites ... 6-12
6.2.3.3.1 EMSTATE Directory: ... 6-12
6.2.3.3.2 EMSTATE Directory Location: ... 6-12
6.2.3.3.3 EMSTATE Directory Space Requirements: ... 6-12
6.2.3.3.4 Packages and OS Patches Requirement: ... 6-12
6.2.3.3.5 Operating System Credentials: ... 6-12
6.2.3.3.6 Shared oraInventory ... 6-12
6.2.3.4 Performing the Installation ... 6-12
6.3 Sharing the Agent Oracle Home Using the nfsagentinstall Script ... 6-16
6.3.1 Preinstallation Considerations ... 6-16
6.3.1.1 User Credentials ... 6-16
6.3.1.2 If Agent Is Not the First Oracle Product Installation ... 6-17
6.3.2 Performing an NFS Agent Installation ... 6-17
6.3.2.1 Usage of the nfsagentinstall Script ... 6-17
6.3.3 Deinstalling the NFSAgent ... 6-18
6.4 Installing the Agent Using the agentDownload Script ... 6-19
6.4.1 About agentDownload Script ... 6-19
6.4.2 Benefits of the agentDownload Script ... 6-19
6.4.3 Obtaining the agentDownload Script ... 6-19
6.4.4 Using the agentDownload Script ... 6-20
6.4.4.1 Cluster Installation ... 6-23
6.4.4.2 Script Details ... 6-23
6.4.4.3 Customizing the agentDownload Script ... 6-25
6.4.5 Downloading 10.2.0.3.0 Agent Installation Software for Different Platforms ... 6-25

7 Postinstallation Configuration Tasks

7.1 Running root.sh to Complete the Installation Process (UNIX Only) ... 7-1
7.2 Checking Database Settings ... 7-2
7.2.1 UNDO Tablespace and Temporary Tablespace ... 7-2
7.2.2 Archive Logging ... 7-2
7.2.3 Ensure the Database is Not in QUIESCE Mode ... 7-2
7.3 Accessing the Oracle*MetaLink* Web Site ... 7-2
7.3.1 Accessing Management Packs ... 7-3
7.3.1.1 Impact of Management Packs on Targets ... 7-3
7.3.2 Optional Configurations ... 7-3
7.3.2.1 Specifying the OracleMetaLink Credentials ... 7-4
7.3.2.2 Setting Up Proxy Configuration for the Management Service ... 7-4
7.4 Configuring Database and ASM Targets for Monitoring ... 7-4
7.5 Agent Reconfiguration and Rediscovery ... 7-5
7.5.1 Rediscover and Reconfigure Targets on Standalone Agents ... 7-6
7.5.2 Reconfiguring a Standalone Agent to an Oracle RAC Agent ... 7-6
7.5.3 Reconfiguring an Existing RAC Agent ... 7-6
7.5.4 Rediscovering Targets on a Oracle RAC Agent ... 7-6

8 Deploying Cluster Agent

8.1 Installing the Agent on a Release 9.2 Cluster 8-1
8.1.1 Installing a Standalone Agent on a Release 9.2 Cluster Node 8-1
8.1.1.1 Installing a Standalone Agent Using the agentDownload Script 8-1
8.1.1.2 Installing a Standalone Agent Using the Agent Deploy Application 8-1
8.1.1.3 Installing a Standalone Agent Using Oracle Universal Installer 8-2
8.1.2 Installing a Cluster Agent on a Release 9.2 Cluster 8-2
8.1.2.1 Installing a Cluster Agent Using the agentDownload Script 8-2
8.1.2.2 Installing a Cluster Agent Using the Agent Deploy Application 8-2
8.1.2.3 Installing a Cluster Agent Using the Interactive Installer 8-2
8.2 Installing the Agent on Oracle Clusterware 8-2
8.2.1 Installing a Standalone Agent on Oracle Clusterware 8-3
8.2.1.1 Installing a Standalone Agent Using agentDownload Script 8-3
8.2.1.2 Installing a Standalone Agent Using the Agent Deploy Application 8-3
8.2.1.3 Installing a Standalone Agent Using Oracle Universal Installer 8-3
8.2.2 Installing a Cluster Agent on Oracle Clusterware 8-3
8.2.2.1 Installing a Cluster Agent Using the agentDownload Script 8-3
8.2.2.2 Installing a Cluster Agent Using the Agent Deploy Application 8-4
8.2.2.3 Installing a Cluster Agent Using Oracle Universal Installer 8-4
8.2.3 Installing Oracle RAC Agent on Windows 8-4

9 Management Agent Cloning

Part III Postinstallation Configuration

10 Getting Started with Enterprise Manager

10.1 Enterprise Manager's Ready-To-Use Configuration 10-1
10.1.1 Default Super Administrator: SYSMAN 10-1
10.1.2 E-mail Notifications 10-2
10.1.3 Notification Rules 10-2
10.1.4 Automatic Discovery 10-2
10.1.4.1 Troubleshooting Issues Concerning Target Discovery 10-3
10.2 Using the Enterprise Manager Grid Control Console for the First Time 10-3
10.2.1 Enabling or Disabling the Licensed Function 10-3
10.3 Controlling the Management Repository, Service, and Agent 10-4
10.3.1 Starting the Management Repository Database 10-4
10.3.2 Starting and Stopping the Management Service 10-4
10.3.3 Starting and Stopping the Management Agent 10-5
10.3.4 Starting the Oracle Application Server Console 10-6
10.3.5 Accessing Enterprise Manager Grid Control 10-6
10.3.6 Unlock the DBSNMP User Account 10-7
10.3.7 Set Monitoring Credentials 10-7
10.3.7.1 Setting Monitoring Credentials for Database Targets 10-7
10.3.7.2 Setting Monitoring Credentials for ASM Targets 10-8

Part IV Enterprise Manager Upgrade

11 Upgrading Enterprise Manager Grid Control

11.1 Software Prerequisites 11-1
11.2 Checks to Be Performed Before Starting the Upgrade 11-2
11.2.1 Shut Down Enterprise Manager Before Upgrade 11-2
11.2.2 Check for Symbolic Links 11-2
11.2.3 Customizations and User Permissions 11-2
11.2.4 Recompile EMD_MAINTENANCE for Manually Upgraded Databases 11-3
11.2.5 Verify Inventory.xml for Oracle Home Path 11-3
11.2.6 Select an Agent that Is Not Secure 11-3
11.2.7 Shut Down Database Listener (UNIX Only) 11-3
11.2.7.1 Impact on Firewall Ports and Software Load Balancers 11-4
11.3 Manual Configuration to Be Performed For Upgrade 11-4
11.3.1 Tasks to be Performed Before Upgrading from 10.1.0.4 to 10.2.0.1 or 10.2.0.2 11-4
11.3.2 Tasks to be Performed For Upgrading from 10.1.0.4 to 10.2.0.1 or 10.2.0.2 11-5
11.3.3 Tasks to be Performed Before Upgrading from 10.2.0.1 to 10.2.0.2 or 10.2.0.3.0 11-5
11.3.4 Tasks to be Performed For Upgrading from 10.2.0.1 to 10.2.0.2 or 10.2.0.3.0 11-6
11.4 Upgrade Scenarios 11-6
11.4.1 Upgrading Oracle Management Service that Is Installed Using a New Database 11-6
11.4.2 Upgrading Management Service that Is Installed Using an Existing Database 11-6
11.4.3 Upgrading the Oracle Management Service 11-7
11.4.4 Upgrading the Management Agent 11-8
11.4.4.1 Upgrading 10.1.0.4 Agents that Monitor User-Defined Metrics 11-8
11.5 Enterprise Manager Upgrade 11-8
11.5.1 Enterprise Manager Upgrade Using Oracle Universal Installer 11-9
11.5.1.1 Upgrade Logs 11-14
11.5.1.2 Post-Upgrade Configuration 11-14
11.5.1.2.1 For Oracle Management Service 11-14
11.5.1.2.2 For Oracle Database Upgrade 11-15
11.5.1.2.3 For Management Agent 11-16
11.5.1.3 Enterprise Manager Grid Control Upgrade Diagnostics 11-16
11.5.1.3.1 Management Service Upgrade Stops At IASUA failure 11-16
11.5.1.3.2 Management Service Upgrade Stops at EMDeploy Failure 11-16
11.5.1.3.3 Management Service Upgrade Stops at the Repository Schema Upgrade (RepManager) 11-17
11.5.2 Upgrading Management Agent Using the Agent Deploy Application 11-17
11.5.2.1 Possible Parameters that You Can Specify During Agent Upgrade 11-20
11.5.3 Upgrading Management Agent Using agentDownload Script 11-21
11.5.4 General System Installation Requirements for Real Application Clusters 11-22
11.5.4.1 Hardware Requirements for Real Application Clusters Setup 11-22
11.5.4.2 Software Requirements for Real Application Clusters Setup 11-23

Part V Appendixes

A Troubleshooting Enterprise Manager

A.1 Installation Issues A-1
A.1.1 Installation Fails with an Abnormal Termination A-1

A.1.2 PERL Environment Variable is Forced on the environment During an Enterprise Manager 10*g* R2 (10.2.0.2) Installation A-1
A.1.3 Management Agent Installation Fails A-1
A.1.3.1 Prerequisite Check Fails with Directories Not Empty Error During Retry A-2
A.1.3.2 Agent Deployment on Linux Oracle RAC 10.2 Cluster Fails A-2
A.1.3.3 SSH User Equivalence Verification Fails During Agent Installation A-3
A.1.3.3.1 Sample sshd_config File A-3
A.1.3.4 SSH Setup Fails with "Invalid Port Number" Error A-5
A.1.3.5 sshConnectivity.sh Script Fails A-6
A.1.3.6 Troubleshooting the "command cygrunsrv not found" Error. A-6
A.1.3.6.1 If SSHD Service Is Not Running A-6
A.1.3.6.2 If Your Cygwin Installation Was Unsuccessful A-7
A.1.3.7 SSH Setup Verification Fails with "Read from socket failed: Connection reset by peer." Error A-7
A.1.3.8 SSHD Service Fails to Start A-8
A.1.3.9 Timezone Prerequisite Check Fails A-8
A.1.3.10 OMS Version Is Not Displayed A-8
A.1.3.11 Discrepancy Between Agent and Repository URL Protocols A-9
A.1.3.12 Last Successful Upload Does Not Have a Time Stamp A-9
A.1.3.13 emctl status Log File is Empty A-9
A.2 Configuration Issues A-10
A.2.1 Configuration Assistants Fail During Enterprise Manager Installation A-10
A.2.1.1 Invoking the One-Off Patches Configuration Assistant in Standalone Mode.. A-10
A.2.1.2 Invoking the Database Configuration Assistant in Standalone Mode A-10
A.2.1.3 Invoking the OMS Configuration Assistant in Standalone Mode A-10
A.2.1.4 Invoking the Agent Configuration Assistant in Standalone Mode A-11
A.2.1.5 Invoking the OC4J Configuration Assistant in Standalone Mode A-11
A.2.1.6 Enterprise Manager Deployment Fails A-11
A.2.2 Oracle Management Service Configuration Fails A-12
A.2.2.1 Oracle Management Service Fails While Deploying Enterprise Manager AgentPush Application A-12
A.2.2.2 In 'Enterprise Manager with new Database' Install, Oracle Management Service Configuration Fails While Unlocking Passwords A-12
A.2.2.3 Dropping of Repository Hangs If SYSMAN Sessions are Active A-12
A.2.2.4 If Oracle Management Service Configuration is Retried, oracle.sysman.emSDK.svlt.ConsoleServerHost and oracle.sysman.emSDK.svlt.ConsoleServerName in emoms.properties are Swapped and There is an Extra Underscore in ConsoleServerHost A-12
A.3 Enterprise Manager Upgrade and Recovery Issues A-13
A.3.1 Agent Upgrade Issues A-13
A.3.1.1 Agent Does Not Start Up After Upgrade A-13
A.3.1.2 Missing Directories When Upgrading Agent from 10.1.0.5 to 10.2.0.1 .... A-14
A.3.2 Enterprise Manager Recovery A-14
A.3.2.1 Steps to Follow for Agent Recovery A-14
A.3.2.2 Steps to Follow for OMS Recovery A-14
A.3.2.3 Steps to Re-create the Repository A-15
A.3.2.3.1 Dropping the Repository A-15
A.3.2.3.2 Creating the Repository A-15

A.3.3 Repository Creation Fails A-16
A.3.4 Collection Errors After Upgrade A-16
A.4 Oracle Management Service Upgrade Issues A-17
A.4.1 OMS Upgrade Stops at OracleAS Upgrade Assistant Failure A-17
A.4.2 OMS Configuration Stops at EMDeploy Failure A-17
A.4.3 OMS Configuration Stops at Repository Schema Failure (RepManager) A-17
A.4.4 Monitoring Agent Does Not Discover Upgraded Targets A-17
A.4.5 CSA Collector Is Not Discovered During Agent Upgrade A-18
A.4.6 ias_admin Password Is Set To welcome1 After Upgrade A-18
A.4.7 Oracle Management Service Upgrade Fails If Older Listener Is Running On A Port Other Than 1521 ..... A-18
A.5 Network Issues A-18
A.5.1 Incorrect Format For Entries In /etc/hosts File A-18
A.5.2 Enterprise Manager Installation on Computers With Multiple Addresses A-19
A.5.3 Agent Configuration Fails on A Non-Network Computer A-19
A.5.4 Loopback Adapter On Windows and Related Known Issues A-19
A.6 Other Installation and Configuration Issues A-19
A.6.1 Storage Data Has Metric Collection Errors A-20
A.6.2 Cannot Add Systems to Grid Environment from the Grid Control Console A-20
A.7 Error During Deinstallation of Grid Control Targets A-20
A.8 Need More Help A-20

B Platform-Specific Package and Kernel Requirements

B.1 Package Requirements B-1
B.1.1 Required Packages on Linux B-1
B.1.2 Required Packages on Solaris B-2
B.1.2.1 Checking for 32-Bit and 64-Bit Application Support B-3
B.1.2.2 Required Patches B-3
B.1.2.3 Checking for Patches B-4
B.1.3 Required Packages on HP-UX B-4
B.1.4 Required Packages on AIX B-5
B.1.4.1 To Verify Whether the Filesets Are Installed and Committed B-6
B.1.4.2 Verify Whether or Not APAR is Installed B-6
B.2 Kernel Parameter Requirements B-7
B.2.1 Kernel Parameter Requirements on Linux B-7
B.2.2 Kernel Parameter Requirements on Solaris B-8
B.2.2.1 View and Change Kernel Parameter Values on Solaris 8 and 9 ..... B-9
B.2.2.2 View and Change Kernel Parameter Values on Solaris 10 ..... B-10
B.2.3 Kernel Parameter Requirements on HP-UX B-10
B.2.3.1 View and Change Kernel Parameter Values B-11
B.2.4 Configure Shell Limits and System Configuration Parameters on AIX B-12
B.2.4.1 Configuring Shell Limits B-12
B.2.4.2 Specifying System Configuration Parameters B-12

C Agent Deploy Application - Installation Prerequisites

C.1 Prerequisites C-1
C.1.1 Check Platform-Specific Package Requirements for Agent Installation C-1

C.1.2 Set Up SSH (Secure Shell) User Equivalence C-3
C.1.2.1 Setting Up SSH User Equivalence Using sshConnectivity.sh C-3
C.1.2.1.1 sshConnectivity.sh Script Usage C-4
C.1.2.2 Setting Up SSH on UNIX Using sshUserSetup.sh C-5
C.1.2.3 Setting Up SSH Server (SSHD) on Microsoft Windows C-7
C.1.2.4 Setting Up SSH on Microsoft WIndows Using sshUserSetupNT.sh C-11
C.1.2.5 Setting Up the Timezone Variable on Remote Hosts C-14
C.1.2.5.1 Set the TZ variable and Restart the SSH Daemon C-14
C.1.2.5.2 Set the TZ Variable in the "Shell rc" File C-14
C.1.2.6 Dropping SSH Connection C-15
C.1.2.7 Checking if SSH Connection is Removed C-16
C.1.3 Validate All Command Locations C-16
C.1.3.1 Location of Properties File C-18
C.1.3.2 Location of Installation Logs C-19
C.1.4 Modify Response File for Big IP Host and Port C-19
C.1.5 Verify oraInventory Permissions on Remote Hosts C-19
C.1.6 Verify User Credentials C-19
C.2 Prerequisite Checks Executed by Agent Deploy C-19
C.2.1 Prerequisite Checks Executed on the Local Host C-19
C.2.2 Prerequisite Checks Executed on Remote Hosts C-20
C.3 Troubleshooting Failed Prerequisite Checks C-21
C.3.1 Prerequisite Check Errors and Resolutions on Local Host C-21
C.3.2 Prerequisite Check Errors and Resolutions on Remote Hosts C-22
C.4 Commands and Arguments Executed to Run Agent Deploy Plugins C-24
C.5 Sample Properties Files C-25

D Additional Parameters for Agent Deploy

D.1 Additional Parameters Supported by agentDownload Script D-1
D.2 Additional Parameters Supported by Oracle Universal Installer D-2
D.2.1 Command-Line Variable Usage During Silent Installation D-3

E Enterprise Manager Firewall Port Requirements

F Installation and Configuration Log File Locations

F.1 Enterprise Manager Grid Control Installation Log Files F-1
F.1.1 Configuration Logs F-1
F.1.2 Installation Logs F-2
F.1.3 Repository and Secure Logs F-2
F.1.3.1 Repository Log Location F-2
F.1.3.2 Secure Log Location F-2
F.2 Agent Deploy Log Files F-2

G Oracle Reserved Words

G.1 List of Oracle Reserved Words G-1

Index

Preface

This guide is your primary source of preinstallation requirements and certifications, and describes the installation options, and postinstallation configuration information for Oracle Enterprise Manager 10*g* Grid Control.

Note that later releases of this and other Enterprise Manager documentation may be available on the Oracle Technology Network at

`http://www.oracle.com/technology/documentation/oem.html`

This preface contains the following topics:

- Intended Audience
- Documentation Accessibility
- Related Documents
- Conventions

Intended Audience

This guide is written for Oracle Database system administrators who want to install and configure Oracle Enterprise Manager Grid Control. You should already be familiar with Oracle Database and the administrative tasks you want to perform.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

`http://www.oracle.com/accessibility/`

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

For more information, see the following books in the Oracle Enterprise Manager documentation set:

- *Oracle Enterprise Manager Concepts*
- *Oracle Enterprise Manager Grid Control Quick Installation Guide*
- *Oracle Enterprise Manager Advanced Configuration*
- *Oracle Enterprise Manager Configuration for Oracle Collaboration Suite*
- *Oracle Enterprise Manager Policy Reference Manual*
- *Oracle Enterprise Manager Metric Reference Manual*
- *Extending Oracle Enterprise Manager*
- *Oracle Enterprise Manager Command Line Interface*
- *Oracle Enterprise Manager SNMP Support Reference Guide*

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

`http://otn.oracle.com/documentation/oem.html`

Oracle Enterprise Manager also provides extensive online Help. Click **Help** at the top of any Enterprise Manager page to display the online help window. This installation guide has been designed to work in close association with the online help provided with the installation.

Conventions

This section describes the conventions used in the text and code examples of this documentation set. It describes:

- Conventions in Text
- Conventions in Code Examples

Conventions in Text

The following table describes those conventions and provides examples of their use.

Convention	Meaning	Example
Bold	Bold typeface indicates an element in the user interface.	Click **Help** for more information.
Italics	Italic typeface indicates book titles or emphasis.	*Oracle Database Concepts* Ensure that the recovery catalog and target database do *not* reside on the same disk.

Convention	Meaning	Example
`lowercase monospace (fixed-width font)`	Lowercase monospace typeface indicates executables, file names, directory names, and sample user-supplied elements. Such elements include computer and database names, net service names, and connect identifiers, as well as user-supplied database objects and structures, column names, packages and classes, user names and roles, program units, and parameter values. **Note:** Some programmatic elements use a mixture of UPPERCASE and lowercase. Enter these elements as shown.	Enter `sqlplus` to open SQL*Plus. The password is specified in the `orapwd` file. Back up the datafiles and control files in the `/<DVD>/oracle/dbs` directory. The `department_id`, `department_name`, and `location_id` columns are in the `hr.departments` table. Set the `QUERY_REWRITE_ENABLED` initialization parameter to `true`. Connect as `oe` user. The `JRepUtil` class implements these methods.

Conventions in Code Examples

Code examples illustrate SQL, PL/SQL, SQL*Plus, or other command-line statements. They are displayed in a monospace (fixed-width) font and separated from standard text as shown in this example:

```
SELECT username FROM dba_users WHERE username = 'MIGRATE';
```

The following table describes typographic conventions used in code examples and provides examples of their use.

Convention	Meaning	Example
`< >`	Angle brackets in command syntax denote an item for which you can substitute a real value. Do not enter the angle brackets.	`<host>:<port>:<oracle_sid>`
`Italics`	Italicized text indicates placeholders or variables for which you must supply particular values.	`CONNECT SYSTEM/`*`system_password`* `DB_NAME =` *`database_name`*

What's New

This chapter describes new features in the Enterprise Manager 10*g* Grid Control Release 3 (10.2.0.3.0) installer.

The new Enterprise Manager installer provides an installation that is almost completely automated. In this release, the Enterprise Manager installer also provides the following:

- Renders seamless multiple Oracle home installations and configurations during a single session.
- Facilitates individual maintenance cycles for each of the top-level product components.

  This is brought about by installing the database and Oracle Management Service (OMS) in separate Oracle homes. In this release, the Enterprise Manager installer will perform a chain install, wherein it will install the OMS, database, and the agent in separate Oracle homes (`oms10g`, `db10g`, and `agent10g`).
- Facilitates an Oracle Management Service upgrade from 10.1.0.4 release (and later) to 10.2.0.3.0
- Facilitates an Oracle Management Agent upgrade from 10.1.0.3 release (and later) to 10.2.0.3.0
- Facilitates mass deployment of the Management Agent using the Agent Deploy application.
- Provides a ready-to-use secure Enterprise Manager Grid Control environment.
- Provides automated startup scripts that help start the Oracle Database, Management Service, listener, and the Management Agent during a machine reboot (UNIX platforms only).
- Allows the user to resume the installation process from the point where it was terminated, through the built-in resumability feature of the installer.

> **Note:** For information about Management Agent deployment best practices, see the Agent Best Practices paper available at http://www.oracle.com/technology/products/oem/pdf/10gr2_agent_deploy_bp.pdf.

Multiple Oracle Home Installations

The Enterprise Manager installer provides for a seamless installation experience by performing multiple Oracle home installations, depending on the type of installation that you select.

An Oracle Enterprise Manager Grid Control installation using a new database will create a separate Oracle home for:

- Oracle Management Service
- Oracle Database
- Oracle Management Agent

Note: The Oracle homes that are created as subdirectories by the installer will be placed under the Parent Directory that you specify. The Oracle homes will be created as `db10g`, `oms10g`, and `agent10g`.

Seamless Oracle Home Configurations

The Enterprise Manager installer performs multiple Oracle home configurations during the installation process. The configuration tools that are run during installation will depend on the installation type that you have selected.

The following table lists all the configuration tools that are run during an Enterprise Manager installation using a new database:

Product	Configuration Tools
Oracle Enterprise Manager Repository Database	▪ Oracle Net Configuration Assistant ▪ Oracle Database Configuration Assistant
Oracle Enterprise Manager Grid Console	▪ OC4J Configuration Assistant ▪ HTTP Server Configuration Assistant ▪ Java Configuration Assistant ▪ Web Cache Configuration Assistant ▪ Oracle AS Instance Configuration Assistant ▪ Register DCM Plug-ins with Enterprise Manager ▪ DCM Repository Backups Assistant ▪ Enterprise Manager Technology Stack Upgrade ▪ Oracle Management Service Configuration
Oracle Management Agent	▪ Agent Configuration Assistant

Note: Depending on the installation type you have chosen, any or all of the configuration tools listed in the preceding table will be run.

Running Root.sh (UNIX only)

You are now required to run only one script, `allroot.sh`, in this release of the installer, as compared to the three `root.sh` scripts (one for each Oracle home) that you had to run in the previous release.

Note: If Enterprise Manager is the first Oracle product that you are installing, you will also be prompted to execute `orainst Root.sh` along with `all root.sh`.

Resuming an Enterprise Manager Grid Control Installation

In the event of an unexpected termination of the installation process, the Resumability feature of the installer allows you to resume the installation process (the next time the installer is invoked) from the point where the installation was aborted.

Out-of-Box Secure Grid Environment

The new Enterprise Manager 10*g* installer provides a secure Grid Control environment that is immediately ready to use.

Automated Startup Scripts (UNIX Only)

In this release of Enterprise Manager, the startup scripts to run the Oracle database, Management Service, listener, and agent are automatically executed in case a machine reboots. The services that are automatically started depend on the installation type that you chose.

Installing	Automated Scripts Start the
Enterprise Manager Using New Database	Repository database, listener, Management Service, and the agent.
Enterprise Manager Using Existing Database	Management Service and agent.
Additional Management Service	Management Service and agent.
Additional Management Agent	Agent only.
NFS Agent	NFS Agent

Note: On Microsoft Windows, the services are started automatically by the operating system.

Automated Secure Shell (SSH) Setup During Push Install

In Enterprise Manager Grid control 10.2.0.3.0, users do not have to run the SSH user equivalence script (`sshUserSetup.ssh/sshUserSetupNT.ssh`, `sshConnectivity.sh`) before starting the push install, to establish the SSH user equivalence between the Oracle Management Service and agent targets. In Enterprise Manager Grid Control 10.2.0.3.0, the push application sets up and drops the SSH connection automatically between the Oracle Management Service and the agent targets accordingly, but if agent targets are on Windows operating systems, then user needs to setup Cygwin as explained in Appendix C.1.2.3, to start the push agent install.

Oracle Configuration Manager

Oracle Configuration Manager (OCM) is designed to gather and provide customer's configuration information and store it in Oracle repository for maintenance and other related tasks. This feature was introduced from Grid Control Release 10.2.0.2.0 onwards.

Enhanced Installer Screens

The Enterprise Manager 10*g* R2 installer's enhanced Graphical User Interface (GUI) provides for a more user-friendly installation experience.

Installation Location

After you select the appropriate installation option in the first screen (Specify Installation Type), you will be prompted to specify the Parent Directory in the Specify Installation Location screen, wherein the Oracle homes are created automatically.

Specify Configuration

The Specify Configuration screen for installing Enterprise Manager using an existing database has changed. The single Connect String value (comprising a host name, port, and SID) that you had to specify in the previous release has been changed to three input fields.

Language Selection

This screen has been removed. You can now select the required languages by clicking **Product Languages** in the Installation Location screen.

Prefill Tablespace Location

The Specify Repository Database Configuration screen now includes the Prefill Tablespace Locations button. Upon clicking this button, the installer queries the database that you have specified, looks for the `SYSAUX` tablespace location, and automatically prefills that path in the appropriate tablespace location text boxes.

Note: If the tablespaces are stored in a raw device/ASM disk, then you must ensure the raw device/ASM disk is accessible to store the SYSMAN tablespaces.

Part I

Preinstallation

The Preinstallation part of this guide contains information on the preinstallation requirements and certifications including hardware, software, browser, and target certifications.

Part I contains the following chapters:

- Chapter 1, "Preinstallation Requirements"
- Chapter 2, "Things to Know Before Installation"

1

Preinstallation Requirements

This chapter introduces Enterprise Manager and its components, and provides preinstallation requirements and certifications. This chapter also lists all targets that Enterprise Manager is certified to manage.

Oracle recommends reading this chapter before proceeding with your installation for a better understanding of the requirements and certifications for the Enterprise Manager installation environment.

The following topics are covered in this chapter:

- Planning Your Installation
- Enterprise Manager Components Overview
- Preinstallation Considerations for Enterprise Manager
- Preinstallation Requirements for Enterprise Manager
  - Enterprise Manager Hardware Requirements
  - Enterprise Manager Platform and Target Certification Requirements
  - Enterprise Manager Software Requirements
- Running the Prerequisite Check in Standalone Mode

Note: Ensure you also read the Enterprise Manager Grid Control Release Notes that accompany the product.

1.1 Planning Your Installation

The following sections will give you a better understanding of the Oracle Enterprise Manager Grid Control installation process and facilitate a successful installation:

- Enterprise Manager Components Overview: This section briefly describes each Enterprise Manager component.
- Preinstallation Considerations for Enterprise Manager: This section provides information on the preinstallation requirements. You must ensure these requirements are met before starting the Enterprise Manager installation.
- Installing Enterprise Manager: This chapter provides detailed information on how to use Oracle Universal Installer to install Enterprise Manager.
- Deploying the Management Agent: This chapter provides information on various methods of deploying the Management Agent.

- Postinstallation Configuration Tasks: This chapter describes the tasks that must be completed after the installation.

1.2 Enterprise Manager Components Overview

Enterprise Manager is a single, integrated solution for administering and monitoring certified targets. See Section 1.4.2.4, "Certified Enterprise Manager Targets" for a list of Oracle targets and components that Enterprise Manager can manage.

Enterprise Manager includes the Management Agent, Management Service (OMS), and Management Repository, as well as the Grid Control console, which is a browser-based central console through which administrators can perform all monitoring, administration, and configuration tasks for the enterprise.

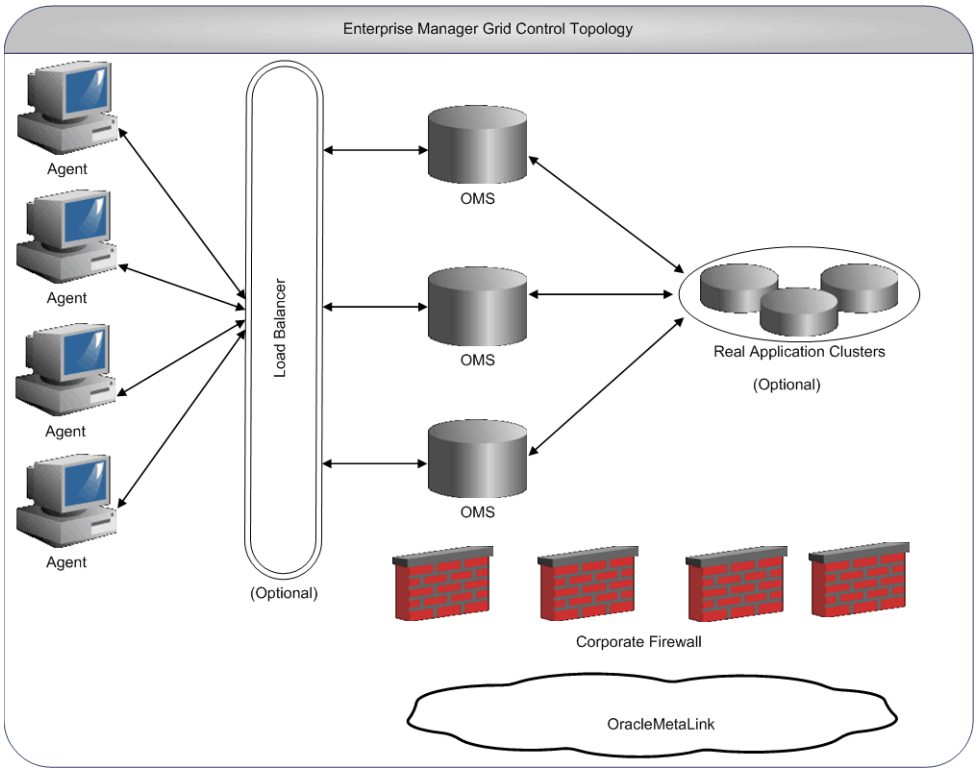
Table 1–1 explains the different Enterprise Manager components and how they work together to manage your enterprise.

Table 1–1 Enterprise Manager Grid Control Components

Component	Definition
Grid Control Console	From the Grid Control console, you can monitor and administer your entire computing environment from one location on the network. All the services within your enterprise, including hosts, databases, listeners, application servers, Oracle Collaboration Suite applications, and Web applications are easily managed from one central location (console).
Management Agent	The Management Agent is a process that is deployed on each monitored host. It is responsible for monitoring all targets on the host, for communicating that information to the middle-tier Management Service, and for managing and maintaining the host and its targets.
Management Service	The Management Service is a J2EE Web application that renders the user interface for the Grid Control console. It works with all Management Agents to process monitoring and jobs information, and uses the Management Repository to store data.
Management Repository	The Management Repository consists of objects such as database jobs, packages, procedures, views, and two tablespaces in Oracle Database that contain all available information about administrators, targets, and applications managed within Enterprise Manager. The Management Service uploads the monitoring data it receives from the Management Agents to the Management Repository. The Management Repository then organizes the data so that it can be retrieved by the Management Service and displayed in the Grid Control console. Because data is stored in the Management Repository, it can be shared between any number of administrators accessing the Grid Control console.

1.2.1 Enterprise Manager - Topology

Figure 1–1 Typical Enterprise Manager Topology



1.3 Preinstallation Considerations for Enterprise Manager

This section provides information about Oracle Universal Installer and other concepts you should know when you plan the installation.

- Licensing Information
- Oracle Directory
- Multiple Oracle Home Support

1.3.1 Licensing Information

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 Services does not provide support for components for which licenses have not been purchased.

For more information refer to *Oracle Enterprise Manager Licensing Information*.

1.3.2 Oracle Directory

If you choose to install Enterprise Manager Grid Control using a new database on a computer with no other Oracle software installed, Oracle Universal Installer creates an Oracle base directory for you. If Oracle software is already installed, then one or more Oracle base directories already exist. In the latter case, you must specify the Oracle base directory into which you want to install Oracle Database.

You are not required to create an Oracle base directory before installation, but you can do so if desired. You can set the `ORACLE_BASE` environment directory to point to this directory, which the Oracle Universal Installer will recognize.

> **Note:** You can choose to create a new Oracle base directory, even if other Oracle base directories exist on that system.

1.3.3 Multiple Oracle Home Support

Enterprise Manager is installed on multiple Oracle homes within the Oracle base directory. This means that a typical Enterprise Manager Grid Control installation creates three Oracle homes in different Oracle home directories. For example, `oms10g`, `db10g`, and `agent10g`.

> **Note:** You must ensure that you install this product into a new Oracle home directory. You cannot install products from one release of Enterprise Manager into an Oracle home directory of a different release. For example, you cannot install 10*g* R2 (10.2) software into an existing Oracle9*i* home directory. If you attempt to install this release into an Oracle home directory that contains software from an earlier Oracle release, the installation will fail.

You can install this release more than once on the same system, as long as each installation is done in a separate Oracle home directory.

1.4 Preinstallation Requirements for Enterprise Manager

This section provides information about the minimum hardware and software requirements for Enterprise Manager components:

- Enterprise Manager Hardware Requirements
- Enterprise Manager Software Requirements

1.4.1 Enterprise Manager Hardware Requirements

This section lists the recommended hardware requirements for running the various Enterprise Manager deployment sizes on all the supported platforms.

1.4.1.1 Recommended CPU and Memory Allocation

Table 1–2 and Table 1–3 approximate the host, CPU, and physical memory requirements for running an Enterprise Manager Grid Control deployment (typical scenario with 2 to 3 GHz machines), based on experiences with real-world Enterprise Manager deployments.

Table 1–2 CPU and Memory Allocation for Oracle Management Service

Deployment Size	Host	CPU/Host	Physical Memory (RAM)/Host	Total Recommended Space
Small (100 monitored targets)	1	1 (3 GHz)	2 GB	2 GB
Medium (1,000 monitored targets)	1	2 (3 GHz)	2 GB	Number of OMS x 5 GB

Table 1–2 (Cont.) CPU and Memory Allocation for Oracle Management Service

Deployment Size	Host	CPU/Host	Physical Memory (RAM)/Host	Total Recommended Space
Large (10,000 monitored targets)	2	2 (3 GHz)	2 GB	Number of OMS x 10 GB

Table 1–3 CPU and Memory Allocation for Oracle Management Repository

Deployment Size	Host	CPU/Host	Physical Memory (RAM)/Host	Total Repository Storage
Small (100 monitored targets)	1[1]	1 (3 GHz)	2 GB	10 GB
Medium (1,000 monitored targets)	1	2 (3 GHz)	4 GB	30 GB
Large (10,000 monitored targets)	2	4 (3 GHz)	6 GB	150 GB

[1] Share Host with the Oracle Management Service for small deployments.

ATTENTION: Oracle recommends that you allocate a minimum default size of 1 GB hard disk space for the `MGMT_ECM_DEPOT_TS` tablespace and allocate the rest of the recommended repository database space for the `MGMT_TABLESPACE`.

Oracle also recommends that you keep the auto-extend feature enabled for the tablespace data files.

Note that the space requirement increases as the number of monitored targets increase, along with the input/output performance demands on the storage devices.

1.4.1.2 Temporary Disk Space Requirements on HP-UX

To determine the amount of free disk space available in the `/tmp` directory, enter the following command:

```
# bdf /tmp
```

If there is less than 1.2 GB of disk space available in the `/tmp` directory, then complete one of the following steps:

- Delete unnecessary files from the `/tmp` directory.
- Set the `TEMP` and `TMPDIR` environment variables to a writable directory with at least 1.2 GB of available disk space.
- Extend the file system that contains the `/tmp` directory. If required, contact your system administrator for information about extending file systems.

1.4.1.3 Temporary Disk Space Requirements on IBM AIX

To determine the amount of free disk space available in the `/tmp` directory, enter the following command:

```
# df /tmp
```

If there is less than 1300 MB of disk space available in the `/tmp` directory, then complete one of the following steps:

- Delete unnecessary files from the `/tmp` directory.
- Set the `TEMP` and `TMPDIR` environment variables to a writable directory with at least 1300 MB of available disk space.
- Extend the file system that contains the `/tmp` directory. If required, contact your system administrator for information about extending file systems.

For Management Agent deployments, make sure that `/tmp` directory has 1300 MB of disk space available on the target machine.

1.4.1.4 Considering Resource Allocation

Carefully consider resource allocation when choosing the disk on which to install the Management Service and Management Repository database. Enterprise Manager's ready-to-use monitoring starts generating information upon installation, meaning that resource consumption begins immediately. As such, consider the base system resource consumption prior to installing. Select your installation locations strategically, taking into account system load, memory usage, and disk input/output.

For example, you can split the input/output load across disks. Avoid installing the Management Repository database or the Management Service on the swap volume, a volume with a busy state (as per `iostat`) of 10 percent or more, or on a memory-constrained system. As with any data-intensive application, if your Management Repository is going to service a large number of targets, it is important to tune the database appropriately to maximize input/output capacity. Refer to the *Database Performance Tuning Guide* for more information.

While adding more resources can help alleviate potential problems (for instance, adding a second disk dedicated to the Management Service on a system), understanding and accounting for resource allocation is the best way to achieve strategic setup and good performance.

1.4.2 Enterprise Manager Platform and Target Certification Requirements

This section contains certification information for each Enterprise Manager component, including the Management Repository, Management Service, and the Management Agent. Browser certifications for the Grid Control console have also been detailed.

Also included in this section are the certifications for all targets managed by Enterprise Manager:

- Operating System Certifications
- Browser Certifications for the Enterprise Manager Console
- Certified Enterprise Manager Targets

1.4.2.1 Operating System Certifications

The operating system platforms certified for Enterprise Manager Grid Control components are listed in Table 1–4.

Table 1–4 Certified Operating System Platforms for Enterprise Manager Grid Control

Operating System	Platform	Version
Linux	▪ x86 32-bit	▪ Red Hat Enterprise Linux AS/ES 3.0 ▪ Red Hat Enterprise Linux AS/ES 4.0 ▪ SUSE Linux Enterprise Server 9
Solaris	SPARC 64-bit	▪ Solaris 8 Update 7 or later ▪ Solaris 9 Update 6 or later ▪ Solaris 10
Microsoft Windows (32-bit)	▪ NT ▪ 2000 ▪ XP	▪ NT ▪ 2002 ▪ XP (Service Pack 2)
HP-UX PA-RISC (64-bit)	PA-RISC (64-bit)	▪ HP-UX 11i V1 (11.1) ▪ HP-UX 11i V2 (11.23)
AIX	AIX 5L	▪ Version 5.2 ▪ Version 5.3

Important: The platforms listed in Table 1–4 are certified for the Management Agent that is packaged along with the Oracle Management Service.

If you are installing a standalone Management Agent or using the `agentDownload` script for agent installation, refer to the *AgentDownload Install Readme* for more information on the certified platforms.

Refer to the Oracle Technology Network Web site's "Certify and Availability" page for the latest information on all supported platforms.

1.4.2.2 Required Packages and Kernel Parameters

For detailed information on the required packages and kernel parameters for each platform, see Appendix B, "Platform-Specific Package and Kernel Requirements".

1.4.2.3 Browser Certifications for the Enterprise Manager Console

The browser versions that are certified for viewing the Grid Control console are the following:

- Internet Explorer 6.0 (SP2)
- Netscape 7.2
- Mozilla 1.7
- Firefox 1.0.4
- Safari 1.2

Note: For services monitoring, you can record and play back Web application transactions using the Transaction Recorder. The Transaction Recorder is supported only on Microsoft Internet Explorer 5.5 (Service Pack 1) and later, and not on other browsers. Alternatively, if you do not have this requirement, you can configure Web transaction steps manually. Refer to the Enterprise Manager online Help for details on creating Web transactions for monitoring.

1.4.2.4 Certified Enterprise Manager Targets

Table 1–5 identifies the Oracle targets and components that Enterprise Manager Grid Control can manage.

Table 1–5 Certified Oracle Targets

Supported Targets	Release
Oracle Application Server	9.0.4.2 and later patchsets 10.1.2.0.0 (Phase 1) 10.1.0.2.0.1 (SEONE) 10.1.2.0.2 (Phase 2) 10.2.0.2.1 Patchset 10.1.3 (Standalone OC4J)
Oracle Database[1], Listener	8.1.7.4 9.0.1.5 9.2.0.7 and later patchsets 10.1.0.4 and later patchsets 10.2
Oracle Real Application Clusters Database	9.2.0.6 10.1.0.4 10.1.0.5 10.2
Oracle Collaboration Suite	9.0.4.2 and later 10.1.1
Management Service and Repository[2]	10.2
Management Agent[3]	10.1.0.2 10.2
Enterprise Manager Web site	10.2
Host	Linux x86 32-bit Red Hat Enterprise Linux AS/ES 3.0 **Oracle recommends that the target host on which you are installing the Management Agent have a static IP address and not DHCP.**

[1] Enterprise Edition, Standard Edition, Personal Edition

[2] The Management Service and Management Repository releases correspond to the release of the Grid Control installation and not the release in which the repository is created.

[3] The Management Agent includes Beacon function.

1.4.3 Enterprise Manager Software Requirements

This section describes the software requirements for each Enterprise Manager component.

1.4.3.1 Management Repository Software Requirements

The embedded Oracle Database 10*g* Release 1 (10.1.0.4), Enterprise Edition, is supported for Management Repository creation. Otherwise, you may only install the Management Repository in one of the following existing databases:

- Oracle Database 10*g* Release 1 (10.1.0.4 and later), Enterprise Edition

  Note: If you are performing an Enterprise Manager Grid control installation using an existing database, ensure the database is a 10.1.0.3 release or later.

- Oracle Real Application Clusters 10*g* Release 1 (10.1.0.4 and later)

  Note: If you are performing an Enterprise Manager Grid control installation using an existing database, ensure the existing Oracle RAC database is a 10.1.0.3 release or later.

- Oracle9*i* Database Release 2 (9.2.0.6 and later), Enterprise Edition
- Oracle9*i* Real Application Clusters Release 2 (9.2.0.6 and later)

Note that the Enterprise Edition database you use for the Management Repository must have fine-grained access control turned on. This is required for successful Management Repository creation. Check `v$options` for this setting.

When using an existing database for the repository, be sure that all software, patch, and tuning requirements are met for the existing database and host, as well as for the repository.

Note: Refer to the Oracle Technology Network Web site for the latest information on the certified Management Repository platforms.

For more information on the recommended database initialization parameters refer to Section 3.3.2.1.1, "Check Database Initialization Parameters".

1.4.3.2 Management Service Software Requirements

The Management Service has no additional software requirements.

The Oracle Management Service is installed with and deployed on Oracle Application Server. As a result, when you install the Oracle Management Service, the installation procedure first installs Oracle Application Server.

Specifically, the installation procedure installs the Oracle Application Server J2EE and Web Cache installation type. The Management Service is deployed on its own OC4J container in this application server instance.

1.4.4 Network Requirements

The Oracle Management Service host and Repository host must be located in close proximity to each other. Ideally, the round trip network latency between the two should be less than 1 millisecond.

See Section A.5, "Network Issues" for more information about network requirements.

1.4.5 Prerequisite Checks

Table 1–6 lists all the prerequisite checks that the installer performs for each installation type.

Table 1–6 Prerequisites Checks for Each Installation Type

Installation Type	Component Name	Checks
Installing Enterprise Manager Using New Database	`oracle.sysman.top.em_seed`	**1.** Required Packages on the machine **2.** Certified Versions (that is, whether the Oracle software is certified on the current Operating System) **3.** Whether the required GLIBC is installed on the machine (UNIX only) **4.** Whether the machine has sufficient physical memory **5.** Kernel parameters **6.** Oracle home compatibility[1] **7.** Oracle home space check **8.** Checking host name **9.** Whether Oracle home is empty

Table 1–6 (Cont.) Prerequisites Checks for Each Installation Type

Installation Type	Component Name	Checks
Installing Enterprise Manager Using Existing Database	`oracle.sysman.top.oms`	**1.** Required Packages on the machine **2.** Certified Versions (that is, if the Oracle software is certified on the current operating system) **3.** If the required GLIBC is installed on the machine (UNIX only) **4.** If the machine has sufficient physical memory **5.** Oracle home compatibility **6.** If Oracle home is empty **7.** Checking host name **8.** Oracle home space check
Installing Additional Management Service	`oracle.sysman.top.oms`	**1.** Required Packages on the machine **2.** Certified Versions (that is, if the Oracle software is certified on the current operating system) **3.** If the required GLIBC is installed on the machine (UNIX only) **4.** If the machine has sufficient physical memory **5.** Oracle home compatibility **6.** If Oracle home is empty **7.** Oracle home space check **8.** Checking host name[2]
Installing Additional Management Agent	`oracle.top.agent`	**1.** Required Packages on the machine **2.** Certified Versions (that is, if the Oracle software is certified on the current operating system) **3.** If the required GLIBC is installed on the machine (UNIX only) **4.** The Targets monitored by the Management Agent Note that the Management Agent cannot monitor targets that have been installed by different users. **5.** Oracle home compatibility **6.** Checking host name **7.** Oracle home space check

[1] Disallowed component = oracle.rsf.oracore_rsf.

[2] The name of the host on which the installation is being performed should neither be `localhost.localdomain` nor an IP address. It must be a valid host name. At the time of invoking the installer, you can pass `ORACLE_HOSTNAME` as an argument.

1.5 Running the Prerequisite Check in Standalone Mode

You can run the prerequisite check in standalone mode prior to starting the `runInstaller`. This helps you identify and resolve issues that might otherwise cause the installation to fail.

Table 1–7 lists the prerequisite check that is run for each installation type followed by the command that you must execute to run these checks:

Table 1–7 Installation Type and the Corresponding Prerequisite Check

Installation Type	Component Name
Installing Enterprise Manager Using a New Database	`oracle.sysman.top.em_seed`
Installing Enterprise Manager Using an Existing Database	`oracle.sysman.top.oms`
Installing an Additional Management Service	`oracle.sysman.top.oms`
Installing an Additional Management Agent	`oracle.sysman.top.agent`

To run the prerequisite checker in standalone mode, execute the following command:

```
<DVD>/install/runInstaller -prereqchecker PREREQ_CONFIG_
LOCATION=<DVD>/rdbms/Disk1/stage/prereq -entryPoint <component name>_Core
-prereqLogLoc <log location>  -silent  -waitForCompletion
```

For the prerequisite checker to run successfully, ensure that the filepath specified in `--prereqLogLoc` exists on the machine. Substitute the data in contained within the angled brackets (< >) with the appropriate prerequisite check component name. For example, if you want to run the prerequisite check for the first installation type, execute the following command:

```
<DVD>/install/runInstaller -prereqchecker PREREQ_CONFIG_
LOCATION=<DVD>/rdbms/Disk1/stage/prereq -entryPoint oracle.sysman.top.em_seed_Core
-prereqLogLoc <log location>  -silent  -waitForCompletion
```

Note: On Microsoft Windows, replace `/runInstaller` with **`setup.exe`** and execute the command.

2

Things to Know Before Installation

This chapter provides information that helps you prepare better for an Enterprise Manager Grid Control installation. This chapter contains the following sections:

- Extracting Software from the Zip Files
- Oracle Directory
- Installing in an Existing Oracle Home
- First-Time Installation of Oracle Enterprise Manager Grid Control
- Installing Additional Languages
- Passwords and Restrictions
- Why Must I Log In as Root During Installation (UNIX Only)?
- Starting Oracle Universal Installer (OUI)

2.1 Obtaining Software from the Oracle Technology Network

You can download the Enterprise Manager software from the Oracle Technology Network (OTN) at

`http://www.oracle.com/technology/documentation`.

All OTN files have been archived using Info-ZIP's highly portable Zip utility. After downloading one or more of the archives, you will need the UnZip utility to extract the files. You must unzip the archive on the platform for which it was intended.

For example, if you download the file for the Linux Operating System version of Oracle Enterprise Manager, you must unzip the file on a Linux Operating System computer. If you unzip the file on a Microsoft Windows computer, and then move the stage area to a Linux Operating System machine, the stage area files will be corrupted because Microsoft Windows does not preserve the case sensitivity or the permission bits of Linux file names.

2.1.1 Extracting Software from the Zip Files

Verify that the file size of your downloaded file matches the file size displayed on OTN. Unzip each Zip file into a single directory.

If you plan to store the files on a DVD-ROM, create a DVD-ROM from the contents of the zip file (extracted contents) and not the Zip files itself; you need the unzipped contents of the Zip files to do the installation.

2.2 Oracle Directory

The directories in which you install Oracle Enterprise Manager components are called the Oracle homes. During installation, you specify the full path to a directory that contains all the Oracle homes as subdirectories. This parent directory is called the Oracle home directory or base directory.

If you choose to install Enterprise Manager Grid Control using a new database on a computer with no other Oracle software installed, Oracle Universal Installer creates an Oracle base directory for you. If Oracle software is already installed, then one or more Oracle base directories already exist. In the latter case, Oracle Universal Installer offers you a choice of Oracle base directories into which to install Oracle Database.

You are not required to create an Oracle base directory before installation, but you can do so if required. You can set the `ORACLE_BASE` environment directory, which Oracle Universal Installer will recognize.

> **Note:** You can choose to create a new Oracle base directory, even if other Oracle base directories exist on that system.

Names of Oracle homes must be 128 characters or fewer, and can contain only alphanumeric characters and underscores.

> **ATTENTION:** Spaces are not allowed anywhere in the Oracle home directory path. The installer validates this. If you have spaces in the Oracle home directory path, the installation will fail.

2.3 Installing in an Existing Oracle Home

Generally, you cannot install Enterprise Manager in an existing Oracle home, unless the Oracle home is empty.

2.4 First-Time Installation of Oracle Enterprise Manager Grid Control

If Enterprise Manager Grid Control is the first Oracle product that you are installing, the installer prompts you to specify an inventory directory (also called the `oraInventory` directory). This inventory directory is used by the installer to place all the installer files and directories on the computer. The installer automatically sets up subdirectories for each Oracle product to contain the inventory data.

The inventory directory is separate from the Oracle home directory.

When you specify the Oracle inventory directory path, you must also 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.

If you have a previous version of Enterprise Manager installed on the computer, the installer uses the existing inventory directory. Ensure that you have write permissions on that directory. The best way of ensuring this is to run the installer as the same operating system user who installed the existing release of Enterprise Manager Grid Control.

2.4.1 Installing Additional Languages

By default, the installer installs Oracle Enterprise Manager with text in English and in the operating system language. If you need additional languages, select the required languages in the Select Languages screen of the installer.

When you select additional languages to install, the installer also installs fonts required to display the languages.

For some components, languages are installed only if you select them during installation. In this case, if you access the application in a language that is not available, it reverts to the server locale language.

For other components, available languages are installed regardless of what you select during installation. In this case, however, fonts are installed only for the languages that are explicitly selected. When you access the application, it uses text in your language because the language was installed. However, if you do not have the appropriate fonts to render the text, the text appears as square boxes. This usually applies to the Chinese, Japanese, and Korean languages.

2.5 Passwords and Restrictions

The installer prompts you to specify the passwords that are used to secure your entire Grid Control environment. This includes the Management Service and Management Repository passwords. One of the database passwords that you specify is the password required to access the application server (`ias_admin`). The `ias_admin` user is the administrative user for Oracle Application Server instances. To manage Oracle Application Server instances using Application Server Control, you must log in as `ias_admin`. Ensure the passwords you specify have all the required permissions.

Password Restrictions

The following restrictions apply to passwords:

- Passwords must be between 5 and 30 characters long.
- Passwords cannot be the same as the user name.
- Passwords must include only lowercase or uppercase alphanumeric characters.

> **Note:** The SYSMAN password can include underscore (_), hyphen (-), dollar ($), and hash (#) along with alphanumeric characters. Alphabetic characters can be lowercase or uppercase.

- Passwords have at least one letter, one integer, and one special character (underscore).
- Passwords cannot be Oracle reserved words. See Appendix G, "Oracle Reserved Words" for a complete list of reserved words.

Oracle recommends that the passwords that you specify are not simple or obvious words, such as welcome, account, database, or user.

2.6 Why Must I Log In as Root During Installation (UNIX Only)?

At least once during installation, the installer prompts you to log in as the `root` user and run a script. You must log in as `root` because the script edits files in the `/etc` directory.

2.6.1 Running root.sh During Installation (UNIX Only)

The installer prompts you to run the `root.sh` script in a separate window. This script creates files in the local bin directory (`/usr/local/bin`, by default).

On IBM AIX and HP UX platforms, the script the files in the `/var/opt` directory.

2.7 Starting Oracle Universal Installer (OUI)

To set the mount point manually, complete these steps:

1. DVD-ROM users: Insert the Oracle Enterprise Manager Grid Control DVD-ROM into the DVD-ROM drive.
2. Start Oracle Universal Installer by executing the `runInstaller` script for Linux from the top directory of the DVD.

   Alternatively, you can change the directory to the `ORACLE_BASE`, the root directory where you will install the Oracle home, then specify the full path to `<DVD>/runInstaller` in OUI.

DVD-ROM

prompt> `cd`

prompt> `mount_point/10.2<DVD>/runInstaller`

This launches Oracle Universal Installer through which you install Enterprise Manager Grid Control.

2.8 Enterprise Manager Configuration Plug-in (EMCP)

When you perform an Enterprise Manager installation, this installation does not include the Enterprise Manager Configuration Plug-in (EMCP) in the database Oracle home. EMCP is part of the Management Repository Oracle home only when you perform a standalone database installation.

Part II

Enterprise Manager Installation

Part 2 of the book provides information and step-by-step instructions on the various Enterprise Manager installation types. It also contains detailed information on all Management Agent deployment mechanisms.

Part 2 contains the following chapters:

- Chapter 3, "Installing Enterprise Manager"
- Chapter 4, "Enterprise Manager Silent Installations"
- Chapter 6, "Deploying the Management Agent"
- Chapter 8, "Deploying Cluster Agent"
- Chapter 9, "Management Agent Cloning"

3

Installing Enterprise Manager

This chapter describes the installation options available for Enterprise Manager, and provides basic instructions for installing using Oracle Universal Installer. This chapter contains the following sections:

- Accessing the Installation Software
- Using Oracle Universal Installer
- Enterprise Manager Installation Types
- Deinstallation of Enterprise Manager Grid Control

Note: No environment variable specific to Enterprise Manager need to be set prior to installation. The `$ORACLE_HOME` and `$ORACLE_SID` variables should not be set; Oracle directories should not appear in the PATH.

See Also: For information on migrating to Oracle Enterprise Manager 10*g* from previous versions of Enterprise Manager, see *Oracle Enterprise Manager Advanced Configuration*.

3.1 Accessing the Installation Software

The Oracle Enterprise Manager Grid Control software is available on a DVD-ROM, or you can download it from the Oracle Technology Network (OTN) Web site. You can access and install Enterprise Manager Grid Control by using the following scenarios:

- Installing from a Remote DVD Drive (UNIX Only)
- Installing on Remote Computers Using Remote Access Software

3.1.1 Installing from a Remote DVD Drive (UNIX Only)

If the computer where you want to install Enterprise Manager does not have a DVD drive, you can perform the installation from a remote DVD drive by mounting (sharing) that DVD drive.

3.1.1.1 Setting the Mount Point for the DVD-ROM on Linux

On most Linux systems, the disk mounts automatically when you insert it into the disk drive. To mount the disk, complete the following steps:

1. Insert the Oracle Enterprise Manager DVD into the disk drive.
2. To verify if the disk is automatically mounted, enter 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, enter 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>
     ```

3.1.2 Setting the Mount Point for the DVD-ROM on AIX

On most AIX systems, the disk mounts automatically when you insert it into the disk drive. To manually mount the disk, complete the following steps:

1. Switch the user to `root` user by executing the following command:

   ```
   $ su -root
   ```

2. If required, enter a command similar to the following to eject the currently mounted disk and to remove it from the drive:

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

3. Insert the disk into the drive.
4. Enter a command similar to the following:

   ```
   # /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.

5. If Oracle Universal Installer displays the Disk Location dialog box, enter the disk mount point directory path. For example: `/SD_DVD`

3.1.3 Installing on Remote Computers Using Remote Access Software

Consider a scenario where the remote computer has the hard drive and will run Enterprise Manager, but you do not have physical access to the computer. You can perform the installation on the remote computer, provided it is running remote access software such as VNC or Symantec pcAnywhere. You also need the remote access software running on your local computer.

You can install Enterprise Manager on the remote computer in one of two ways:

- If you have copied the contents of the Oracle Enterprise Manager Grid Control DVD to a hard drive, you can install from the hard drive.
- You can insert the DVD into a drive on your local computer, and install from the DVD.

3.1.3.1 Installing from a Hard Drive

If you have copied the contents of the Oracle Enterprise Manger DVD to a hard drive, you can install from the hard drive.

The steps that you need to complete are the following:

1. Ensure the remote access software is installed and running on the remote and local computers.
2. Share the hard drive that contains the Oracle Enterprise Manager DVD.
3. Map a drive letter on the remote computer to the shared hard drive. You would use the remote access software to do this on the remote computer.
4. Run Oracle Universal Installer on the remote computer using the remote access software. You can access Oracle Universal Installer from the shared hard drive.

For more information on running the installer, see Section 3.2.2, "Starting the Installer" for more information.

3.1.3.2 Installing from a Remote DVD Drive

You can insert the DVD into a drive on your local computer, and install from the DVD.

The steps that you need to complete are the following:

1. Ensure the remote access software is installed and running on the remote and local computers.
2. Share the DVD content on the local computer.

   Map a drive letter on the remote computer to the shared hard drive. You would use the remote access software to do this on the remote computer.
3. Run Oracle Universal Installer on the remote computer using the remote access software. You access Oracle Universal Installer from the shared DVD drive.

For more information on running the installer, see Section 3.2.2, "Starting the Installer" for more information.

3.2 Using Oracle Universal Installer

The Enterprise Manager installation uses Oracle Universal Installer, a Java-based graphical user interface application that enables you to install Oracle components from a DVD, multiple DVDs, or the Web.

> **See Also:** For information on using Oracle Universal Installer to install Oracle software, refer to the *Oracle Universal Installer and OPatch User's Guide*.

3.2.1 Specifying a Temporary Directory

When you start Oracle Universal Installer (OUI), it automatically copies some executable files and link files into the default `/tmp` directory (`C:\Documents and Settings\<user ID>\Local Settings\Temp` on Microsoft Windows) on the machine. If the machine is set to run `cron` jobs (along with many other processes that may be running) periodically, these jobs attempt to clean up the default temporary directory, thereby deleting some files and causing OUI to fail.

If there are any `cron` jobs or processes that are automatically run on the machines to clean up the temporary directories, ensure you set the `TMP` or `TEMP` environment variable to a different location (than the default location) that is secure on the hard

drive (meaning a location on which the cleanup jobs are not run). Also ensure that you have write permissions on this alternative `TEMP` directory. This must be done before you execute `runInstaller` (`setup.exe` on Microsoft Windows).

> **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.

3.2.2 Starting the Installer

Start Oracle Universal Installer by executing the `runInstaller` (or `setup.exe` on Microsoft Windows) from the top-level directory of the DVD.

Alternatively, you can change the directory to the `Parent Directory` (or the root directory) where you will install the Oracle home, then specify the full path to `/runInstaller` (`setup.exe` on Microsoft Windows).

To specify a response file for a silent installation, use the following command:

```
$ ./<runInstaller or setup.exe> -responseFile <responsefile_location> <optional_
parameters> -silent
```

> **See Also:** Refer to the Creating and Customizing Response Files chapter of the *Oracle Universal Installer and OPatch User's Guide* for more information on silent installations.

When you invoke the installer, the installation runs prerequisite checks on the following:

- Operating System Version
- Operating System Packages
- Operating System Patches
- User Credentials
- TEMP and SWAP space
- DISPLAY Colors
- Additional Patches
- Kernel version
- Oracle home is empty
- Oracle home space
- Physical memory

The list of prerequisite checks that must be executed can be viewed in the initialization parameters file located in the following directory of the product-specific installation:

```
<DVD>/install/oraparam.ini
```

If a prerequisite check fails, you are prompted to continue, or stop the installation process. You may install the missing software at this point, or discontinue the installation. Note, however, that you may have newer patches that supersede the required patches.

Once you continue, follow the installation instructions on the screen. At any time while installing Enterprise Manager, you can click **Help** for information about the pages.

3.3 Enterprise Manager Installation Types

This section contains the following topics:

- Installing Enterprise Manager 10g Grid Control Using a New Database
- Installing Enterprise Manager 10g Grid Control Using an Existing Database
- Installing an Additional Management Service
- Installing a Management Agent

The following predefined installation options, described in Table 3–1, determine which components will be installed on your system. During installation, you are prompted to choose one of the following options. Note that the hard disk space represents the *footprint* that the components of the installation consume, and the physical memory prerequisites refer to the initial RAM required for installation, and not the operating memory.

Table 3–1 Enterprise Manager Installation Options

Installation Option	Description	Hard Disk Space (Oracle Homes)	Physical Memory
Enterprise Manager 10*g* Grid Control Using a New Database	Installs Enterprise Manager Grid Control onto the host machine, creating the Management Repository on a new Enterprise Edition Oracle Database 10g Release 1 (10.1.0.4). *Note:* Enterprise Manager Grid Control consists of the Management Repository, Management Service, Management Agent, and OracleAS J2EE and Web Cache, against which the middle-tier Management Service Web application is deployed.	▪ 4.5 GB (Linux/Solaris) ▪ 9GB (HP-UX) ▪ 4.5 GB (Win) ▪ 9 GB (AIX)	▪ 2 GB (Linux/Solaris) ▪ 2 Gb (HP-UX) ▪ 2 GB (Win) ▪ 2 GB (AIX)
Enterprise Manager 10*g* Grid Control Using an Existing Database	Installs Enterprise Manager Grid Control onto the host machine, creating the Management Repository on a qualified existing database, which may be local to the host or remote. See Section 1.4.3.1, "Management Repository Software Requirements" for more information on supported repository releases. *Note:* If the repository is on the same machine as the Management Service, allow 1 GB more memory than recommended. Oracle recommends installing Enterprise Manager on a separate machine from the Oracle Database that contains the Management Repository.	▪ 2.5 GB (Linux/Solaris) ▪ 5 GB (HP-UX) ▪ 2.5 GB (Win) ▪ 5 GB (AIX)	▪ 2 GB (Linux/Solaris) ▪ 2 GB (HP-UX) ▪ 2 GB (Win) ▪ 2 GB (AIX)
Additional Management Service	Installs the Management Repository onto the host machine. Allows you to specify an existing Management Repository, either local or remote.	▪ 2 GB (all UNIX platforms) ▪ 2.5 Gb (Win)	▪ 2 GB (all UNIX platforms) ▪ 2 GB (Win)

Table 3–1 (Cont.) Enterprise Manager Installation Options

Installation Option	Description	Hard Disk Space (Oracle Homes)	Physical Memory
Additional Management Agent	Installs the Management Agent on the target machine you want to monitor with the Grid Control console. The Management Service and Management Repository are not required on the same machine as the Management Agent, but must exist within the enterprise. The Management Agent may be installed on a cluster node. Oracle recommends that the target host on which you are installing the agent have a static IP address and not DHCP.	▪ 400 MB (all UNIX platforms) ▪ 500 MB (Win)	No minimum requirement

Note: When you perform an Enterprise Manager installation, this installation does not include Enterprise Manager Configuration Plug-in (EMCP) in the database Oracle home. EMCP is part of the repository database Oracle home only when you perform a standalone database installation.

See Also: Refer to *Oracle Enterprise Manager Concepts* for more detailed information about the Grid Control Console, the Management Repository, Management Service, and Management Agent, and how they work together.

See Chapter 4, "Enterprise Manager Silent Installations" for more information.

Installation Instructions

Start Oracle Universal Installer by executing the `runInstaller` script in Linux (`<DVD>/runInstaller`).

On Microsoft Windows, execute `<DVD>/setup.exe` to start the Oracle Universal Installer.

Installation types are predefined component sets that determine which components to install. The Enterprise Manager 10*g* Grid Control installation involves four top-level components, each representing an installation type. Select one of the installation types described in the following sections.

3.3.1 Installing Enterprise Manager 10*g* Grid Control Using a New Database

This option is selected by default when you run the Enterprise Manager Grid Control installer. Keep this selection if you want to install Enterprise Manager and all its dependent components on a single host. If you choose this installation option, you do not need an existing Enterprise Edition database, because one is created during the installation.

Note: The default port for the listener is 1521 for the Oracle Database 10*g* R2 (10.2.0.2) provided with the full installation.

3.3.1.1 Permissions and Prerequisites

The installation should not be run by the `root` user (UNIX only). Ensure the following prerequisites are met:

- User should be a DBA user.
- User should be able to create process-level tokens (Microsoft Windows only).
- User should be able to log in as a batch job (Microsoft Windows only).
- User should be able to adjust memory quota for process (Microsoft Windows only).
- User should be part of the ORA-DBA group (Microsoft Windows only) and have Administrator permissions.
- The name of the host on which the installation is being performed should neither be `localhost.localdomain` nor an IP address. It must be a valid host name. At the time of invoking the installer, you can pass `ORACLE_HOSTNAME` as an argument.

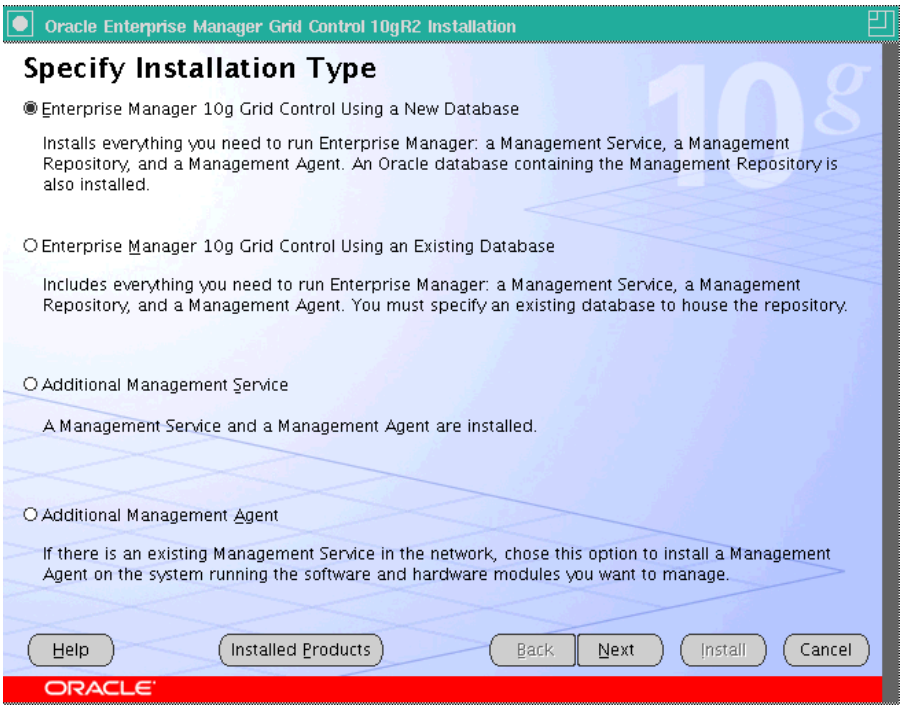
> **Caution:** Do not pass the argument as `ORACLE_HOSTNAME=<localhost.localdomain>` or `ORACLE_HOSTNAME=<IP address>`. You must pass the argument as **`ORACLE_HOSTNAME=<valid host name>`**.

3.3.1.2 To Install Enterprise Manager Using a New Database

Complete the following steps to perform an Enterprise Manager installation using a new database:

1. Select the first option (**Enterprise Manager 10g Grid Control Using a New Database**). By default, this option is selected when you invoke the installer.

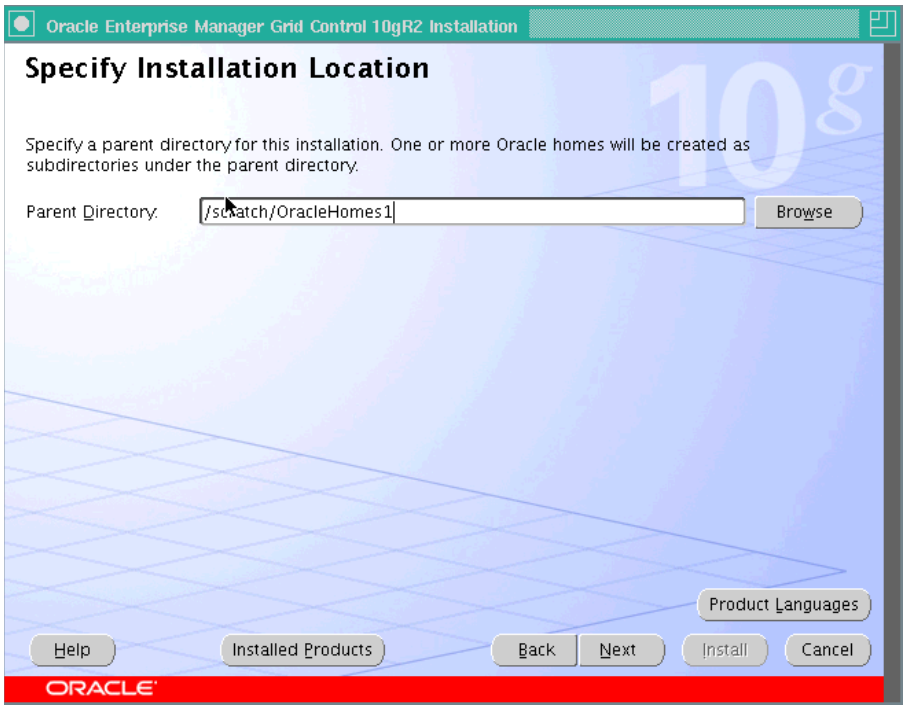
Figure 3–1 Specify Installation Type



2. Click **Next.** In the Specify Installation Location screen that appears, specify a parent directory (base directory), for example, `/scratch/OracleHomes` (on Linux), for the new installation. All the Oracle homes created during this installation are created as subdirectories under this parent directory. For example: *db10g*, *oms10g*, and *agent10g*.

Note: Ensure you do not use symbolic links to specify the Oracle home path.

Figure 3–2 Specify Installation Location



The selected products are installed in the English language by default. If you want to install the product in a different language, click **Product Languages**.

The Language Selection screen appears.

Figure 3–3 Language Selection

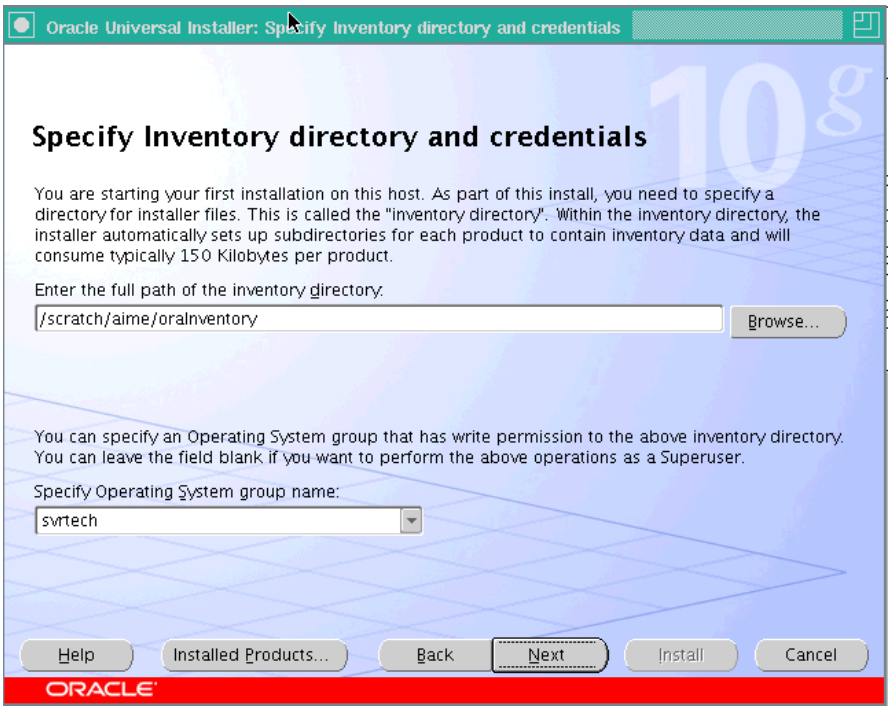
Choose the languages that you want to use to run Enterprise Manager.

Note: The languages that you select here change the language of Enterprise Manager only, and not the language of the installation itself.

---

3. Click **Next**. The Specify Inventory Directory and Credentials screen appears only if Enterprise Manager Grid Control is the first Oracle product that you are installing on the machine.

Figure 3–4 Specify Inventory Directory and Credentials



a. Specify the full path to the directory where Oracle Universal Installer (OUI) should place inventory files and directories. For example, `oracle_base/oraInventory` (on Linux).

Note: If you are performing the installation on a **Microsoft Windows** platform, the Specify Inventory Directory and Credentials screen will not appear.

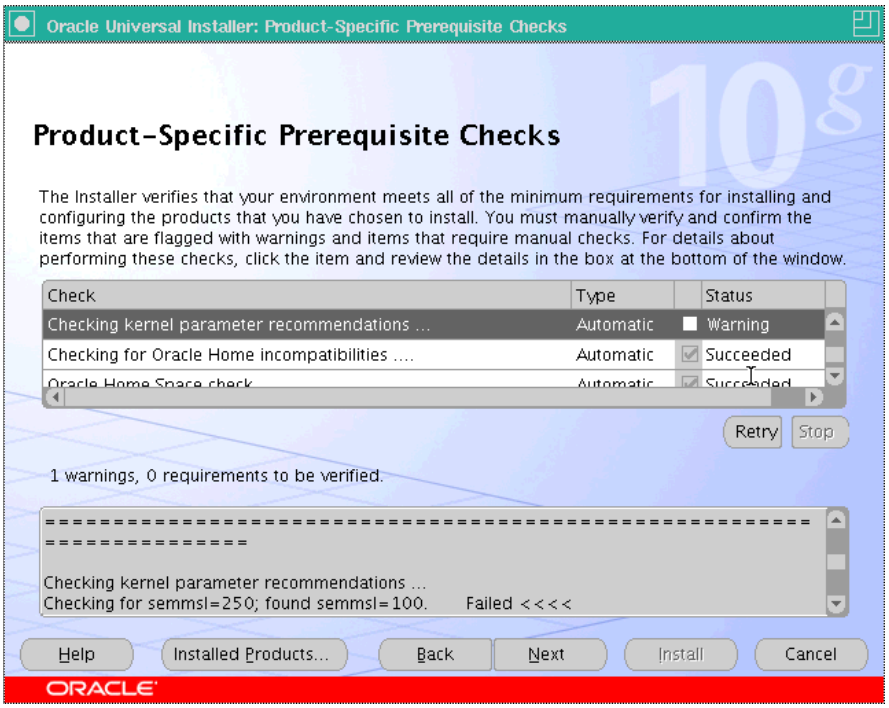
On Microsoft Windows, the default inventory files location is `<system drive>\Program Files\Oracle\Inventory`.

Refer to the Enterprise Manager online Help for more information on guidelines recommended by Oracle for naming the directories.

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.

4. Click **Next**. The Product-Specific Prerequisite Checks screen appears.

Figure 3–5 Product-Specific Prerequisite Checks



At this point, the installer runs some prerequisite checks to verify if the environment meets the minimum requirements for a successful Enterprise Manager installation.

Early detection of system environment problems such as insufficient disk space, missing patches, inappropriate hardware, and so on results in a smoother installation later.

This screen displays the name, type, and status for all prerequisite checks designed for the installation. Automatic checks are run first, followed by optional and manual checks.

Depending on the status of the automatic checks, you must verify all warning and manual checks. At some point, if you have stopped the prerequisite check and want to rerun these checks, select the checks that you want to rerun and click **Retry**. As each check runs, a progress bar is shown, and test details (expected results, actual results, error messages, instructions) are displayed in the details section at the bottom of the screen.

Note: You can also run these prerequisite checks in standalone mode, prior to starting the `runInstaller`. See Section 1.5, "Running the Prerequisite Check in Standalone Mode" for more information.

---

a. To stop all prerequisite checks, click **Stop**. At any point in time, click a prerequisite check to view its corresponding details, including the recommended user actions.

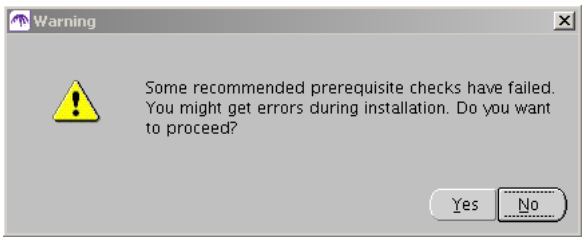
Note: You must manually verify and confirm all checks that were flagged with a warning, skipped (stopped by user), or failed.

---

b. To continue with the installation without retrying, click **Next**.

An error message is displayed if some recommended prerequisite checks have failed.

Figure 3–6 Warning



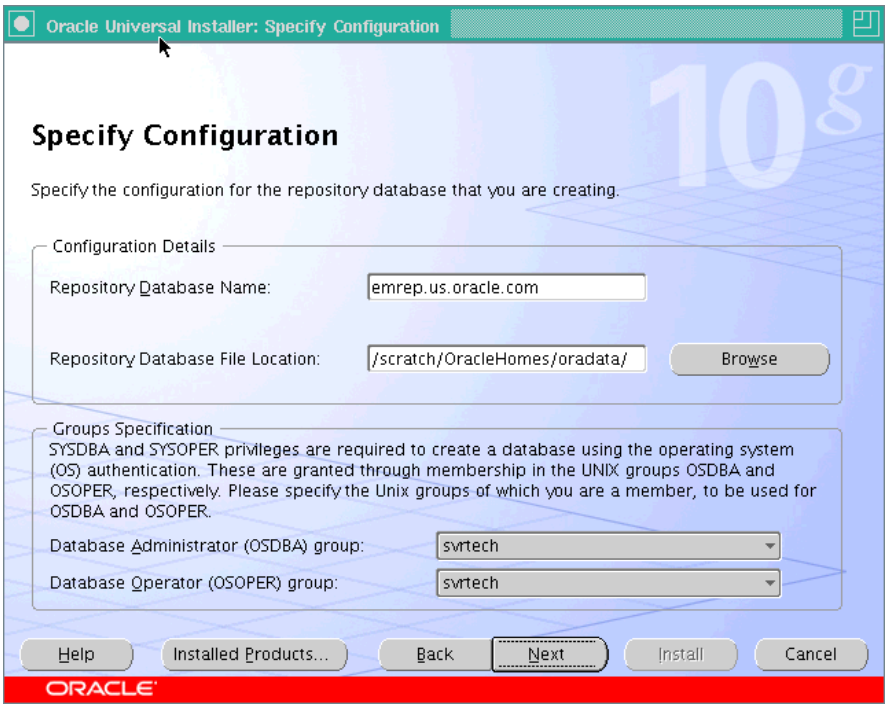
c. Click **No** to go back and rerun the prerequisite check. Click **Yes** to ignore the message and continue with the installation.

Note: It is recommended that you retry checks that were flagged with warnings, failed, or were skipped (stopped by the user) before continuing with the installation.

---

5. The Specify Configuration screen appears.

Figure 3–7 Specify Configuration



You must specify the configuration details for the new database that you are creating, and select the appropriate recipients of the OSDBA and OSOPER privileges (on UNIX only).

Note: Your Management Repository may also require patches to be applied after successful installation. See Section 1.4.2, "Enterprise Manager Platform and Target Certification Requirements" for more information.

---

a. Specify the new Database Name and the Database File Location (location where the new database is going to reside).

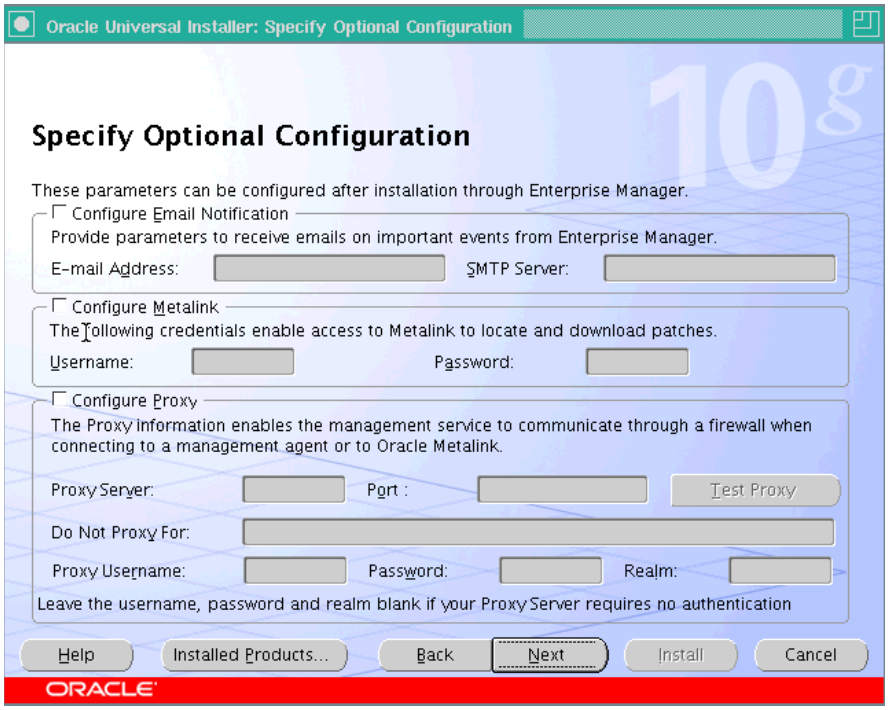
Note: It is recommended that you specify a fully qualified database name (for example, `emrep.<domain_name>`), though appending the database name with the domain name is not mandatory.

---

b. In the Group Specification section, select the OSDBA and OSOPER groups of which you are a member. These memberships are required to grant the SYSDBA and SYSOPER permissions that are, in turn, required to create the new database using the operating system authentication.

6. Click **Next**. The Specify Optional Configuration screen appears.

Figure 3–8 Specify Optional Configuration



As the name suggests, all the fields on this screen are optional, and are disabled by default. Select the required check box to enable the corresponding fields.

a. In the Configure Email Notification section, specify an appropriate e-mail address, and the corresponding SMTP server name. You will receive important information on the condition of the monitored targets, including critical alerts at this e-mail address.

The e-mail address that you specify should be associated with the SYSMAN user to receive notifications.

The SMTP Server is the name of the mail server (for example `mail.acme.com`). For Linux, the default SMTP server is the local host name. Use the fully qualified host name (including domain).

Note: If you do not provide the e-mail notification information, this feature is not enabled upon installation. You may also choose to configure these settings through the Enterprise Manager console by clicking **Notification Methods** under Setup. Refer to the Enterprise Manager online Help for more information.

---

b. Specify the Oracle*MetaLink* credentials.

If you prefer, you can also enter this information through the Enterprise Manager console after installation by clicking **Patching Setup**, under Setup.

Note: Enterprise Manager uses these credentials to search for and download patches from `http://oracle.com/support/metalink/index.html`

---

c. Specify the Proxy Information if Enterprise Manager is using a proxy server for external access. Table 3–2 describes each of the fields under this section.

Table 3–2 Specify Proxy information - Input Fields

Input	Description
Proxy Server	Specify the proxy server host name. For example, **`www-fooproxy.here.com`**
Port	Specify the port at which the server is listening. For example, **`80`**. See Appendix E, "Enterprise Manager Firewall Port Requirements" for more information on specifying ports when you are using a firewall in your grid environment.
Do Not Proxy For	Specify the URLs that do not need the proxy server to be accessed. You can specify multiple comma-separated values. For example, .here.com, .us.mycompany.com, .uk.mycompany.com, and so on. Note that you must always specify *fully qualified host names.*
Proxy User and Password	Specify the user name and password only if the proxy server has been configured to use these credentials for authentication. These are optional fields.
Realm	Specify an appropriate realm value. This becomes a mandatory field only if the proxy server credentials have been configured using a realm. A realm is a string value assigned by the proxy server to indicate the secure space that requires authentication.
Test Proxy	Click this button to verify your proxy server settings.

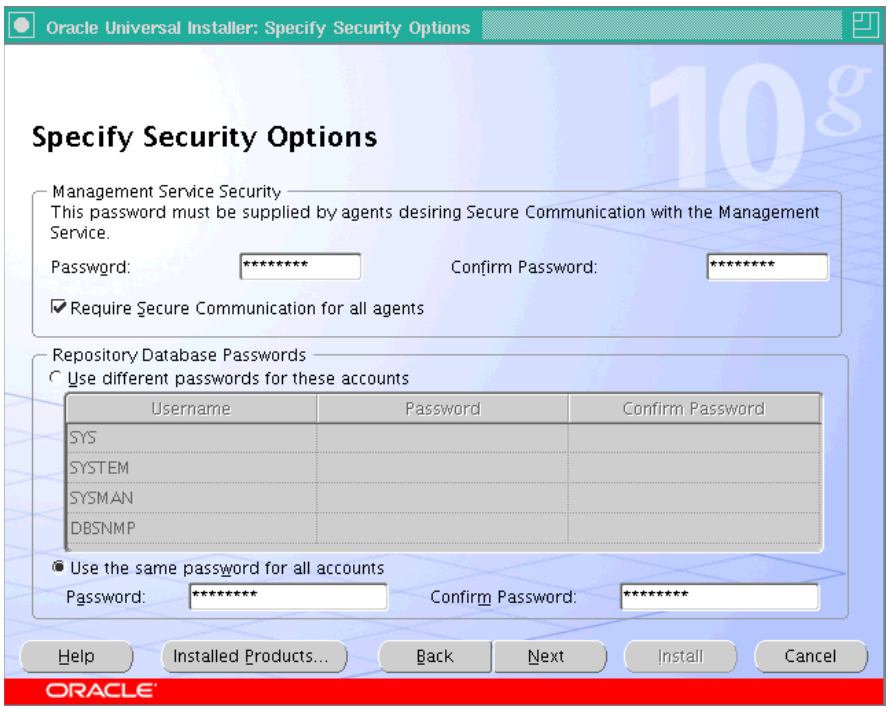
Note: When you search for a patch, if the proxy properties (saved in the `sysman/config/emoms.properties` file) are not set, or are set incorrectly, you receive an error message indicating that Enterprise Manager cannot access the Oracle*MetaLink* Web site.

Caution: If the proxy server requires user authentication before providing access, you must specify these credentials here or through the Patching Setup screen under Setup in the Grid Control console.

---

7. Click **Next**. The Specify Security Options screen appears.

Figure 3–9 Specify Security Options



You must specify the passwords that are used to secure your entire Grid Control environment. This screen has two sections - Management Service Security, and Repository Database Passwords.

- Management Server Security: The password that you specify here is used to secure and lock the Oracle Management Service (OMS).

  Select **Require Secure Communications for all agents** if you want the secure OMS to communicate only with secure Management Agents. This is optional, though recommended.

  For example, consider you have unsecured 10.1.*n* agents in the Grid and you have secured the OMS. Now, if you select the Require Secure Communications option, then all communication between the 10.2 OMS and 10.1.*n* agents fails (because these agents have not been secured).

Note: To secure a Management Agent, execute following command:

```
<AGENT_HOME>/bin/emctl secure agent
```

- Repository Database Passwords: Specify the passwords for each of the administrative database accounts listed in Table 3–3.

Table 3–3 Repository Database Passwords

User Account	Applies to	Description
SYS	Management Repository	Super Administrator for the Management Repository database.
SYSTEM	Management Repository	Administrator for the Management Repository database.
DBSNMP	Management Repository	Monitoring user for the Management Repository database.
SYSMAN	Management Repository, Application Server, and Grid Control	The default Grid Control Super Administrator and Owner of the Management Repository database schema and the Grid Control application user. The default ias_admin password is the same as the password assigned to the SYSMAN account. This is required to access the Oracle application server (`ias_admin`). The `ias_admin` user is the administrative user for the Oracle Application Server console.

You can use the same password for all four accounts, or specify a different password for each one. These passwords are used to secure the Management Repository database.

To specify a different password for each account, select **Use different passwords for these accounts** and specify the passwords for each account.

To specify the same password for all accounts, select **Use the same password for all accounts** and specify one password to be used for all database accounts.

Note: The SYS, SYSMAN, DBSNMP, and SYSTEM users are privileged database users. You must remember the passwords that you specify for them. For more information on password restrictions and recommendations, see *Oracle Database Administrator's Guide*.

Password Restrictions and Recommendations

The following restrictions apply to passwords:

– Passwords must be between 5 and 30 characters long.

– Passwords should not start with a number.

– Passwords cannot be the same as the user name.

– Passwords must include letters (lowercase/uppercase) and numbers only.

Note: The SYSMAN password can include underscores (_), and hyphens (-), dollar ($), and hash (#) along with alphanumeric characters. Alphabetic characters can be uppercase or lowercase.

– Passwords cannot be Oracle reserved words. See Appendix G, "Oracle Reserved Words" for more information.

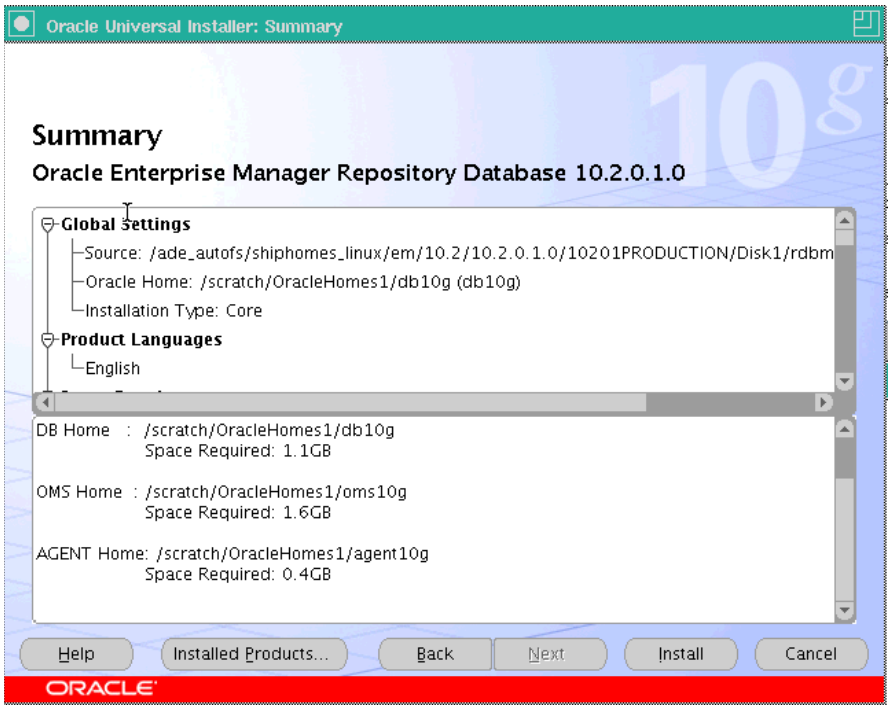
Note: Oracle recommends that the passwords you specify have the following characteristics:

1. Have at least one letter, one integer, and one special character (underscore).
2. Are not simple or obvious words such as welcome, account, database, or user.

---

8. Click **Next**. The Summary screen appears.

Figure 3–10 Installation Summary



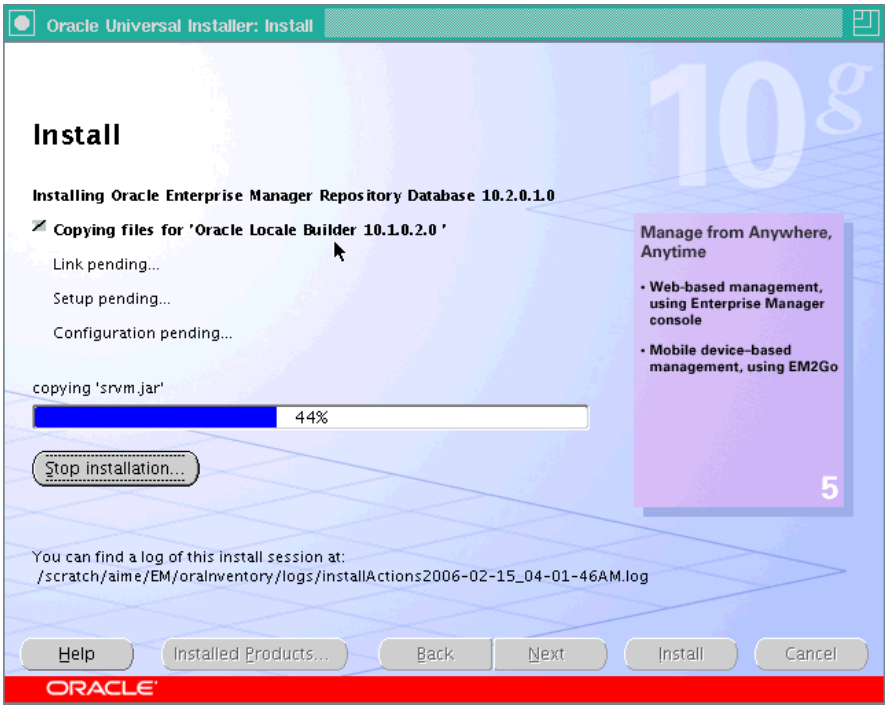
This screen provides a summary of the options that you have selected during the installation process. Depending on the installation type, it also provides any or all of the following details:

- Global Settings
- Product Languages
- Space Requirements
- Installed Products

Verify the choices that you have made.

a. Click **Install** to start the installation. The Install screen that appears displays the installation progress bar.

Figure 3–11 Installation in Progress

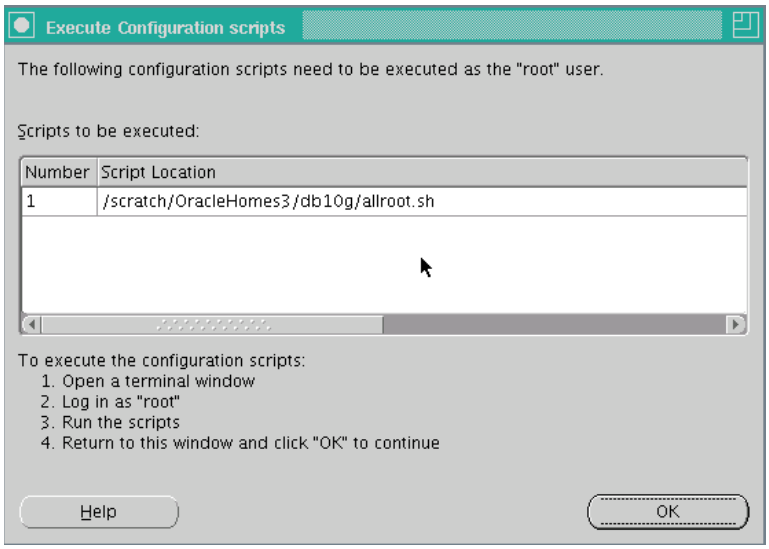


The installer seamlessly installs all Grid Control components based on the installation type you selected.

b. During the installation, you are prompted to execute certain configuration scripts. These scripts and their locations are listed in the Execute Configuration Scripts dialog box that appears (on UNIX only).

Note: The Execute Configuration Scripts dialog box will not appear on Microsoft Windows. You will be directed to the Configuration Assistants screen (step 9) in the next step.

Figure 3–12 Execute Configuration Scripts

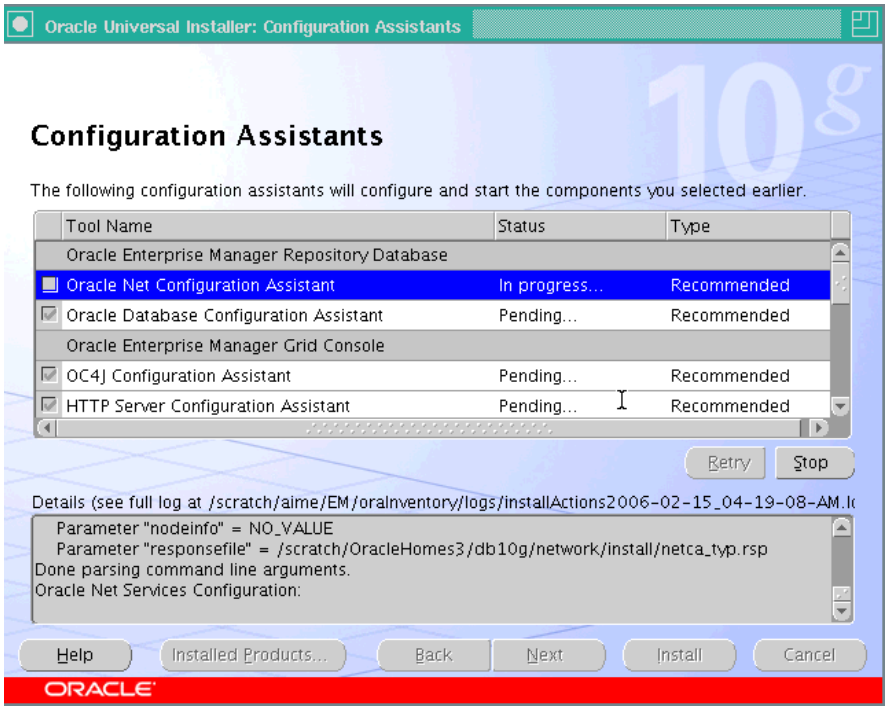


Go to the computer window, log in as `root`, and run these configuration scripts.

c. Return to the dialog box (shown in Figure 3–12) after executing the scripts, and click **OK** to continue the installation.

9. The Configuration Assistants screen appears. At this point, the installer starts running the configuration assistants.

Figure 3–13 Configuration Assistants



This screen displays the name, status, and the type of each configuration tool that Oracle recommends to be run before completing the installation.

Table 3–4 lists all the configuration tools that are run during a typical Enterprise Manager installation (Install Enterprise Manager Using a new database).

Table 3–4 Enterprise Manager Configuration Tools

Product	Configuration Tool[1]
Oracle Repository Database	▪ Oracle Net Configuration Assistant ▪ Oracle Database Configuration Assistant ▪ OC4J Configuration Assistant
Oracle Enterprise Manager Grid Console	▪ OC4J Configuration Assistant ▪ HTTP Server Configuration Assistant ▪ Java Configuration Assistant ▪ Web Cache Configuration Assistant ▪ OracleAS Instance Configuration Assistant ▪ Register DCM Plugins with Enterprise Manager ▪ DCM Repository Backups Assistant ▪ Enterprise Manager Technology Stack Upgrade ▪ Oracle Management Service Configuration
Oracle Management Agent	▪ Agent Configuration Assistant

[1] Depending on the installation type that you have selected, any or all of the configuration tools listed in this table will be run.

For more information on the installation logs that are created and their locations, see Appendix F, "Installation and Configuration Log File Locations". In case of failure of any configuration assistant, refer to the logs and re-rerun the configuration assistants as described in Section A.2.1, "Configuration Assistants Fail During Enterprise Manager Installation".

Note: The individual log files for each configuration tool are available at the following directory:

```
ORACLE_HOME/cfgtoollogs/cfgfw
```

Besides the individual configuration logs, this directory also contains `cfmLogger_timestamp.log` (The timestamp depends on the local time and has a format such as `cfmLogger_2005_08_19_01-27-05-AM.log`.). This log file contains all the configuration tool logs.

---

a. To stop running a configuration tool, select it and click **Stop**.

b. To rerun a configuration tool, select it and click **Retry**.

Note: The installation is considered successful even if all the configuration tools fail, irrespective of their type (recommended/optional). However, failing to successfully run all the configuration tools results in an improperly configured product, which may not function. Refer to the Enterprise Manager installation online Help for more information.

Note: In the event a particular configuration assistant fails, you can choose to rerun only that configuration assistant (in standalone mode). See Section 3.4, "Executing the runConfig Tool from the Command Line" for more information.

10. After successfully running all the recommended configuration tools, the End of Installation screen appears.

    This screen displays some important information about the products you have installed. This information is also available in the `<AGENT_HOME>/sysman/setupinfo.txt` file.

    For example, it might contain information about the URLs for particular Web applications.

3.3.2 Installing Enterprise Manager 10*g* Grid Control Using an Existing Database

Select this option if you want to perform a complete Enterprise Manager Grid Control installation and have a qualified existing database in which to create the Management Repository. The database can be local or remote to the machine on which you are installing. Oracle Real Application Clusters (RAC) databases must be on a shared disk.

The hardware requirements for the Management Repository and the operating system patch requirements for the host machine must be satisfied regardless of whether you choose to create a new database or use an existing database for the Management Repository during the installation session.

If you plan to use an existing database for your Management Repository creation, check all software requirements for the database and host, as well as for the repository.

3.3.2.1 Prerequisites

- Ensure the installation is not run by the `root` user.
- Verify Database Setting (Initialization Parameters).
- Ensure the existing database and listener are up.
- Ensure that the profile of the Password Verification resource name has the "Default" value. If the Password Verification is enabled, repository creation may fail.
- Ensure there is sufficient physical memory available for this installation type. See Table 3–1, " Enterprise Manager Installation Options" for more information on the recommended hard disk and memory requirements. See Section 1.4.1.1, "Recommended CPU and Memory Allocation" for more information.
- Ensure the database release should be 9.2.0.6 and later, or 10.1.0.4 and later. Execute `select banner from v$version` to find out the current database version.

- Ensure the name of the host on which the installation is being performed is neither be `localhost.localdomain` nor an IP address. It must be a valid host name. At the time of invoking the installer, you can pass `ORACLE_HOSTNAME` as an argument.

> **Caution:** Do not pass the argument as `ORACLE_HOSTNAME=<localhost.localdomain>` or `ORACLE_HOSTNAME=<IP address>`. You must pass the argument as **`ORACLE_HOSTNAME=<valid host name>`**.

See Section 3.3.2.1.1, "Check Database Initialization Parameters" for a detailed list of database initialization parameter settings based on the Enterprise Manager deployment size.

Section 1.4.3, "Enterprise Manager Software Requirements" includes information on the releases of Oracle Database and Oracle Real Application Clusters Database that qualify for Management Repository creation.

See Chapter 1, "Preinstallation Requirements" for more information on hardware and software requirements.

3.3.2.1.1 Check Database Initialization Parameters

The initialization parameters must be set correctly for your qualified existing Enterprise Edition database to be able to run a Management Repository. You should also set all *fixed* parameters for your Management Repository database.

> **See Also:** For more information about managing initialization parameters, refer to the *Managing Initialization Parameters Using a Server Parameter File* chapter of the *Oracle Database Administrator's Guide*.

After making the changes, you must shut down and restart the database.

> **See Also:** For instructions on shutting down the database, refer to the *Starting Up and Shutting Down* chapter in the *Oracle Database Administrator's Guide*.

Fixed Initialization Parameter Values

The following table lists the parameters and their fixed values that must be met for successful Management Repository database creation. These parameters are verified by Oracle Universal Installer prerequisite checks during installation.

> **Note:** Make sure that the Enterprise Edition database you select for your Management Repository has the **fine-grained access control** option set to true. This is required for successful Management Repository creation. Check `v$options` for this setting.

Table 3–5 Fixed Initialization Parameter Values

Parameter	Value
job_queue_processes	10
db_block_size	8192

Table 3–5 (Cont.) Fixed Initialization Parameter Values

Parameter	Value
timed_statistics	TRUE
open_cursors	300
session_cached_cursors	200
aq_tm_processes[1]	1
compatible	<currently installed Oracle Database release> (default)
undo_management	AUTO
undo_retention	10800
undo_tablespace	<any acceptable name>
processes	150
log_buffer	1048576
statistics_level	TYPICAL (Note that this value is specific only to Enterprise Manager 10*g* Repository Database release and later.)
TEMP space (Tablespace)[2]	50 MB (extending to 100 MB)
_b_tree_bitmap_plans	false (hidden parameter)

[1] Setting the aq_tm_processes parameter is not a prerequisite if you are using a 10.*n* Oracle Database.

[2] The TEMP space is an initialization parameter only when you are performing an Enterprise Manager installation using a new database.

Variable Initialization Parameter Values

The variable parameter setting values are based on the size of the Enterprise Manager Grid Control environment. For the sake of clarity, the environment has been categorized as Small, Medium, and Large based on the number of targets in the environment, where:

- Small = Approximately 100 monitored targets
- Medium = Approximately 1000 monitored targets
- Large = 10000 or more monitored targets

Table 3–6 lists the variable parameter setting values.

Table 3–6 Variable Initialization parameter Values

Size	pga_ aggregate_ target	Redo logs[1]	db_cache_size (for 9*1* rep. DB)	shared_pool_ size (for 9*1* rep. DB)	sga_target (for 10*g* rep. DB)[2]
Small	256 MB	100 MB	384 MB (or more)	128 MB	512 MB (or more)
Medium	384 MB	512 MB	1024 MB (or more)	384 MB	1408 MB (or more)
Large	512 MB	1024 MB	2048 MB (or more)	512 MB	2560 MB (or more)

[1] One redo log group with four members each of the listed size

[2] This new setting replaces settings for db_cache_size and shared_pool_size from Oracle9*i*.

3.3.2.1.2 NLS_LANG Environment Variable

If your operating system is Linux, ensure the `NLS_LANG` environment variable is set with a value that is compatible with the operating system default locale setting and the Management Repository database character set. For information on the specific values for language, territory, or character set, refer to the Globalization Support Guide of the Oracle product that you are using.

A Typical Installation Scenario

If you choose to install Enterprise Manager using an existing database, you must provide the location of an existing database where the installer will create the repository. Here again, the database should be of release 9.2.0.6 and later, or 10.1.0.4 and later. If you have an earlier database release installed, you must first upgrade this database instance to the specified minimum release (9.2.0.6 and later, or 10.1.0.4 and later) and then proceed with the Enterprise Manager installation.

3.3.2.2 To Install Enterprise Manager Using Existing Database

Complete the following steps to install Enterprise Manager using an existing database:

1. Start Oracle Universal Installer by running the `runInstaller` script in Linux (`<DVD>/runInstaller`) from the top directory of the DVD.
2. In the Specify Installation Type screen, select the second option (**Enterprise Manager 10g Grid Control Using an Existing Database**). Click **Next**.

Figure 3–14 Specify Installation Type

3. The Specify Installation Location screen appears.
   a. Specify the full path to the parent directory (base directory), for example, `/scratch/OracleHomes`. All the Oracle homes created during the installation are placed as subdirectories under this parent directory. For example: `oms10g`, and `agent10g`.

Caution: Do not use symbolic links to specify the Oracle home path.

The installer by default installs the selected products in the English language.

b. If you want to install the product in a different language, click **Product Languages**.

The Language Selection screen appears. Make the required language selections here, and click **Next**. See Figure 3–3, "Language Selection" for details.

4. Click **Next**. The Specify Inventory Directory and Credentials screen appears if Enterprise Manager is the first Oracle product that you are installing on the machine. See Figure 3–4, "Specify Inventory Directory and Credentials" for details.

5. Click **Next.** The Product Specific Prerequisites Check screen appears.

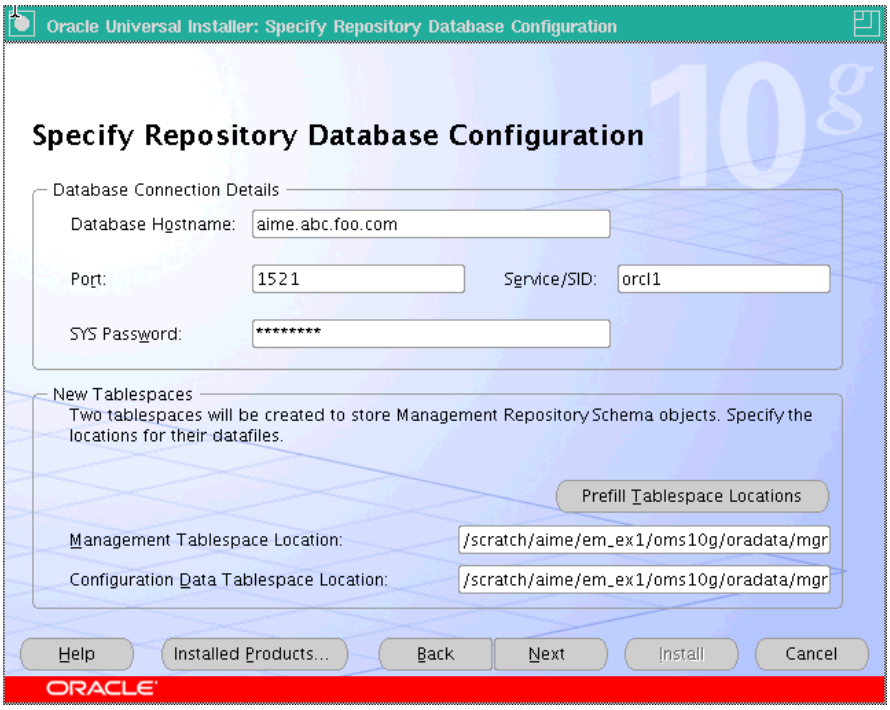
This screen displays the name, type, and status for all prerequisite checks designed for the installation. Automatic checks are run first, followed by optional and manual checks.

Depending on the status of the automatic checks, you must verify all warning and manual checks. At some point, if you have stopped the prerequisite check and want to rerun these checks, select the checks that you want to rerun and click **Retry**. As each check runs, a progress bar is shown, and test details (expected results, actual results, error messages, instructions) are displayed in the details section at the bottom of the screen. See Figure 3–5, "Product-Specific Prerequisite Checks" for details.

Note: You can also run these prerequisite checks in standalone mode, prior to starting the `runInstaller`. See Section 1.5, "Running the Prerequisite Check in Standalone Mode" for more information.

6. Click **Next**. The Specify Repository Database Configuration screen appears.

Figure 3–15 Specify Repository Database Configuration



Specify the connection details for the existing database in which the Management Repository should be created. The Management Repository database can be created on the following database releases:

- Oracle Database 10*g* Release 1 (10.1.0.4 and later), Enterprise Edition

  Note: If you are performing an Enterprise Manager Grid control installation using an existing database, ensure the database is of a 10.1.0.3 release or later.

- Oracle Real Application Clusters 10*g* Release 1 (10.1.0.4 and later)

  Note: If you are performing an Enterprise Manager Grid control installation using an existing database, ensure the existing Oracle RAC database is of a 10.1.0.3 release or later.

- Oracle9*i* Release 2 (9.2.0.6 and later), Enterprise Edition
- Oracle9*i* Real Application Clusters Release 2 (9.2.0.6 and later)

a. In the Database Connection Details section, specify a fully qualified host name, listener Port number, SID (system identifier) for the database instance, and the SYS password.

The SID identifies a specific Oracle Database and distinguishes it from other databases on the computer.

Note: When selecting an existing cluster database for creating the Management Repository, you can either specify the SID value, or use the Management Service name.

b. Enter the password for the SYS user. This account is used to create the SYSMAN user, which is the primary owner of the Management Repository schema.

c. In the Additional Tablespace section, specify the location for the following:

- *Management Tablespace Location:* The MGMT_TABLESPACE tablespace holds data for the Management Repository.
- *Configuration Data Tablespace Location:* The MGMT_ECM_DEPOT_TS tablespace holds Configuration Management data for the Management Repository.

Caution: If the existing database that you have selected to create the repository already contains a SYSMAN schema, the installer will display an error similar to the following:

"The Grid Control schema already exists in the database that you have provided."

You can choose to manually drop this schema before proceeding with the repository creation.

You can also click **Continue.** The installer will then automatically drop the existing schema and create a new SYSMAN schema.

For ASM (Automatic Storage Management) devices, the tablespace locations should be specified relative to the ASM disk group. For example: `+<ASM Disk>/emrep/tablespace.dbf`

For tuning/performance reasons, Oracle recommends placing Binary large objects (BLOBs) in their own tablespace. Because Enterprise Configuration Management data support BLOBs, the Management Repository requires two tablespaces: `MGMT_TABLESPACE` and `MGMT_ECM_DEPOT_TS`.

Specify the full path of the file locations for the previously mentioned tablespaces. The directories you specify for these tablespaces must already exist for repository creation to succeed. For raw devices, you must partition your disk before specifying its location. Note that raw device path names vary across volume managers. Ensure to use the right path format for your raw device locations.

If you do not have the complete path for the tablespaces, click **Prefill Tablespace Location**. Note that the Prefill Tablespace button will be enabled only after you have specified all the Database Connection details. The installer then queries the database you have specified. Look for the SYSAUX tablespace location, and prefill that path in the appropriate box.

Note:

- The two tablespaces initially require 120 MB of disk space, with `MGMT_TABLESPACE` requiring 20 MB and `MGMT_ECM_DEPOT_TS` requiring about 100 MB. Ensure there is enough disk space available.
- If you are selecting an existing cluster database for the new Management Repository, the management tablespace file locations must be on a shared device that is accessible to all instances that provide the database service.

Caution: If the `DBMS_SHARED_POOL` package has not been installed at the time of the database creation, Oracle Universal Installer displays an error message and prompts you to execute this package before proceeding with the installation.

To check whether or not the `DBMS_SHARED_POOL` package has been installed, login to the database and execute the following query:

```
Select count(*) from dba_objects where OWNER = 'SYS'
AND object_name = 'DBMS_SHARED_POOL'
AND object_type IN ( 'PACKAGE','PACKAGE BODY') ;
```

This query should return a count of **2.**

To install the `DBMS_SHARED_POOL` package, execute the following script:

```
<DB_HOME>/rdbms/admin/dbmspool.sql
```

7. Click **Next**. The Specify Optional Configuration screen appears.

   As the name suggests, all the fields on this screen are optional, and are disabled, by default. Select the required check box to enable the corresponding fields.

   a. In the Configure Email Notification section, specify an appropriate e-mail address, and the corresponding SMTP server name in this section. You will receive information on important developments and events in Grid Control, including critical alerts, at this e-mail address.

      The e-mail address that you specify should be associated with the SYSMAN user to receive notifications.

      The SMTP server is the name of the mail server (for example `mail.acme.com`). For Linux, the SMTP server must be the local host name. Use the fully qualified host name (including domain).

      Note: If you do not provide the e-mail notification information, this feature is not enabled upon installation. You may also choose to configure these settings through the Enterprise Manager console by clicking **Notification Methods** under Setup. Refer to the Enterprise Manager online Help for more information.

   b. Specify the Oracle*MetaLink* credentials if you are going to use a proxy server to access Oracle*MetaLink*.

If you prefer, you may also enter this information through the Enterprise Manager console after installation by clicking **Patching Setup**, under Setup.

Note: Enterprise Manager uses the Oracle*MetaLink* credentials to search for and download patches from
`http://oracle.com/support/metalink/index.html`

---

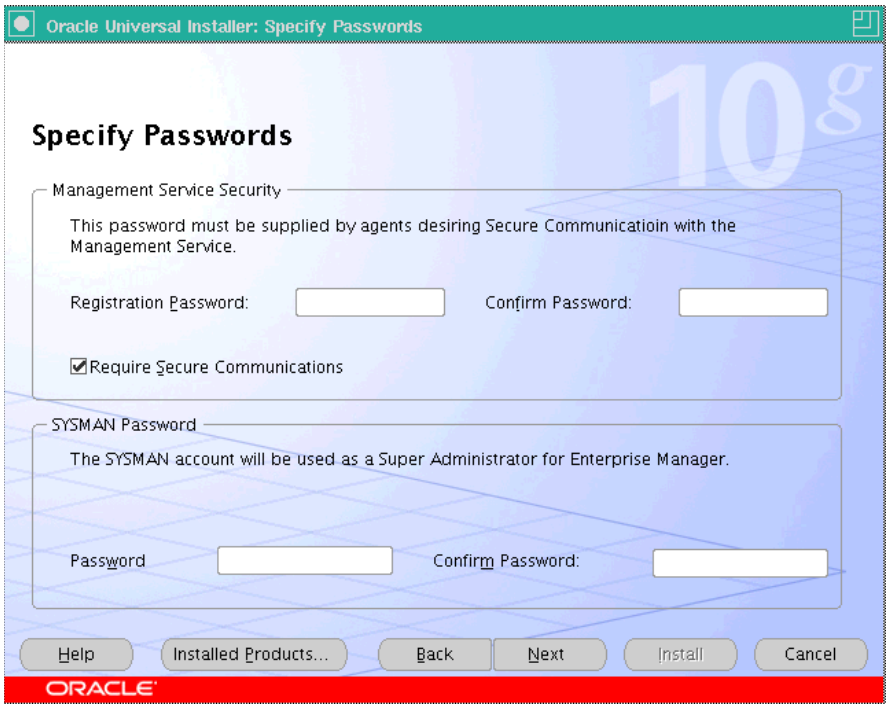
c. Specify the Proxy Information if Enterprise Manager is using a proxy server for external access. See Table 3–2, " Specify Proxy information - Input Fields" for a description on each of the input fields in this section.

Note: If the proxy server requires user authentication before providing access, you must specify these credentials here, or through the Patching Setup screen under Setup in the Grid Control console.

---

8. Click **Next**. The Specify Passwords screen appears.

Figure 3–16 Specify Passwords



a. Specify the Management Service Security, and Repository Database passwords that are used to secure your entire Grid Control environment.

b. Select **Require Secure Communications** if you want the secure OMS to communicate only with Secure Agents. This is optional, though recommended.

For example, if you have 10*g* R1 (10.1.*n*) agents in the Grid environment and you have secured and locked the Oracle Management Service (OMS), and selected the Require Secure Communications option, then all communication

between the 10*g* R2 (10.2) OMS and 10.1 agents fails (because these agents have not been secured).

To secure an agent, execute the following command from the agent Oracle home of that particular target:

```
emctl secure agent
```

See the section on Password Restrictions and Recommendations in this chapter for more information.

9. Click **Next**. The Summary screen appears.

   This screen provides a summary of the options that you have selected during the installation process. Depending on the installation type, this screen also provides any or all of the following details:

   - Global Settings
   - Product Languages
   - Space Requirements
   - New Installations
   - Installed Products

   Verify the choices that you have made and click **Install** to start the installation. The Install screen that appears displays the installation progress bar.

   The installer seamlessly installs all Grid Control components based on the installation type you selected.

10. During the installation, you are prompted to execute certain configuration scripts. These scripts and their locations are listed in the Execute Configuration Scripts dialog box that is displayed (only on UNIX). Refer to Figure 3–12, "Execute Configuration Scripts".

    a. To execute these scripts, go to the computer window, log in as `root`, and run these configuration scripts.

    b. Return to the Execute Configuration Scripts dialog box after executing the scripts, and click **OK** to continue the installation.

11. The Configuration Assistants screen appears. At this point, the installer starts running the recommended Configuration Assistants.

    Note: The OMS Configuration Assistant will create the repository. The repository creation log (`emca_repos_create<TimeStamp>.log For example, emca_repos_create05_13_33.log`) is available at the following directory:

    ```
    OMS_HOME/sysman/log/
    ```

    This screen displays the name, status, and the type of each configuration tool that Oracle recommends to be run before completing the installation. Refer to Table 3–4, " Enterprise Manager Configuration Tools" to see the list of configuration tools that are run. In case of failure of any configuration assistant, refer to the logs and re-rerun the configuration assistants as described in Section A.2.1, "Configuration Assistants Fail During Enterprise Manager Installation".

12. After successfully running all the recommended configuration tools, the End of Installation screen appears.

    This screen tells you whether or not the installation was successful, and displays some important information that you *must remember* about the products you have installed. For example, it might contain information about the URLs for particular Web applications.

3.3.2.2.1 Configuration Assistant

During the installation process, if the `SYSMAN` schema already exists in the database that you specify for the Management Repository, the installer will prompt you to manually drop the schema. If this is not done, the installer will automatically drop the schema before proceeding to the next configuration assistant.

If the Oracle Management Service Configuration Assistant fails before completion, you can click **Retry**, which automatically cleans up the repository when the configuration tool is rerun. To manually clean up the repository, use the following command:

```
OMS_HOME/sysman/admin/emdrep/bin/RepManager <Host name> <Port>
<SID> -ACTION Drop
```

You may need to set the `LD_LIBRARY_PATH` to the Management Service's `ORACLE_HOME/lib` directory before running the script.

Refer to *Oracle Enterprise Manager Advanced Configuration* for further instructions on how to drop the existing repository from the database.

> **Note:** The listener that is associated with the specified database must be running. Otherwise, Management Repository creation may fail.

3.3.3 Installing an Additional Management Service

Select this option if you need to add an additional Management Service to your environment. Note that setting credentials for Oracle*MetaLink* is not necessary for this installation type, as the Management Repository is not affected.

3.3.3.1 Prerequisites

Ensure the following prerequisites are met before starting the installation:

- Ensure the installation is not run by the `root` user.
- Ensure the user has Administrator permissions and is part of the DBA group.
- Ensure the hard disk and physical memory requirements are met. See Table 3–1, " Enterprise Manager Installation Options" for more information.
- Besides the database release, ensure the repository release is 10.2.0.1.0 (or 10.2.0.2 for Microsoft Windows).
- The name of the host on which the installation is being performed should neither be `localhost.localdomain` nor an IP address. It must be a valid host name. At the time of invoking the installer, you can pass `ORACLE_HOSTNAME` as an argument.

Caution: Do not pass the argument as `ORACLE_HOSTNAME=<localhost.localdomain>` or `ORACLE_HOSTNAME=<IP address>`. You must pass the argument as **`ORACLE_HOSTNAME=<valid host name>`**.

See Also: Refer to the Reconfiguring the Management Agent and Management Service chapter of the Oracle Enterprise Advanced Configuration Guide for more information on controlling the Management Service.

See Appendix G, "Assigning Custom Ports" for more information on assigning port numbers for Enterprise Manager components.

3.3.3.2 To Install an Additional Management Service

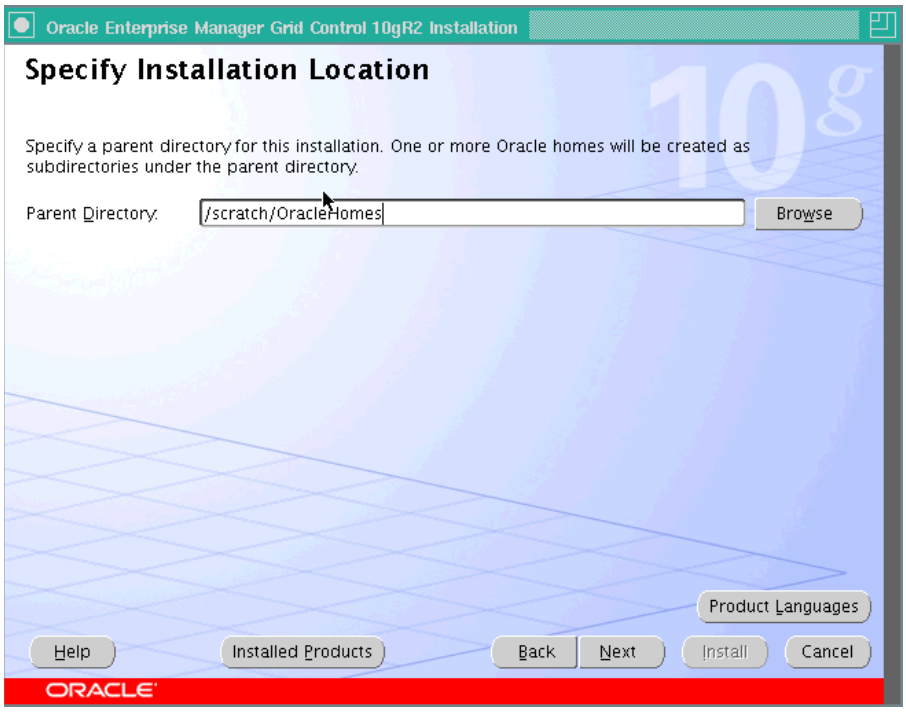
Complete the following steps to install an additional Management Service:

1. Start Oracle Universal Installer by running the `runInstaller` script (`<DVD>/runInstaller` on Linux and `/DVD/setup.exe` on Microsoft Windows) from the top directory of the DVD.
2. In the Specify Installation Type screen, select the third option (**Additional Management Service**).

Figure 3–17 Specify Installation Type

3. In the Specify Installation Location screen, specify the full path to the parent directory (base directory), for example, `/scratch/OracleHomes`. The Oracle Management Service (OMS) home created during the installation is placed as a sub-directory under this parent directory. For example: `oms10g`.

Figure 3–18 Specify Installation Location



Note: Ensure you do not use symbolic links to specify the Oracle home path.

The installer by default installs the selected products in the English language.

a. If you want to install the product in a different language, click **Product Languages**.

b. The Language Selection screen is displayed. Make the required language selections here. See Figure 3–3, "Language Selection" for details.

4. Click **Next**. The Product Specific Prerequisites Check screen appears.

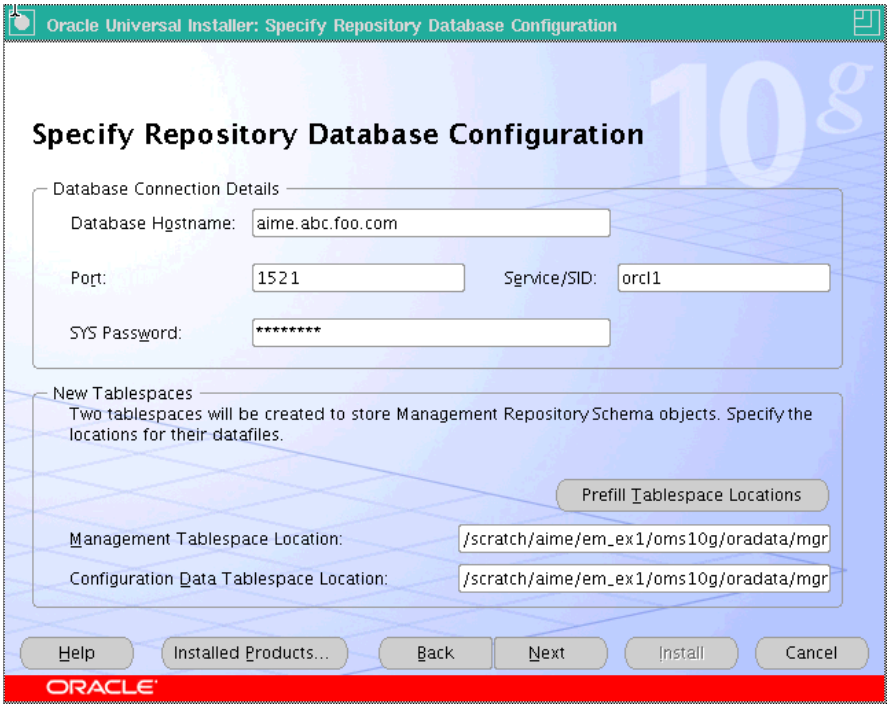
This screen displays the name, type, and status for all prerequisite checks designed for the installation. Automatic checks are run first, followed by optional and manual checks.

Depending on the status of the automatic checks, you must verify all warning and manual checks. At some point, if you have stopped the prerequisite check and want to rerun these checks, select the checks that you want to rerun and click **Retry**. As each check runs, a progress bar is shown, and test details (expected results, actual results, error messages, instructions) are displayed in the details section at the bottom of the screen. See Figure 3–5, "Product-Specific Prerequisite Checks" for more information.

Note: You can also run these prerequisite checks in standalone mode, prior to starting the `runInstaller`. For more information on running these prerequisite checks in standalone mode, see Section 1.5, "Running the Prerequisite Check in Standalone Mode" for more information.

5. Click **Next**. The Specify Repository Database Configuration screen appears.

Figure 3–19 Specify Repository Database Configuration



a. You must configure the additional Management Service to establish the connections with the existing Management Repository.

Note: The existing Management Repository database must be one of the following releases:

- Oracle Database 10*g* Release 1 (10.1.0.4), Enterprise Edition
- Oracle Real Application Clusters 10*g* Release 1 (10.1.0.4)
- Oracle9*i* Database Release 2 (9.2.0.6 and later), Enterprise Edition
- Oracle9*i* Real Application Clusters Release 2 (9.2.0.6 and later)

The Management Repository database may also require patches to be applied, prior to successful installation. See Section 1.4.2, "Enterprise Manager Platform and Target Certification Requirements" for more information.

---

b. In the Repository Database Connection Details section, specify a fully qualified host name on which the Management Repository database is installed, the repository port, and the SID (system identifier) for the database instance.

The SID identifies a specific Oracle database and distinguishes it from other databases on the computer.

Note: When selecting an existing cluster database for creating a Management Repository, you must replace the SID value with the Management Service name.

---

c. Enter the password for the SYSMAN user (the default Super Administrator account for Enterprise Manager).

d. In the Management Service Security section, specify the password used to secure and lock the Oracle Management Service (OMS).

e. Select **Require Secure Communications for all agents** if you want the secure OMS to communicate only with Secure Agents. This is optional, though recommended.

   For example, if you have 10*g* R1 (10.1.n) agents in the Grid environment, and you have secured the OMS and selected the **Require Secure Communications** option, then all communication between the Oracle Management Service 10*g* R2 (10.2) and Oracle Management Agent 10*g* R1 (10.1) fails (because these agents have not been secured).

   To secure an agent, execute the following command from the agent Oracle home of that particular target:

```
emctl secure agent
```

   See the section Password Restrictions and Recommendations in this chapter for more information.

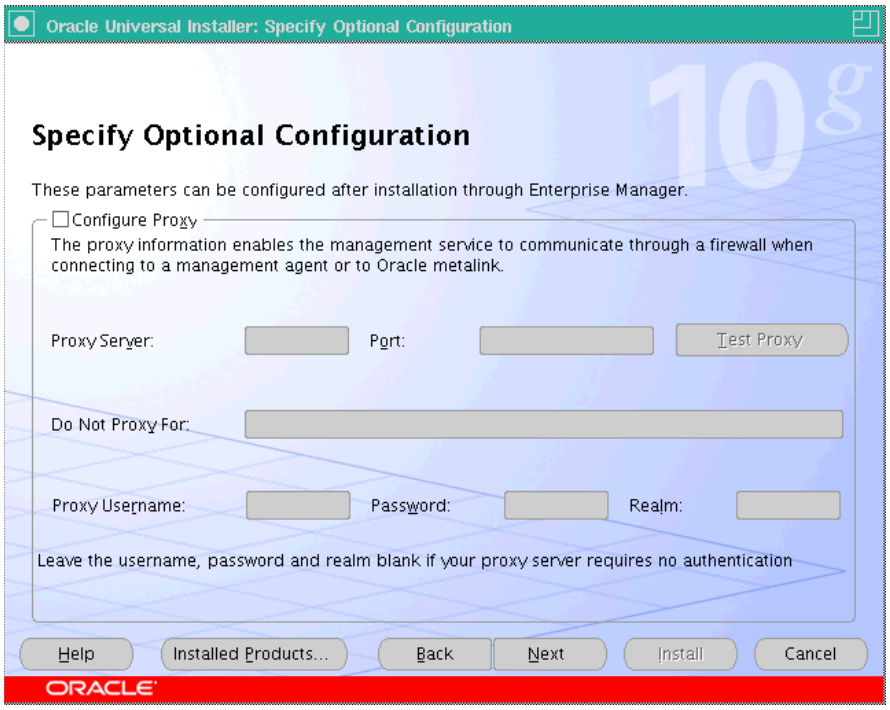
Note: The password that you specify here must be the same as the password that you specified to secure the Management Service.

Ensure that all Management Service instances using the same repository must use the same secure password.

---

6. Click **Next**. The Specify Optional Configuration screen appears.

Figure 3–20 Specify Optional Configuration



As the name suggests, all the fields on this screen are optional, and are disabled, by default. Select the required check box to enable the corresponding fields.

a. Select the Configure Proxy check box (optional) if Enterprise Manager is using a proxy server for external access. Specify the properties for the proxy server host name (enter a fully qualified host name), port number, Do Not Proxy for list, and the Proxy user credentials. See Table 3–2, " Specify Proxy information - Input Fields" for a description of the input fields.

b. Specify an appropriate **Realm** value. This becomes a mandatory field only if the proxy server credentials have been configured using a Realm, in which case, you must specify an appropriate Realm value.

A Realm is a string value that is assigned by the proxy server to indicate the secure space that requires authentication.

7. Click **Next**. The Summary screen appears.

This screen displays a summary of the options that you have selected during the installation process. Depending on the installation type, this screen displays any or all of the following details:

- Global Settings
- Product Languages
- Space Requirements
- New Installations

For more information on each of the previously listed details, see the Enterprise Manager online Help.

Verify the choices that you have made and click **Install** to start the installation. The installer begins installing the selected Oracle product.

8. During the installation, you are prompted to execute certain configuration scripts. These scripts and their locations are listed in the Execute Configuration Scripts dialog box that is displayed (only for Linux). Refer to Figure 3–12, "Execute Configuration Scripts".

   a. To execute these scripts, go to the computer window, log in as `root` and run these configuration scripts.

   b. Return to the Execute Configuration Scripts dialog box after executing the scripts, and click **OK** to continue the installation.

9. The Configuration Assistants screen appears. At this point, the installer starts running the recommended configuration tools.

   This screen displays the name, status, and the type of each configuration tool that Oracle recommends to be run before completing the installation. Refer to Table 3–4, " Enterprise Manager Configuration Tools" to see the list of configuration tools that are run. In case of failure of any configuration assistant, refer to the logs and re-rerun the configuration assistants as described in Section A.2.1, "Configuration Assistants Fail During Enterprise Manager Installation".

10. After successfully running all the recommended configuration tools, click **Next**. The **End of Installation** screen appears.

    This screen tells you whether or not the installation was successful and displays some important information that you must remember about the product you have installed. For example, it might contain information about the URLs for particular Web applications.

3.3.4 Installing a Management Agent

Select this option to install the Management Agent in an Oracle home directory on a specified host target. Each host you wish to monitor must have a Management Agent installed.

You can install the Management Agent in the following ways:

- On each host computer, run Oracle Universal Installer from the Enterprise Manager DVD-ROM and select the Additional Management Agent installation type. This method installs one Management Agent at a time in interactive GUI mode. You may also perform silent installations using a response file.
- Use the Agent Deploy application to perform a new agent installation (standalone or cluster agent) or a shared agent installation.
- Use the `nfsagentinstall` script to install and deploy the shared Management Agent.
- Use the `agentDownload` script to install and deploy Management Agents to many managed hosts through HTTP or over the network.

> **See Also:** Chapter 6, "Deploying the Management Agent" for a full and detailed explanation on installing Management Agents using the `agentDownload` script and the `nfsagentinstall` script.
>
> See Appendix G, "Assigning Custom Ports" for information on assigning custom port numbers for Enterprise Manager components.

Caution: If you install the Management Agent on a system where you have already installed an Oracle Application Server instance, you must install the Management Agent from a user account that belongs to the same OS Group group that was used to install the Application Server. Otherwise, you cannot monitor the application server metrics.

- To see which group was used to install the Application Server, type `ls -l` on the command line in the directory containing `opmn.xml: <AS_ORACLE_HOME>/opmn/conf`.
- To see the groups to which you belong, type `groups` on the command line. You may be a member of several groups. Note that it is not sufficient to be a member of the group used to install the Application Server; that group must be your current group.
- To see which user/group you are currently using, type `id` on the command line. Use the `newgrp` command to change to the group used to install the Application Server. Oracle recommends installing all software using a single group.

3.3.4.1 Prerequisites

- Ensure the Management Agent Oracle home must not contain any other Oracle software installation.
- The name of the host on which the installation is being performed should neither be `localhost.localdomain` nor an IP address. It must be a valid host name. At the time of invoking the installer, you can pass `ORACLE_HOSTNAME` as an argument.

Caution: Do not pass the argument as `ORACLE_HOSTNAME=<localhost.localdomain>` or `ORACLE_HOSTNAME=<IP address>`. You must pass the argument as **`ORACLE_HOSTNAME=<valid host name>`**.

Note: Enterprise Manager does not support uploading of data to the same Management Repository from two Management Agents running on the same host.

3.3.4.2 To Install an Additional Management Agent Using OUI

1. Start the Oracle Universal Installer by running the `runInstaller` script in Linux (`<DVD>/runInstaller`) from the top directory of the DVD.
2. In the Specify Installation Type screen, select the fourth option (**Additional Management Agent**), and specify the parent directory path and installation name.

Figure 3–21 Specify Installation Type

3. In the Specify Installation Location screen, specify the full path to the parent directory (base directory), for example, `/scratch/OracleHomes`. The agent home created during the installation is placed as a sub-directory under this parent directory. For example: `agent10g`.

   Note: Ensure you do not use symbolic links to the Oracle home path.

   The installer by default installs the selected products in the English language.

   a. If you want to install the product in a different language, click **Product Languages**.

   b. The Language Selection screen appears. Make the required language selections here, and click **Next**. See Figure 3–3, "Language Selection" for details.

4. The Product Specific Prerequisites Checks screen appears.

   This screen displays the name, type, and status for all prerequisite checks designed for the installation. Automatic checks are run first, followed by optional and manual checks.

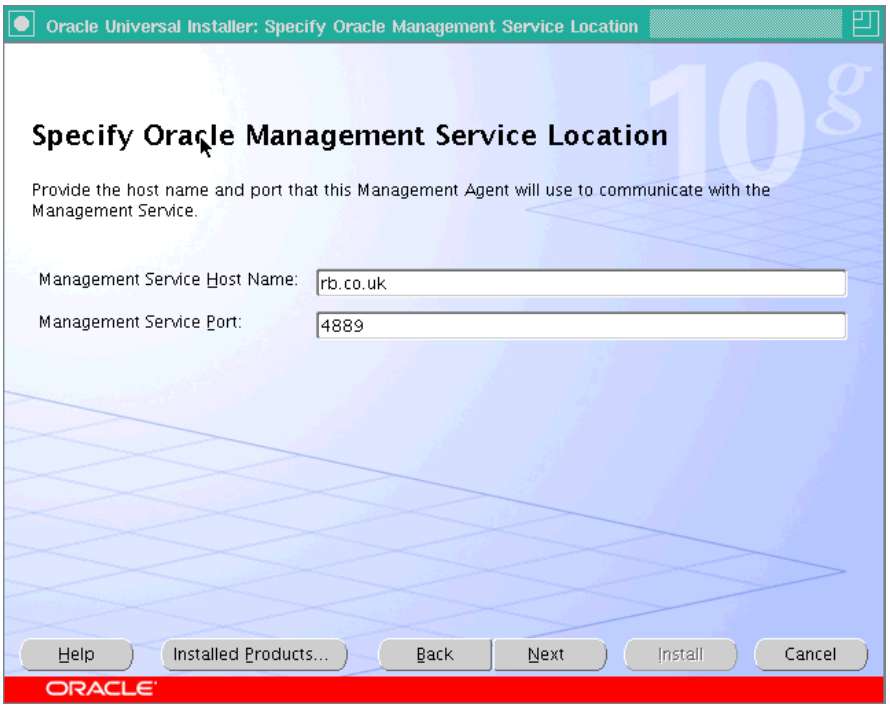
   Depending on the status of the automatic checks, you must verify all warning and manual checks. To do this, select the appropriate prerequisite status check box and click **Retry**. As each check runs, a progress bar is shown, and test details (expected results, actual results, error messages, instructions) are displayed in the details section at the bottom of the screen. See Figure 3–5, "Product-Specific Prerequisite Checks" for more information.

Note: You can also run these prerequisite checks in standalone mode, prior to starting the `runInstaller`. For more information on running these prerequisite checks in standalone mode, see Section 1.5, "Running the Prerequisite Check in Standalone Mode"for more information.

---

5. Click **Next**. The Specify Oracle Management Service Location screen appears.

Figure 3–22 Specify Oracle Management Service Location



a. Specify the Management Service host name. For example: `dlsun1444.acme.com`. Use the fully qualified host name (including domain).

Caution: When specifying the host name, ensure you do not include the protocol (that is, `http://` or `https://`).

---

b. Enter the port number for the Management Service. The default port is 4889 and the default secure port number is 1159.

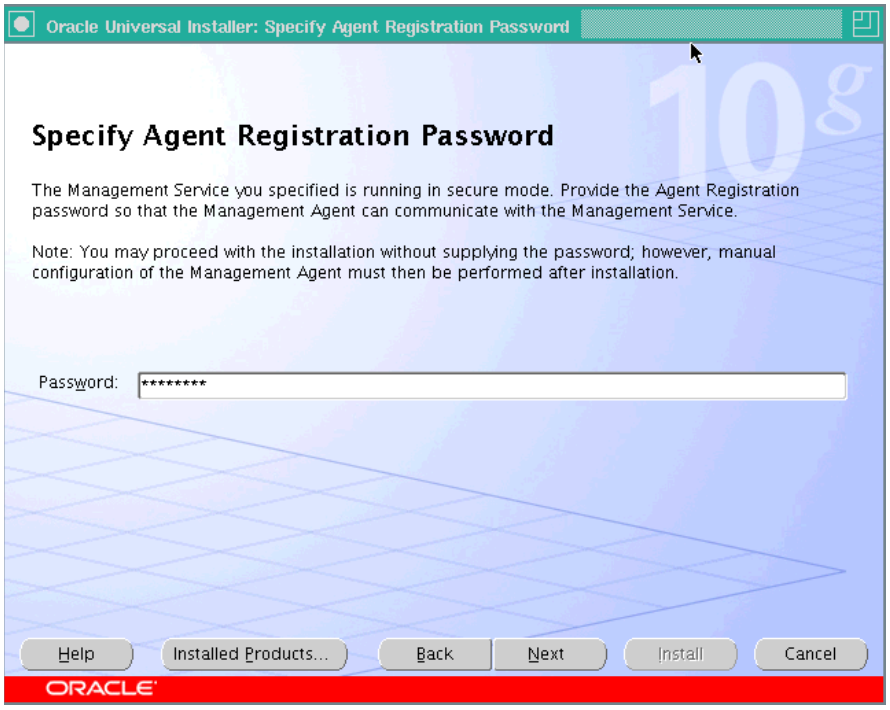
However, even if you are specifying a secure and locked Management Service, you must still enter the nonsecure port number (4889) here. You must connect over HTTP to receive the certificate before you can connect over HTTPS.

Note: If your Management Service has been secured and locked, you are prompted to enter the Agent Registration password (used to secure the Management Service environment). If you do not know the password, obtain it from the user who configured the Management Service for SSL.

---

6. Click **Next**. If the Management Service is found to be running in a secure mode, the Specify Agent Registration Password screen appears. You must provide the correct password to enable communications between the new Management Agent and the Secure Sockets Layer (SSL)-enabled Management Service.

Figure 3–23 Specify Agent Registration Password



Note: If you do not know the password and choose to leave the Password field blank, you must do the following after installation to enable communication between the Management Agent and secure OMS:

- Find out the correct password for the secure and locked OMS environment. If you do not know the password, obtain it from the user who configured the Management Service for SSL.
- In the `<AGENT_HOME>/bin` directory, execute any of the following commands:

  ```
  emctl secure agent -reg_passwd <password>
  ```

  The variable <passwd> should be replaced with the Agent Registration password.

  ```
  emctl secure agent
  ```

  When you execute this command, you will be prompted to specify the Agent Registration password.

7. Click **Next**. The Summary screen appears.

   This screen displays a summary of the options that you have selected during the installation process. Depending on the installation type, this screen displays any or all of the following details:

   - Global Settings
   - Product Languages
   - Space Requirements
   - New Installations

   For more information on each of the previously listed details, see the Enterprise Manager online Help.

   Verify the choices that you have made and click **Install** to start the installation. The installer starts installing the selected Oracle product.

8. During the installation, you are prompted to execute certain configuration scripts. These scripts and their locations are listed in the Execute Configuration Scripts dialog box that is displayed (only for Linux). Figure 3–12, "Execute Configuration Scripts" provides details on this screen.

   a. To execute these scripts, go to the computer window, log in as `root`, and run these configuration scripts.

   b. Return to the Execute Configuration Scripts dialog box after executing the scripts, and click **OK** to continue the installation.

9. The Configuration Assistants screen appears. At this point, the installer starts running the recommended configuration tools.

   This screen displays the name, status, and the type of each configuration tool that Oracle recommends to be run before completing the installation. Refer to Table 3–4 to see the list of configuration tools that are run. In case of failure of any configuration assistant, refer to the logs and re-rerun the configuration assistants as described in Section A.2.1, "Configuration Assistants Fail During Enterprise Manager Installation".

See Section 3.4, "Executing the runConfig Tool from the Command Line" for information on executing the runConfig tool.

10. After successfully running all the recommended configuration tools, click **Next**. The End of Installation screen appears.

    This screen displays some important information about the products you have installed. This information is also available in the `<AGENT_HOME>/sysman/setupinfo.txt` file.

    For example, it might contain information about the URLs for particular Web applications.

3.4 Executing the runConfig Tool from the Command Line

This command-line tool is typically used to run any of the failed configuration tools of your product(s) under an Oracle home.

The usage to execute the runConfig tool is:

```
./runConfig.sh OPTION1=value1 OPTION2=value2 ...
```

The options, OPTION1, OPTION2, and so on, can be the options discussed in the following section.

Note: On Microsoft Windows, replace `runConfig.sh` with `runConfig.bat` or just `runConfig` (without the file extension).

3.4.1 Options You Can Specify to Execute runConfig

You can specify the following options to execute the `runConfig` tool.

3.4.1.1 ORACLE_HOME

This is the absolute location of the Oracle home. All products/top-level components under this Oracle home that have been installed using the Oracle Universal Installer (OUI) 10*g* R 2 (10.2) are eligible for the **ACTION.** Products installed using an OUI that is earlier to 10.2 are not eligible for this ACTION.

3.4.1.2 ACTION

This is a mandatory option. This option can have values such as **`configure`**/**`clone`** / **`addnode`**/**`addlanguage`**/**`deconfigure`**/**`patchsetConfigure`**.

3.4.1.3 MODE

This is optional, and can have values such as **`perform`**/**`showStatus`**/**`listTools`**. For example, if the value is **`perform`**, then that ACTION is performed.

If **MODE** is absent, the MODE option will assume a default value of **`listTools`**.

If the value is **`showStatus`**, the status of the last-performed ACTION is displayed to the user.

Examples

```
Tool1 - Optional    - Failed
Tool2 - Recommended - Succeeded
Tool3 - Optional    - Succeeded
```

If the value of MODE option is **`listTools`**, a list of recommended/optional/other tools for the specified ACTION are displayed.

Example

```
Recommended Tools(1): Tool2
Optional Tools (2): Tool1, Tool3
Other Tools(0):
```

3.4.1.4 COMPONENT_XML

This is optional. You can specify a comma-separated list of Aggregate XML names from the OH/inventory/ContentsXML/ConfigXML/ and only these XMLs and the items dependent on them will be configured. If there are two components with the same name in the ORACLE_HOME, the one that is of a later version is considered for the ACTION option.

3.4.1.5 RESPONSE_FILE

This is optional. This is the absolute location of the response file that is used to overwrite some existing parameters. Pairs such as `ComponentID|variable = value` are to be specified in this file, per line, per variable as:

```
oracle.assistants.server|var1=true
oracle.network.client|var2=orcl
```

Example

```
RESPONSE_FILE=/scratch/rspfile.properties
```

Note: Secure variables are not stored in the instance aggregate XML files and hence while running runConfig, if any of the configuration tools that you want to run use secure variables, such as passwords, you must supply the value of these secure variables using the RESPONSE_FILE option of runConfig. Otherwise, the tools with secure variables as arguments fail.

3.4.1.6 INV_PTR_LOC

This is optional. This is the full path of `oraInst.loc` file.

The `orainst.loc` file contains `inventory_loc=<location of central inventory>`

inst_group=<>

Example

```
INV_PTR_LOC=<absolute path of oraInst.loc>
```

3.4.1.7 RERUN

This is **optional.** Possible values are **true** and **false**. RERUN has a default value of `false`. This means that only failed tools or those tools that were skipped are executed. All those tools that were successfully executed are skipped during the rerun.

A `RERUN=true` value will execute all the tools anew, including the tools that completed successful runs.

3.4.1.8 Typical Usage of the runConfig.sh

A typical usage of the `runConfig.sh` script is as follows:

```
./runConfig.sh ORACLE_HOME=<path of database home> ACTION=configure
MODE=perform COMPONENT_XML={encap_emseed.1_0_0_0_0.xml}
```

> **Note:** On Microsoft Windows, replace `runConfig.sh` with `runConfig.bat` or just `runConfig` (without the file extension).

3.4.1.9 runConfig Log Files

The log files for `runConfig configActions<timestamp>.log/.err` are generated under `ORACLE_HOME/cfgtoollogs/oui/`.

3.4.2 Executing the configToolFailedCommands Script (UNIX Only)

During the installation, if any of the configuration assistants fails to run successfully, a `configToolFailedCommands` script is created in the respective Oracle home directories. If you want to rerun the failed configuration tools, you can either execute the `runConfig` tool, or navigate to the `configToolFailedCommands` script under the corresponding Oracle home location, and execute this script.

A typical usage of the configToolFailed Commands scripts is as follows:

```
./configToolFailedCommands
```

3.5 Deinstallation of Enterprise Manager Grid Control

If you deinstall the Enterprise Manager 10*g* Oracle homes using Oracle Universal Installer, the Oracle homes are de-registered from the central inventory and the `oratab` file. However, some files may remain in these Oracle homes.

If an Oracle home has been successfully removed (verify this in OUI by clicking **Installed Products**), you can manually delete the files through the operating system.

The proper deinstallation sequence is the following:

1. Shut down all `opmn` processes that are running by executing the following command:

   ```
   <OMS_HOME>/opmn/bin/opmn stopall
   ```

2. Shut down the Management Agent in the Agent Oracle home using the `emctl stop agent` command.
3. Stop Enterprise Manager by executing the following command:

   ```
   <OMS_HOME>/bin/emctl stop em
   ```

4. Shut down the repository database (if the database software is installed as a part of the Management Service Oracle home being uninstalled).
5. Shut down the Oracle Database listener.
6. Run the Database Configuration Assistant (DBCA) to delete the database before proceeding to deinstall the Oracle home.
7. Run the Oracle Universal Installer and select the Oracle home to deinstall. It is removed from the Central Inventory.

Caution: After deinstallation of certain Grid Control targets, when you try and remove the same targets from the Grid Control console, you may encounter an error.

To resolve this issue, deinstall the Grid Control targets and wait for at least 15 minutes before you attempt to remove the targets from the Grid Control console using the Hosts screen.

3.5.1 Additional Deinstallation Steps for Windows Operating Systems

For Windows operating system, you will need to perform the following manual steps to remove entries from the registry. Ensure that you are logged in as a user with Administrator privileges on that computer.

3.5.1.1 Remove Entries in Windows Registry

1. Start the registry editor. Choose **Start > Run > regedit**.
2. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\
3. Go to HKEY_LOCAL_MACHINE\SOFTWARE\ODBC and expand all subkeys and remove the key "Oracle in <HOME_NAME>". Check if the "Oracle ODBC Driver" key contents refer to the ORACLE_HOME to be deleted. If yes, delete the key.
4. Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services. Delete the keys that begin with Oracle.
5. Go to HKEY_LOCAL_MACHINE\SYSTEM\ControlSet2\Services. Delete the keys that begin with Oracle.
6. Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\...\Application. Delete the keys whose names begin with Oracle and contain references to the EventMessageFile string entry for the ORACLE_HOME to be deleted or a location under it.
7. Go to HKEY_CLASSES_ROOT and search in the keys starting with `Ora` or `ORCL` (for example, Oracle..., ORADC... ..., OraPerf..and ORCL...). Delete keys which include string values with the specific ORACLE_HOME that is to be deleted.
8. Close the registry editor.

3.5.1.2 Clean Up Environment Settings

1. On Windows NT: Choose **Start > Settings > Control Panel > System > Environment**.

   On Windows 2000 and Windows XP: Choose **Start > Settings > Control Panel > System > Advanced > Environment Variables**.
2. In the System Variables section, click the variable PATH in order to modify the value. For example, you may see a path similar to this one:

   ```
   C:\ORACLE\EM10g\BIN
   C:\PROGRAM FILES\ORACLE\JRE\1.1.7\BIN
   ```

   If you are deleting the Oracle home `C:\ORACLE\EM10g`, remove the C:\ORACLE\EM10g\BIN expression from the PATH variable.

Delete any path expression in the PATH variable that contains the Oracle home to be removed or some location underneath.

3. If there is a CLASSPATH variable under "System Variables", delete the path expressions in the variable that contains the ORACLE_HOME to be removed or some location underneath.
4. Check if there are any other Oracle variables set in "System Variables". Delete those variables that contain the ORACLE_HOME that you are trying to remove. For example, `ORACLE_HOME, ORACLE_SID, TNS_ADMIN, inventory_loc,` and so on.
5. Click **Apply** and then click **OK**.
6. Close the Control Panel window.

3.5.1.3 Delete Software and Start Menu Icons

1. On Windows NT: Choose **Start > Programs > Windows NT Explorer**.

   On Windows 2000 and Windows XP: Choose **Start > Programs > Accessories > Windows Explorer**.
2. On Windows NT: Go to %SystemDrive%\WINNT\PROFILES\ALL USERS\START MENU\PROGRAMS

   On Windows 2000 and Windows XP: Go to %SystemDrive%\DOCUMENTS AND SETTINGS\ALL USERS\START MENU\ ...\PROGRAMS

   Note: These locations depend on whether the operating system was upgraded from NT or was a new install of Windows 2000 or Windows XP.

3. Delete the folders `-Oracle - <HOME_NAME>` where <HOME_NAME> is the Oracle home that you are trying to remove.

   Note: To locate your System Drive, type `echo %SystemDrive%` in the Command Prompt.

4. Go to the temp directory and delete all files and directories at the following locations:

   On Windows NT: `%SystemDrive%\Temp`

   On Windows 2000 and Windows XP: `%SystemDrive%\Documents and Settings\<username>\Local Settings\Temp\`
5. Reboot the machine.

4

Enterprise Manager Silent Installations

This chapter contains the following sections:

- Performing Silent Installations
- Assigning Custom Ports (Static Ports Feature)

4.1 Performing Silent Installations

Enterprise Manager supports silent installations in which you can install the Enterprise Manager Grid Control components (Management Service, additional Management Service, or Management Agent) without going through an interview phase (displaying pages or responding to questions). In silent installations, a response file provides the necessary installation information, typically answered by the user, using stored values.

> **Note:** You do not need to set the DISPLAY environment variable for silent installations using Oracle Universal Installer.

Table 4–1, " Available Response Files for Silent Installation" shows the response files made available for each installation type. The response files are available on the installation DVD-ROM at:

```
<DVD>/response
```

Executing the Response File on UNIX

Instantiate the appropriate response file and execute it as shown in the following code excerpt:

```
./runInstaller -silent -responseFile=<absolute path of the response file>
-waitforcompletion
```

Executing the Response File on Microsoft Windows

Instantiate the appropriate response file and execute it as shown in the following code excerpt:

```
./setup.exe -silent -responseFile <absolute path of the response file>
```

Table 4–1 Available Response Files for Silent Installation

Installation Option	Response File
Enterprise Manager 10*g* Grid Control Using a New Database	em_with_new_db.rsp
Enterprise Manager 10*g* Grid Control Using an Existing Database	em_using_existing_db.rsp
Additional Management Service	additional_mgmt_service.rsp
Additional Management Agent	additional_agent.rsp

See Also: Chapter 6, "Deploying the Management Agent" for more information on performing silent installations of Management Agents using the `agentDownload` script.

Silent installation on a UNIX environment can bee seen as a three-step process:

1. `noconfig`: In the first step, you must execute the `-noconfig` option. This will copy all the bits into the corresponding Oracle homes.
2. `allroot.sh`: After the bits have been copied, the installer will prompt you to run the `allroot.sh` (and `orainstRoot.sh`) or `root.sh` script (depending on the the installation type. This is required to run the configuration scripts. You must run `allroot.sh` from the first Oracle home that was created during the installation (typically the database Oracle home).
3. `runconfig.sh`: You must pass this command to execute the configuration assistants.

   For an Enterprise Manager installation using a new database, execute:

   ```
   <DB_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<database home path>
   ACTION=configure MODE=perform COMPONENT_XML={encap_emseed.1_0_0_0_0.xml}
   ```

   For an Enterprise Manager installation using an existing database, execute:

   ```
   <OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<OMS Home> MODE=perform
   ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

   For an additional Management Service installation, execute:

   ```
   <OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<OMS Home> MODE=perform
   ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

   For an additional Management Agent installation, execute:

   ```
   <AGENT_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<Agent Home> MODE=perform
   ACTION=configure
   ```

Note: If you want to use the `-noconfig` option during the silent installation, you must execute the `runconfig.sh` command at the end of the installation in order to run the configuration assistants.

Caution: When you are using the `-noconfig` option in your installation, ensure you also pass `-silent` to invoke the installer. The `-noconfig` option must be executed only during silent installations.

Executing the Response File on Microsoft Windows

On Windows, you can perform an end-to-end silent installation by executing the following command:

```
./setup.exe -silent -responseFile <absolute path of the response file>
```

See Table 4–1 for a list of available response files for silent installations.

4.1.1 Silent Installation of Enterprise Manager Using a New Database

To perform a silent installation of this type:

1. Copy the `<DVD>/response/em_with_new_db.rsp` file to a location on the local machine and modify the *Value Unspecified* entries accordingly.
2. Invoke the runInstaller (`setup.exe` on Microsoft Windows) by executing:

   ```
   <DVD>/<runInstaller or setup.exe> -silent -responseFile <location>/em_with_new_
   db.rsp
   ```

   The following message on the `root.sh` scripts is displayed (for UNIX only):

   ```
   WARNING:A new inventory has been created in this session. However, it has not
   yet been registered as the central inventory of this system.
   To register the new inventory please run the script '<User's Home
   Dir>/oraInventory/orainstRoot.sh' with root privileges.
   If you do not register the inventory, you may not be able to update or patch
   the products you installed.
   The following configuration scripts need to be executed as the root user.
   #!/bin/sh
   #Root script to run
   <User's Home Dir>/oraInventory/orainstRoot.sh
   <Install Location>/db10g/allroot.sh
   To execute the configuration scripts:
       1. Open a terminal window
       2. Log in as root
       3. Run the scripts
       4. Return to this window and click OK to continue
   ```

   Caution: If this is the first time an Oracle product is being installed on the machine, the database listener targets will not be discovered, as the `root.sh` scripts have not been executed.

3. After the installation is complete, you must execute `orainstRoot.sh` and `allroot.sh` scripts as root (UNIX only).
4. To discover the Enterprise Manager targets, you can execute `<Install Location>/agent10g/bin/agentca`, or discover the targets from the Enterprise Manager console. See Section A.2.1.4, "Invoking the Agent Configuration Assistant in Standalone Mode" for more information on executing the Agent Configuration Assistant in standalone mode.

4.1.2 Silent Installation of Enterprise Manager Using an Existing Database

To perform a silent installation of this type:

1. Copy the `<DVD>/response/em_using_existing_db.rsp` file to a location on the local machine and modify the *Value Unspecified* entries accordingly.

2. Invoke the runInstaller (`setup.exe` on Microsoft Windows) by executing:

```
<DVD>/<runInstaller or setup.exe> -silent -responseFile <location>/em_using_
existing_db.rsp
```

The following message on the `root.sh scripts` appears (for UNIX only):

```
WARNING:A new inventory has been created in this session. However, it has not
yet been registered as the central inventory of this system.
To register the new inventory please run the script '<User's Home
Dir>/oraInventory/orainstRoot.sh' with root privileges.
If you do not register the inventory, you may not be able to update or patch
the products you installed.
The following configuration scripts need to be executed as the root user.
#!/bin/sh
#Root script to run
<User's Home Dir>/oraInventory/orainstRoot.sh
<Install Location>/oms10g/allroot.sh
To execute the configuration scripts:
    1. Open a terminal window
    2. Log in as root
    3. Run the scripts
    4. Return to this window and click OK to continue
```

4.1.3 Silent Installation of an Additional Management Service

To perform a silent installation of this type:

1. Copy the `<DVD>/response/additional_mgmt_service.rsp` file to a location on the local machine and modify the *Value Unspecified* entries accordingly.
2. Invoke the `runInstaller` (`setup.exe` on Microsoft Windows) by executing:

```
<DVD>/<runInstaller or setup.exe> -silent -responseFile <location>/additional_
mgmt_service.rsp
```

The following message on the `root.sh scripts` is displayed (for UNIX only):

```
WARNING:A new inventory has been created in this session. However, it has not
yet been registered as the central inventory of this system.
To register the new inventory please run the script '<User's Home
Dir>/oraInventory/orainstRoot.sh' with root privileges.
If you do not register the inventory, you may not be able to update or patch
the products you installed.
The following configuration scripts need to be executed as the root user.
#!/bin/sh
#Root script to run
<User's Home Dir>/oraInventory/orainstRoot.sh
<Install Location>/oms10g/allroot.sh
To execute the configuration scripts:
    1. Open a terminal window
    2. Log in as root
    3. Run the scripts
    4. Return to this window and click OK to continue
```

4.1.4 Silent Installation of an Additional Management Agent

To perform a silent installation of this type:

1. Copy the `<DVD>/response/additional_agent.rsp` file to a location on the local machine and modify the *Value Unspecified* entries accordingly.

2. Invoke the `runInstaller` (`setup.exe` on Microsoft Windows) by executing:

```
<DVD>/<runInstaller or setup.exe> -silent -responseFile <location>/additional_
agent.rsp
```

The following message on the `root.sh scripts` is displayed (for UNIX only):

```
WARNING: A new inventory has been created in this session. However, it has not
yet been registered as the central inventory of this system.
To register the new inventory please run the script '<User's Home
Dir>/oraInventory/orainstRoot.sh' with root privileges.
If you do not register the inventory, you may not be able to update or patch
the products you installed.
The following configuration scripts need to be executed as the root user.
#!/bin/sh
#Root script to run
<User's Home Dir>/oraInventory/orainstRoot.sh
<Install Location>/agent10g/root.sh
To execute the configuration scripts:
    1. Open a terminal window
    2. Log in as root
    3. Run the scripts
    4. Return to this window and click OK to continue
```

Caution: The agent you are installing is not secure by default. To secure the agent, execute the following command:

```
AGE<NT_HOME>/bin/emctl secure agent
```

4.1.4.1 Setting Up Proxy Configuration for the Management Agent

There are two ways to specify proxy information for a Management Agent:

- Specify values for `s_proxyHost` and `s_proxyPort` using a response file when performing a silent installation using Oracle Universal Installer.
- Specify values directly through the command-line option when invoking Oracle Universal Installer. For example:

```
<runInstaller or setup.exe> oracle.sysman.top.agent:s_proxyHost="<value>"
oracle.sysman.top.agent:s_proxyPort="<value>"
```

4.2 Assigning Custom Ports (Static Ports Feature)

You can specify custom port numbers for components instead of having the installer assign default port numbers. This feature is called the static ports feature. To use static ports, you must set up a file with component names and the appropriate port numbers. The installer uses the values from the file instead of the default port numbers.

The `staticports.ini` file is available on the installation DVD-ROM at:

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

To invoke `runInstaller` (`setup.exe` on Microsoft Windows) with the `staticports.ini` option, execute the following command:

```
./<runInstaller or setup.exe> -staticPortsIniFile <location>/staticport.ini
```

This file is called the `staticports.ini` file. Section 4.3, "Formats for the Staticports.ini File" describes the file format.

> **See Also:** *Oracle Application Server 10g Installation Guide* (for your operating system) for more information on assigning custom port numbers for installation components at:
>
> `http://otn.oracle.com/documentation/appserver10g.html`

Edit the local copy (the file on the hard disk) to include the required port numbers.

You do not need to specify port numbers for all components in the `staticports.ini` file. If a component is not listed in the file, the installer uses the default port number for that component.

When installation is complete, you can check the `ORACLE_HOME/install/portlist.ini` file to view the assigned ports.

Note: When choosing port numbers, consider the following:

- Port numbers cannot be greater than 65536.
- If you use a port number less than 1024 for a component, you must run the component as the `root` user.
- If you use a port number less than 1024 for a component, the installer cannot start up the component at the end of installation. You may need to configure the component first before you can start it up. See the appropriate component documentation for details.

The installer verifies that the ports specified in the file are available (free) by reading the `Properties` file in all the Oracle homes. If the installer detects that a specified port is not available, it displays an alert.

A port is considered to be free only if:

- There are no Oracle products assigned to that port.
- There are no processes running on that port.

The installer does not assign a port that is not available. To fix this:

1. Edit the `staticports.ini` file to specify a different port.
2. Click **Retry.** The installer rereads the`staticports.ini` file and verifies the entries in the file again.

Note: The `staticports.ini` file uses the same format as the `ORACLE_HOME/install/portlist.ini` file, which is created after an Oracle Application Server installation. If you have installed Oracle Application Server and you want to use the same port numbers in another installation, you can use the `portlist.ini` file from the first installation as the `staticports.ini` file for subsequent installations.

Edit the local copy (the file on the hard disk) to include the appropriate port numbers.

4.3 Formats for the Staticports.ini File

The `staticports.ini` file has the following format. Replace `port num` with the port number that you want to use for the component.

```
# Enterprise Manager

#Enterprise Manager Central Agent Port=port_num
#Enterprise Manager Central Console Port=port_num
#Enterprise Manager Central Console Secure Port=port_num

# J2EE and Web Cache

#Oracle HTTP Server Listen port=port_num
#Oracle HTTP Server Listen (SSL) port=port_num
#Oracle HTTP Server Diagnostic port=port_num

#Web Cache HTTP Listen port=port_num
#Web Cache HTTP Listen (SSL) port=port_num
#Web Cache Administration port=port_num
#Web Cache Invalidation port=port_num
#Web Cache Statistics port=port_num

#Oracle Notification Server Request port=port_num
#Oracle Notification Server Local port=port_num
#Oracle Notification Server Remote port=port_num
#Application Server Control port=port_num
#Application Server Control RMI port=port_num
#Oracle Management Agent port=port_num
#Log Loader port=port_num
```

> **Note:** After having specified appropriate port values, ensure you remove the comment (#) for those properties before saving the file. The values are not considered otherwise.

4.4 Error Conditions that Cause the Installer to Resort to Default Ports

Check your `staticports.ini` file carefully, because a mistake can cause the installer to use default ports without displaying any warning. Here are some things that you should check:

- If a port is already being used by a component or any other application, do not specify that port (used port) in the `staticports.ini` file.

  > **Note:** If you specify a port that is already in use, the related configuration assistant will also fail.

- If you have specified the same port for more that one component, the installation will display 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), the installer ignores the line. For the components specified on such lines, the installer assigns the default ports. The installer does not display a warning for lines with syntax errors.

- If you misspell a component name, the installer assigns the default port for the component. Names of components in the file are case-sensitive. The installer does not display a warning for lines with unrecognized names.
- If you specify a nonnumeric value for the port number, the installer 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, the installer does not display a warning. It continues and assigns default ports to all components.
- If you specify a relative path to the `staticports.ini` file (for example, `./staticports.ini`) on the command line, the installer does not find the file. The installer continues without displaying a warning and it assigns default ports to all components. You must specify a full path to the `staticports.ini` file.
- If the parameter you specify on the command line does not match the installation type that you are performing (for example, if you specify the parameter for the middle tier but you are installing the infrastructure), the installer does not give a warning. It continues and assigns default ports to all components.

5

Prerequisites for Installing Enterprise Manager on Oracle RAC

This chapter discusses the preinstallation requirements for Enterprise Manager Grid Control in an Oracle Real Application Clusters (Oracle RAC) environment.

This chapter contains the following sections:

- Configure Oracle Cluster Synchronization Services (CSS)
- Certification for Agents on Oracle Real Application Clusters (Oracle RAC)
- Additional Software Requirements for Agent Installation on Clusters
- Preinstallation Tasks for Oracle Real Application Clusters

5.1 Preinstallation Requirements

Before installation, ensure the following preinstallation requirements are met.

5.1.1 Configure Oracle Cluster Synchronization Services (CSS)

The first time you install Oracle Enterprise Manager on a system, Oracle Universal Installer configures and starts a single-node version of the Oracle Cluster Synchronization Services (CSS) service. The CSS service is required to enable synchronization between an Automatic Storage Management (ASM) instance and the database instances that rely on it for database file storage. It is configured and started even if you do not choose Automatic Storage Management as a storage mechanism for database files.

Because it must be running before any Automatic Storage Management instance or database instance is started, Oracle Universal Installer configures it to start automatically when the system starts.

For Oracle RAC installations, the CSS service is installed with Oracle Clusterware in a separate Oracle home directory. For single-node installations, the CSS service is installed in and runs from the same Oracle home as Oracle Database. For this reason, you must use caution when removing Oracle Database software from the system. Before you remove an Oracle home directory that contains Oracle Database, you must either delete the CSS service configuration, or if necessary, reconfigure the CSS service to run from another Oracle home directory.

If you plan to have more than one Oracle Database installation on a single system and you want to use Automatic Storage Management for database file storage, Oracle recommends that you run the CSS service and the Automatic Storage Management

instance from the same Oracle home directory and use different Oracle home directories for the database instances.

5.1.2 Certification for Agents on Oracle Real Application Clusters (Oracle RAC)

See Also: *Oracle High Availability Architecture and Best Practices* for information on cluster configuration recommendations.

5.1.3 Additional Software Requirements for Agent Installation on Clusters

If the Enterprise Manager installation is on a cluster, you must install Oracle Clusterware (formerly called Oracle Cluster Ready Services) or any vendor clusterware separately, besides fulfilling all the other Oracle software requirements (see Section 1.4.3, "Enterprise Manager Software Requirements" for more information). Oracle Clusterware is not available on the Oracle Enterprise Manager Grid Control 10*g* Release 2 (10.2) installation media.

5.1.3.1 Oracle Clusterware/Vendor Clusterware

Oracle Clusterware consists of key subcomponents required by Oracle Real Application Clusters installations. It performs workload management and a component restart. For example, when an instance supporting a particular service fails, Oracle Clusterware restarts the service on the next available instance that you have configured for that service.

You must install Oracle Clusterware before installing Oracle Real Application Clusters. The software is available on the Oracle Clusterware installation media.

See Also: *Oracle Enterprise Manager Licensing Information* available on the Oracle Database installation media for more information.

5.1.4 Preinstallation Tasks for Oracle Real Application Clusters

Before you install and use Oracle Real Application Clusters, you must configure secure shell (SSH) for the Oracle user on all cluster nodes. The installer uses the `ssh` and `scp` commands during installation to run remote commands on and copy files to the other cluster nodes. You must configure SSH so that these commands do not prompt for a password.

Note: If SSH is not available, the installer attempts to use `rsh` and `rcp` instead. However, these services are disabled by default, in most Linux machines.

To configure SSH, complete the following steps on each cluster node:

1. Log in as the Oracle user.
2. If necessary, create the `.ssh` directory in the Oracle user's home directory and set the correct permissions on it:

   ```
   $ mkdir ~/.ssh
   $ chmod 755 ~/.ssh
   ```

3. Enter the following commands to generate an RSA key for version 2 of the SSH protocol:

   ```
   $ /usr/bin/ssh-keygen -t rsa
   ```

At the prompts:

- Accept the default location for the key file.
- Enter and confirm a password (or pass phrase) that is different from the Oracle user's password.

This command writes the public key to the `~/.ssh/id_dsa.pub` file and the private key to the `~/.ssh/id_dsa` file. Never distribute the private key to anyone.

4. Enter the following commands to generate a DSA key for version 2 of the SSH protocol:

```
$ /usr/bin/ssh-keygen -t dsa
```

At the prompts:

- Accept the default location for the key file.
- Enter and confirm a password (or pass phrase) that is different from the Oracle user's password.

This command writes the public key to the `~/.ssh/id_dsa.pub` file and the private key to the `~/.ssh/id_dsa` file. Never distribute the private key to anyone.

5. Copy the contents of the `~/.ssh/id_rsa.pub` and `~/.ssh/id_dsa.pub` files to the `~/.ssh/authorized_keys` file on this node and to the same file on all other cluster nodes.

> **Note:** The `~/.ssh/authorized_keys` file on every node must contain the contents from all of the `~/.ssh/id_rsa.pub` and `~/.ssh/id_dsa.pub` files that you generated on all cluster nodes.

6. Change the permissions on the `~/.ssh/authorized_keys` file on all cluster nodes:

```
$ chmod 644 ~/.ssh/authorized_keys
```

At this point, if you use ssh to log in to or run a command on another node, you are prompted for the password (or pass phrase) that you specified when you created the DSA key.

To enable the installer to use the `ssh` and `scp` commands without being prompted for a password, follow these steps:

1. On the system where you want to run the installer, log in as the Oracle user.
2. Enter the following commands:

```
$ exec /usr/bin/ssh-agent $SHELL
$ /usr/bin/ssh-add
```

3. At the prompts, enter the password (or pass phrase) for each key that you generated.

If you have configured SSH correctly, you can now use the `ssh` or `scp` commands without being prompted for a password or a pass phrase.

4. To test the SSH configuration, enter the following commands from the same session, testing the configuration of each cluster node:

```
$ ssh nodename1 'date'
$ ssh nodename2 'date'
    .
    .
```

These commands should display the date set on each node. If any node prompts for a password or pass phrase, verify that the ~/.ssh/authorized_keys file on that node contains the correct public keys.

5. To ensure that X11 forwarding will not cause the installation to fail, create a user-level SSH client configuration file for the Oracle software owner user, as follows:

   a. Using any text editor, edit to create the `~oracle/.ssh/config` file.

   b. Ensure the ForwardX11 attribute is set to `no`, for example:

   ```
   Host *
         ForwardX11 no
   ```

6. You must run the installer from this session or remember to repeat steps 2 and 3 before you start the installer from a different session.

Some of the other preinstallation tasks are listed below:

- Configure SSH on all nodes.
- Oracle Clusterware/vendor clusterware must be running.

For more detailed information on these preinstallation and installation tasks that you must perform for an Oracle RAC installation, see *Oracle Real Application Clusters Installation and Configuration Guide*.

Note: See Chapter 3, Grid Control Common Configurations in *Oracle Enterprise Manager Advanced Configuration Guide* for more information about installing Enterprise Manager on RAC nodes.

6

Deploying the Management Agent

The Oracle Management Agent, a process that is installed/deployed on each monitored host, is responsible for monitoring all targets on the host, for communicating that information to the Management Service, and for managing and maintaining the host and its targets. This chapter contains the following sections:

- Management Agent Installation/Deployment Options
- Installing the Management Agent Using Agent Deploy
- Sharing the Agent Oracle Home Using the nfsagentinstall Script
- Installing the Agent Using the agentDownload Script

6.1 Management Agent Installation/Deployment Options

You can install/deploy the Management Agent on remote hosts using any of the following installation mechanisms:

- Agent Deploy Application

  Agent Deploy is a J2EE application that is used for mass deployment of Management Agents. See Section 6.2, "Installing the Management Agent Using Agent Deploy" for more information.

- nfsagentinstall Script

  This installation type uses the `nfsagentinstall` script. In this method of the agent installation, the agent bits are located on a shared Net App Filer disk. All the other hosts then share these bits and run the agent processes on each host. See Section 6.3, "Sharing the Agent Oracle Home Using the nfsagentinstall Script" for more information.

- agentDownload Script

  This installation type makes use of the `agentDownload` Script that is fully functional and self-documenting. If required, you can customize this script for installations on specific environments. See Section 6.4, "Installing the Agent Using the agentDownload Script" for more information.

- Cluster Agent Installation

  This type of installation allows you to perform a standalone agent installation on a selected cluster node, or perform a cluster agent installation on a selected cluster. See Chapter 8, "Deploying Cluster Agent" for more information.

- Management Agent Cloning

This type of installation allows you to clone an installed agent (also referred to as the master agent) on multiple destination Oracle homes. See Chapter 9, "Management Agent Cloning" for more information.

- Interactive Installation Using Oracle Universal Installer

  This type of installation is appropriate for first-time Agent installations. You can perform this installation by invoking the installer using Oracle Universal Installer (OUI). The Interactive type is typically a one-node installation. See Section 3.3.4, "Installing a Management Agent" for more information.

- Silent Installation

  This type of installation is done using the appropriate response files. These response files must be edited to prefill the correct values for an uninterrupted installation. You can also use a wrapper script that will perform these tasks and also execute the `root.sh` script (UNIX only), making this type of installation a fully automated activity. See Section 4, "Enterprise Manager Silent Installations" for more information.

6.2 Installing the Management Agent Using Agent Deploy

You can perform a mass deployment of the Management Agent through the Web-based Agent Deploy application. This application is particularly useful when you want to perform remote installations.

For information about patches to be applied before performing cross-platform Agent push, see Section 5.4 of the Agent Best Practice paper located at http://www.oracle.com/technology/products/oem/pdf/10gr2_agent_deploy_bp.pdf.

Note: You can use the Agent Deploy application to mass-deploy the Management Agent from a remote site.

When you are required to perform a standalone installation of the Agent on a local machine, you can choose to either perform the installation using the Agent Deploy application, or use the `agentDownload` script. See the section Section 6.4.1, "About agentDownload Script", for more information.

Note: Oracle recommends that you view the installation status output (emctl status) to ensure the installation was successful. You can view this status by executing the following command:

```
<AGENT_HOME>/bin/emctl status agent
```

See Section A.1.3, "Management Agent Installation Fails" to view a sample of the `emctl status` log and to troubleshoot possible errors that may occur during installation.

Caution: If you are deploying the Management Agent in an environment having multiple Management Service installations that are using a load balancer, you should not access the Agent Deploy application using this load balancer. Oracle recommends that you access the Management Service directly.

6.2.1 Agent Deploy Installation Prerequisites

Ensure the following prerequisites are met before proceeding with the agent installation.

- Set up SSH (Secure Shell) User Equivalence.
- Validate the path to all command locations.
- Modify response file for Big IP host and port.
- Verify `oraInventory` permissions on remote hosts.
- User installing the agent is part of the same operating system group that installed Oracle Application Server and/or Oracle Collaboration Suite.

See Appendix C, "Agent Deploy Application - Installation Prerequisites" for more information.

Note: You can view the prerequisite checks and installation status from the Status screen in the Agent Deploy application.

WARNING: Do not attempt to view the prerequisite check status while the prerequisite checks are still in progress. If you do so while the checks are still in progress, the application will display an error.

6.2.2 Accessing the Agent Deploy Application

To access Agent Deploy application, complete the following steps:

1. Log in to the Grid Control console and go to the Deployments screen.
2. Click **Install Agent** under the Agent Installation section.
3. In the Agent Deploy home page that appears, select the appropriate installation option that you want to perform.

Note: If you want to view the status of an earlier installation/upgrade session, click **Agent Installation Status** in the Deployments screen.

6.2.3 Agent Deploy Installation Types

Agent Deploy provides the following two options for deploying the Management Agent:

- Fresh Installation of the Management Agent
- Installation Using a Shared Agent Home

Note: You can view the installation status from the Status screen in the Agent Deploy application.

WARNING: Do not attempt to view the installation status until the installation is complete. If you do so while the installation is still in progress, the application will display an error.

6.2.3.1 Fresh Installation of the Management Agent

This option helps you perform a new installation of the Management Agent. The Agent Deploy application runs a prerequisite checker to ensure the environment meets the requirements for this installation type. See Section C.2, "Prerequisite Checks Executed by Agent Deploy" for more information.

To perform a new Management Agent installation, complete the following steps:

1. Select **Fresh Install** on the Agent Deploy application home page. The Installation Details screen appears.
2. In the Source Software section, select an installation source directory. This directory can either be the default directory that exists within the Oracle Management Service (OMS), for example `<OMS_HOME>/sysman/agent_download/10.2.0.2.0/<platform>`, or any other location where the software is available.

   Note: At the time of downloading the agent installation software, if the `agentDownload.rsp` file is overwritten, ensure the `s_OMSHost` and `s_OMSPort` values are specified correctly in the response file (`agentdownload.rsp`) before proceeding with the installation steps.

   See Section 6.4.5, "Downloading 10.2.0.3.0 Agent Installation Software for Different Platforms" for more information on obtaining agent binaries for different platforms.

   To choose a location other than the default location from the Management Service, select **Another Location**, and specify the full path to the software location that you want to use.

   Note: Ensure that the path of the software location that you specify is accessible from all remote hosts.

   The application does not copy the software to the remote hosts, but will only access the software from the specified location.

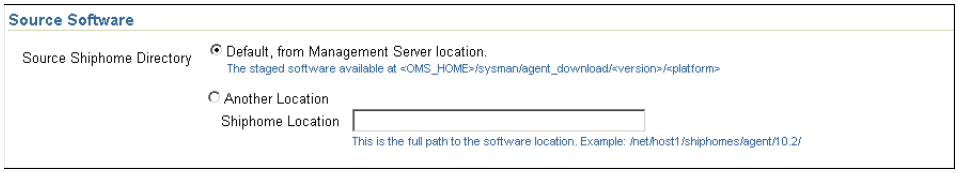
   After you download the agentDownload software, unzip and extract its contents into a new directory. Rename this new `<directory>/$<platform>/agent` to `<directory>/$<platform>/Disk1` and use the **`<directory>/$<platform>`** as the source software location.

Caution: The additional parameters that you specify later in the installation process depend on the source software location that you select here.

if you select the default software location, you must specify additional parameters that are supported by the `agentDownload` script. See Table D–1, " Parameters Supported by agentDownload Script" for a list of parameters supported by this script.

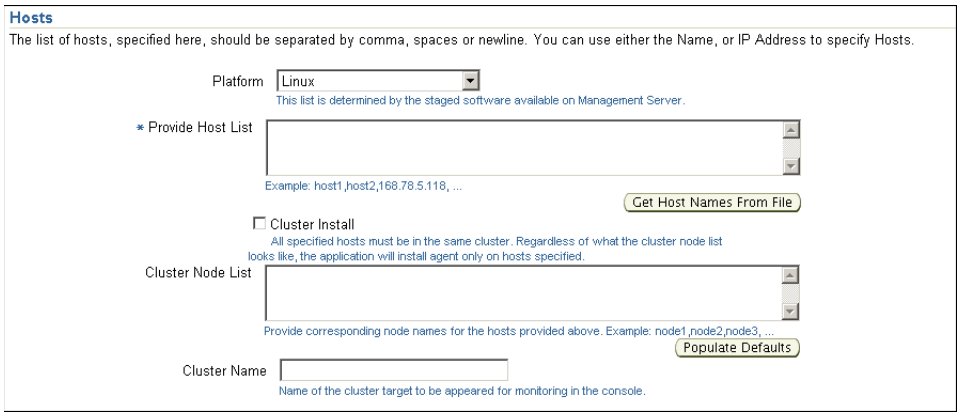
If you select an alternative location, you must specify additional parameters that are supported by Oracle Universal Installer (OUI). See Table D–2, " Parameters Supported by Oracle Universal Installer" for a list of parameters supported by OUI.

Figure 6–1 Source Software Section of the Installation Details Page



3. In the Version section on this screen, select the appropriate version of the agent that you want to install. The values available in this list will depend on the staged software that are available on the Management Service host.
4. Select the appropriate platform on which you want to perform this installation.
5. In the Hosts section, do the following:

Figure 6–2 Hosts Section of the Installation Details Page



a. Select the appropriate platform on which you want to perform this installation.

b. In the Provide Host List text box, specify all the hosts (host names or IP addresses) on which you want to perform the agent installation. Alternatively, click **Get Host Names From File** to browse and select the file that contains a list of all the required host names.

WARNING: Ensure you do not specify duplicate entries of the host list. If there are duplicate host entries in this list, the application hangs.

Also ensure that you use the same host names for which the SSH has been set.

Note: You can use either a comma (,) or a new line as a separator when specifying multiple hosts.

Caution: The Agent Deploy application picks up only the values in the first column of the Host List file that you specify/select.

Ensure the host list format is appropriate, because the Agent Deploy application does not validate this format on the selected file.

A sample host list format is provided in Table 6–1, " Sample Host List Format".

Note: For Enterprise Manager 10.2.0.1 and 10.2.0.2, use the "Populate Details" button to populate the cluster node list or provide a comma-separated list.

Table 6–1 Sample Host List Format

Fully Qualified Host Name	Host Name	Host IP Address
host1.foo.com	host1	154.87.3.229
host2.foo.com	host2	154.87.3.109
host3.foo.com	host3	154.80.5.218

c. Select **Cluster Install** if you want to install the Agent on a cluster.

d. In the Cluster Node List text box, specify the cluster nodes. Alternatively, click **Populate Defaults** to populate this text box with all the host names that you had selected in step *b*.

Note: The node names that you specify here are the machine short names.

If you have set up the cluster over a vendor clusterware, the node names can be different from the machine names.

You can confirm the node names by executing `olsnodes` from the `<Oracle Clusterware home>` on one of the cluster nodes. If you are using Oracle Cluster release 9.2, confirm the node names by executing `lsnodes` from the cluster Oracle home.

See Section 8.2, "Installing the Agent on Oracle Clusterware" for more information.

e. In the Cluster Name text box, specify a unique cluster name. If you are extending a cluster, specify the existing cluster name here. The cluster name that you specify here identifies that cluster in the Grid Control console.

Note: When you select the cluster installation option, Agent Deploy performs the agent installation only on those cluster nodes that you have specified, irrespective of the number of hosts that make up that cluster.

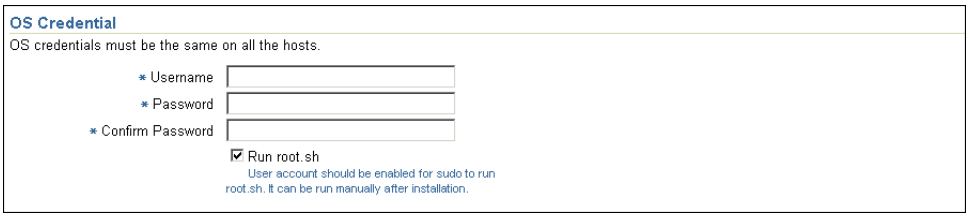
For example, if you choose to perform a cluster installation on a cluster having 10 nodes, but specified only 5 nodes, Agent Deploy installs the agent only on the 5 nodes of the cluster that you have specified.

If you are extending an existing cluster, ensure that the cluster name you specify is the same as the existing cluster. You must also specify all the nodes of the existing cluster along with the new node on which you are installing the cluster agent.

---

6. In the OS Credentials section, specify the appropriate operating system user credentials. Select **Run root.sh** (on UNIX machines only) if you want Agent Deploy to execute this script.

Figure 6–3 OS Credentials Section of the Installation Details Page



Note: The `root.sh` script executes after the configuration assistants are run, and before executing postinstallation scripts (if any).

If you do not select this option here, you must manually run `root.sh` on each node.

Agent Deploy uses `sudo` to run this script. You must specify the *invoking user's password* here. You must also ensure that the `targetpw` is not set in the `/etc/sudoers` file.

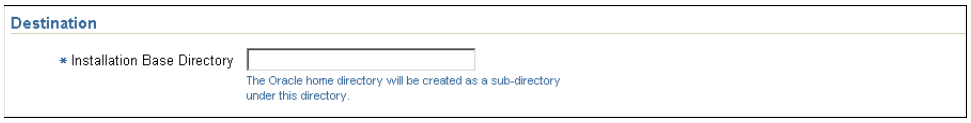
Note: The OS credentials that you specify here must be the same for all the selected hosts.

---

7. In the Destination section, specify the absolute path for the Installation Base Directory. This directory is created on all the specified hosts, and the Agent Oracle home directory is created as a subdirectory under this directory.

Note: For the Agent push to be successful, ensure that you extract the agentDownload kit before performing the Agent push.

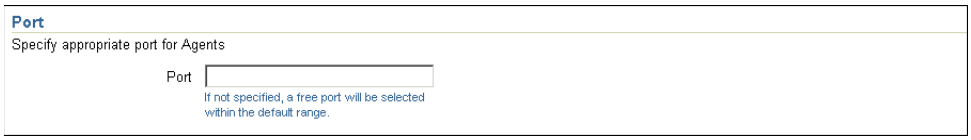
Figure 6–4 Destination Section of the Installation Details Page



Note: Ensure you have write permissions on the installation Base Directory that you specify.

8. Specify the port on which the Agent will communicate. The default port value for 10.2 Management Agent is 3872.

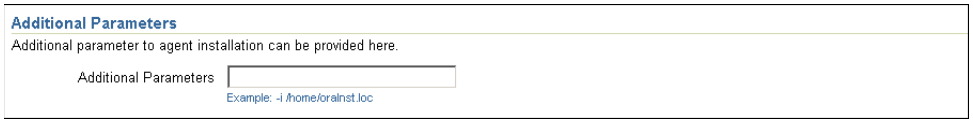
Figure 6–5 Port Section of the Installation Details Page



Note: If the port that you specify is not available, you are prompted to specify an alternative port. If you do not specify a port here, the Agent Deploy application automatically picks up a free port (3872 or in the range of 1830 - 1849).

9. In the Additional Parameters text box, specify any additional parameters that you want to pass during installation.

Figure 6–6 Additional Parameters Section of the Installation Details Page



Caution: The additional parameters that you specify here depend on the software source location that you have selected.

- *Default Management Service Location:* If you have selected the default software source directory, the additional parameters that you specify must be supported by the `agentDownload` script, as the Agent Deploy application uses the `agentDownload.<platform>` script to perform the installation. See Table D.1, "Additional Parameters Supported by agentDownload Script" for a list of all the parameters supported by the `agentDownload` script.
- *Another Location:* If you have selected an alternative software location, the additional parameters that you specify must be supported by Oracle Universal Installer (OUI), as Agent Deploy then uses OUI to perform the installation. See Table D.2, "Additional Parameters Supported by Oracle Universal Installer" for a list of parameters supported by OUI.

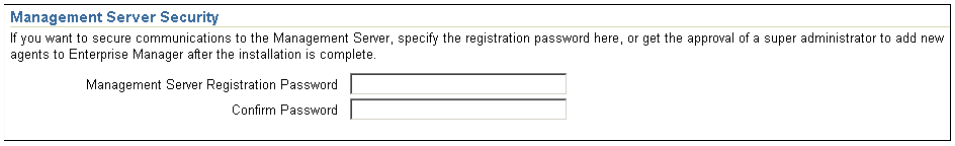
Note: If the same parameters that you specify here are also specified independently (from the command-line option), the value of the parameters that you specify here take precedence over the other.

For example, if the installation base directory is specified independently, and `-b` option is specified here, the latter value (`-b`) is used in the installation.

The important parameters for Agent Installation are `-b, -c, -n, -z` and optionally `-i, -p, -t, -d`.

10. Specify the Management Service Registration Password if you want to secure communications between the agent and Management Service. Alternatively, the super administrator can approve the addition of new agents to Enterprise Manager after the installation is complete.

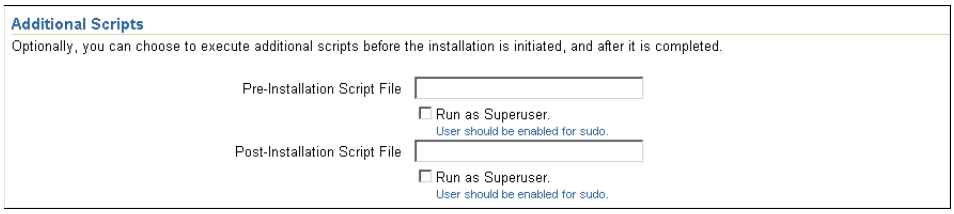
Figure 6–7 Management Server Security Section of the Installation Details Page



Note: An unsecure agent cannot upload data to the secure Management Service. Oracle also recommends for security reasons that you change the Management Service password specified here after the installation is complete.

11. In the *Additional Scripts* section, specify any preinstallation and/or postinstallation scripts that you want to execute.

Figure 6–8 Additional Scripts Section of the Installation Details Page



Select **Run as Superuser** if you want to run these scripts as `root`.

Note: The preinstallation and/or postinstallation scripts that you specify must be available on all the hosts. These files are not copied onto the hosts from the software source location during installation.

---

12. Click **Continue** to start the installation process. As part of this process, Agent Deploy performs some prerequisite checks before proceeding with the installation. When all the prerequisite checks are complete, the application displays the results. You can choose to either retry the prerequisite check on all those failed hosts, or ignore the result and proceed to install the Agent.

Note: After the installation and configuration phase, the Agent Deploy application checks for the existence of the Central Inventory (located at `/etc/oraInst.loc`). If this is the first Oracle product installation, Agent Deploy executes the following scripts:

1. `orainstRoot.sh` - UNIX Machines only: This creates oraInst.loc that contains the central inventory.
2. `root.sh` - UNIX Machines only: This runs all the scripts that must be executed as `root`.

If this is not the first Oracle product installation, Agent Deploy executes only the `root.sh` script.

Note: For more information on the prerequisites check, installation, and configuration logs that are created, see Section F.2, "Agent Deploy Log Files".

6.2.3.1.1 Scenarios to Consider While Performing a Cluster Agent Install

Consider the following scenarios while performing cluster installation:

You are performing a new Agent installation on a cluster that does not have an Agent.

This is a scenario where you have an existing cluster (`cr1` with three nodes n1, n2, and n3) but without an agent installation on any of the nodes. Here, if you specify only two nodes (n1 and n2) for an agent installation, Agent Deploy updates the inventory for these two nodes and the agent is installed and running.

Now, you want to install the agent on the third node (n3) and specify the cluster name as `cr1` and all three hosts and nodes (n1, n2, and n3) this time. Agent Deploy updates the n1 and n2 inventory to include n3 and the agent is installed.

Caution: In a scenario such as the one above, you must specify the same cluster name and include all the existing nodes of that cluster.

You are extending a cluster, but do not include all the existing nodes.

This is a scenario where you want to install an agent on the node (n4) that is an extension of the existing cluster (cr1 with nodes n1, n2, and n3.) But during the agent installation, you specify only the new node (n4) in the Cluster Node List text box. Agent Deploy installs the agent on n4, but does not update the inventory of the other three nodes (n1, n2, and n3) to include n4.

To ensure that the inventory of all the nodes of an existing cluster are updated, you must specify all the hosts and nodes of that cluster along with the new node (n4 in this example.)

If you have specified just the one node and the existing cluster name (cr1), Agent Deploy still creates a new cluster with the same name.

If you have specified just the one node and did not specify a cluster name, Agent Deploy computes a default cluster name and create a new cluster.

You are installing the Agent on two clusters of the same name, but with different nodes.

You have two clusters with the same name but with different nodes, for example `crs` (with n1, and n2) and `crs` (with n3 and n4), and you want both clusters to be managed by the same OMS. To distinguish the two clusters in the Grid Control console, you must do the following:

When you are installing the agent on the first `crs` cluster (with nodes n1 and n2), enter a unique cluster name and perform the installation. Now, enter a different cluster name for the other `crs` cluster (with nodes n3 and n4) and perform the Agent installation.

Now, you can view these clusters in the Grid Control console under unique cluster names that you specified during agent installation.

6.2.3.2 Installation Using a Shared Agent Home

To deploy and install an agent on multiple hosts using an existing Shared Agent Installation, you must have already performed a complete Enterprise Manager product installation (including the agent). Another prerequisite when using this option is that the directory where the agent is installed should be NFS-mounted, meaning the directory must be a shared location on all remote hosts.

The Agent Deploy application runs a prerequisite checker to ensure the environment meets the requirements for this installation type. See Section C.2, "Prerequisite Checks Executed by Agent Deploy" for more information.

Caution: NFS agent deployment is not supported on a cluster. If you want the agent to monitor a cluster and Oracle RAC, you must use the agent deployment with the cluster option, and not the NFS (network file system) deployment method.

Note: You can also perform a Shared Agent Oracle home installation using the `nfsagentinstall` script. See Section 6.3, "Sharing the Agent Oracle Home Using the nfsagentinstall Script" for more information.

6.2.3.3 Concepts and Prerequisites

The following sections briefly discuss the shared agent home concepts, and also list the prerequisites before starting the installation.

6.2.3.3.1 EMSTATE Directory: This is a directory for storing configuration files such as `emd.properties`, `targets.xml`, `log files`, and so on, on each host. Every host that shares the agent binaries has its own `EMSTATE` directory.

6.2.3.3.2 EMSTATE Directory Location:

- The `EMSTATE` directories of agents on different hosts should be local to the host instead of on the mounted drive, for security reasons.
- Since the `EMSTATE` directory contains the targets pertaining to each host, it is highly recommended to have it on a local host.

6.2.3.3.3 EMSTATE Directory Space Requirements: The initial space required for `EMSTATE` directories is 1 MB. Since all the upload files, collection files, and log files are stored in this directory, the size of the directory will increase. Consequently, Oracle recommends that you allocate sufficient space for the `EMSTATE` directories after taking these factors into account.

6.2.3.3.4 Packages and OS Patches Requirement: Currently, no packages are required by the agent to run on the shared hosts.

6.2.3.3.5 Operating System Credentials: When you are performing an agent installation using a shared Oracle home, ensure all the specified hosts have the same operating system credentials and file system structure, including the following:

- Same User names and Group names
- Same user identifiers (UID) and group identifiers (GUID)

This is important for the agent from the remote host (NFS-mounted) to execute certain programs (for example, `ORACLE_HOME/bin/nmo`) that are otherwise not accessible to other users.

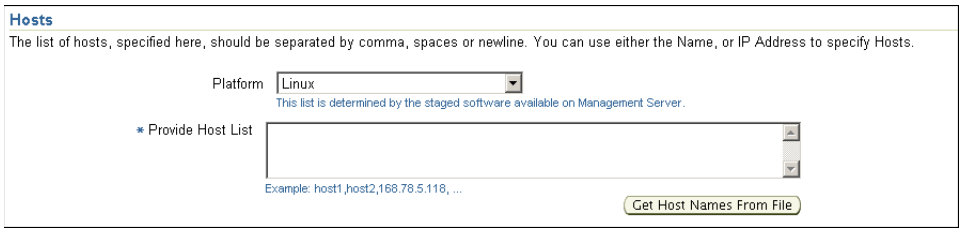
6.2.3.3.6 Shared oraInventory When performing a cluster agent installation using a shared agent Oracle home, ensure the `oraInventory` is shared (accessible by all remote hosts).

6.2.3.4 Performing the Installation

To perform a new Management Agent installation:

1. Select **Shared Agent Home** on the Agent Deploy application home page. The Installation Details screen appears.
2. In the Hosts section:

Figure 6–9 Hosts Section of the Installation Details Page



a. Select the appropriate Platform on which you want to perform this installation.

b. In the Provide Host List text box, specify all the hosts (host names or IP addresses) on which you want to perform the Agent installation. Alternatively, click **Get Host Names From File** to select the file that contains a list of all the required host names.

WARNING: Do not specify duplicate entries of the host list. If there are duplicate host entries in this list, the application hangs.

Use the same host names for which the SSH has been set.

Note: You can use a comma (,) or just white space as a separator when specifying multiple host names.

Caution: If the Installation Base Directory is shared among the hosts that you have specified in the host list, the installer is invoked from one of these hosts (typically, the first host in that list).

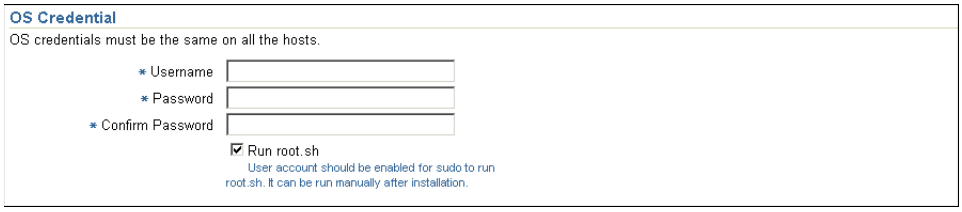
While the installation is performed on only one host, the application executes the configurations on all nodes in the list. That is, the preinstallation, postinstallation, and collect logs are executed on all the nodes.

After the installation is complete, the Installation Status screen displays the status of only this host (from which the installer was invoked). It may not necessarily list the status of all the hosts specified in the host list.

---

3. In the OS Credentials section:

Figure 6–10 OS Credentials Section of the Installation Details Page



a. Specify the appropriate operating system user credentials.

b. Select **Run root.sh** (on UNIX machines only) if you want Agent Deploy to execute this script. Agent Deploy uses `sudo` to run this script. You must specify the invoking user's password here. You must also ensure that the `targetpw` parameter is not set in the `/etc/sudoers` file.

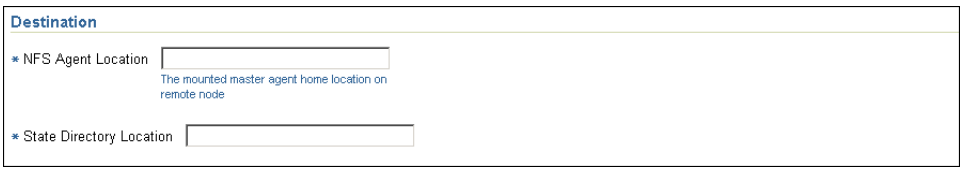
Caution: If you do not want to execute the scripts as root during the installation, ensure you run these scripts manually before performing any other installation on that machine.

Note: The OS credentials that you specify here must be the same for all the selected hosts.

---

4. In the Destination section:

Figure 6–11 Destination Section of the Installation Details Page

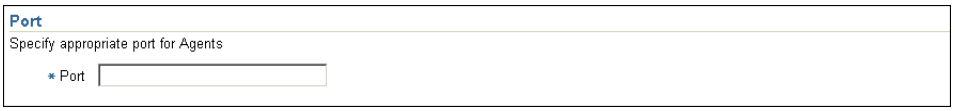


a. Specify the complete path to the NFS Agent Location. This is the shared directory location on the source agent host that must be visible (NFS-mounted) from all remote hosts.

b. Specify an appropriate EMState Directory Location. This is a directory for storing configuration files such as `emd.properties`, `targets.xml`, `log files`, and so on, on each host. Every host that shares the agent has its own `EMSTATE` directory.

5. In the Port section, specify the appropriate port on which the agent will communicate. This is a mandatory field.

Figure 6–12 Port Section of the Installation Details Page



Note: If the port that you specify is busy (not available), you are prompted to specify an alternative port. If you do not specify a port value here, the installation will fail.

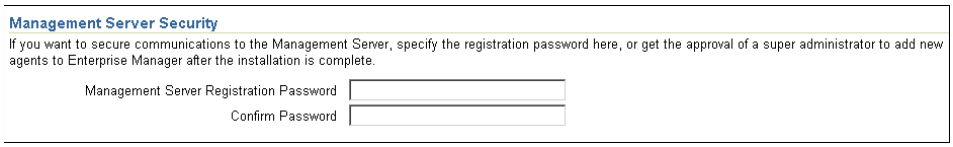
---

6. In the Additional Parameters section, specify the parameters that you may want to pass during installation. You can specify multiple parameters, separated by a space.

Note: Besides the timezone parameter (`-z`), you can also specify all the parameters that are supported by the agentDownload script. See Section D.1, "Additional Parameters Supported by agentDownload Script" for more information.

7. In the Management Server Security section:

Figure 6–13 Management Server Security Section of the Installation Details Page

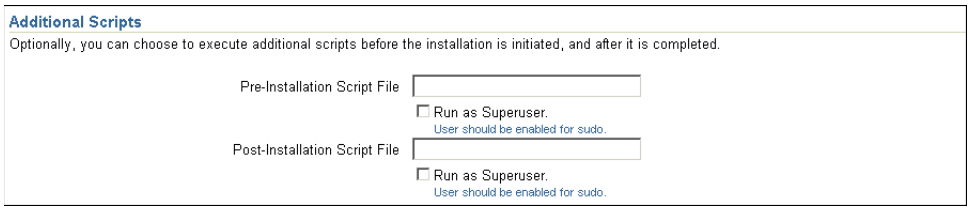


Specify the Management Service Registration Password if you want to secure communications between the Agent and Management Service. Alternatively, the super administrator can approve the addition of new agents to Enterprise Manager after the installation is complete.

Note: An unsecure agent cannot upload data to the Management Service. Oracle also recommends for security reasons that you change the Management Service password specified here after the installation is complete.

8. In the Additional Scripts section:

Figure 6–14 Additional Scripts Section of the Installation Details Page



a. Specify any preinstallation and/or postinstallation scripts that you want to execute. These scripts are optional. If you do not want to customize your installation, leave these fields blank and continue.

b. Click **Continue** to start the installation process.

Caution: If the shared agent is the first Oracle product that is installed on the host, you must execute the following command from the `EMSTATE` directory after completing the installation:

```
<EMSTATE Dir>/bin
./emctl control agent runCollection <Host name>:host Inventory
```

As part of this process, Agent Deploy performs some prerequisite checks before proceeding with the installation. When all the prerequisite checks are

complete, the application displays the results. The results include the name, type, and status for all prerequisite checks designed for the installation.

Besides the successfully run prerequisite checks, the prerequisite checks can return either one of the following messages:

- *Warning*: If there are warnings against certain prerequisite checks, you may choose to ignore these and continue with the installation (though this is not recommended).
- *Failed*: If there are failed prerequisite checks, you cannot continue with the installation. A recommended course of action is to fix the failed prerequisites before proceeding with the installation.

To fix the failed prerequisites, you can either click **Retry**, or go to the Fixup screen of the application. The Fixup screen displays the prerequisites that can be automatically fixed, and those that require manual fixes.

Note: You can view the status of all previous installation instances from the Status screen in the Agent Deploy application. This screen lists all agent installations that were performed using Agent Deploy. You can click the corresponding Status link for each record to view the selected installation details, including user input provided during installation and the final status of that installation.

You can access the Status screen either before starting the installation process, or after the installation is complete. You cannot access the Status screen during an installation.

6.3 Sharing the Agent Oracle Home Using the nfsagentinstall Script

The Enterprise Manager release 10.2 installer supports NFS-mounted agent installations where the agent bits are shared on a Net App Filer disk, and the other hosts share these binaries to run the agent processes on each of the hosts. In this method of agent deployment, the configuration files for each host are stored in the `EMSTATE` directory.

Note: The agent Oracle home cannot be installed in an Oracle Cluster Shared File System (OCFS) drive, but is supported on an NAS (Network Attached Storage) drive.

Caution: You can perform only one nfsagent installation per host. Multiple nfsagent installations on the same host will fail.

6.3.1 Preinstallation Considerations

Consider the following before starting the agent installation using the `nfsagentinstall` script.

6.3.1.1 User Credentials

The shared agent (nfsagent) can be installed only with the same user credentials that were used to perform the master agent installation.

6.3.1.2 If Agent Is Not the First Oracle Product Installation

If this shared agent installation is not the first Oracle product installation and your home directory (of the master agent installation) is shared, you must verify the `oraInst.loc` location under the `/etc` directory.

If `oraInst.loc` and `inventory_loc` are located in the your home directory, you must change this entry point to a non-shared location.

The `oraInst.loc` entry should look like this:

```
inventory_loc=/<any location other than the home directory>/oraInventory
inst_group=<group to which the user belongs>
```

6.3.2 Performing an NFS Agent Installation

To perform an agent installation using `nsfagentinstall` script, complete the following steps:

1. Configure the shared drive on the host in such a way that only one host has read/write access to this shared location, while all the other hosts have only read access.
2. From the host that has read/write access, perform an agent installation in the shared Oracle home location. You can use any agent deployment method. This installation is called as the *master* agent installation.
3. Stop the Agent from the Oracle home.

   Note: You must *not* start the master agent from the installed Oracle home.

4. Now, execute the `OH/sysman/install/nfsagentinstall` script on all the hosts that should share the agent binaries, including the host on which you performed the master agent installation.
5. If this agent installation is the first Oracle product installation on the host, the `nfsagentinstall` script prompts you to execute the following script (on UNIX machines only). You must execute this script manually.

   ```
   <homedir>/oraInventory/orainstRoot.sh
   ```

   The `nfsagentinstall` script also prompts you to execute the `<STATEDIR>/root.sh` command. You must manually execute this command.

   Note: For NFS Agent installation from 10.2.0.3.0 master agents, the NFS agents will be started automatically after rebooting the machine.

   Note: For NFS Agent installation from 10.2.0.3.0 master agents, `agentca` script for rediscovery of targets present in the `<statedir>/bin` directory can be used to rediscover targets on that host.

6.3.2.1 Usage of the nfsagentinstall Script

```
./nfsagentinstall  -s <EMSTATE Directory location> -p <port number>
```

In the preceding command syntax,

- <EMSTATE Directory location> is the full path where you want the state directory to be created by the script.
- <port number> is the port on which the agent runs.

Note: Specifying the <port_number> argument is optional. If you do not specify the port number, the script will automatically select the next available port from that host.

Caution: If the nfsagent is the first Oracle product that is installed on the host, you must execute the following command from the `EMSTATE` directory after completing the installation:

```
<EMSTATE Dir>/bin
./emctl control agent runCollection <Host name>:host Inventory
```

Note: Deployment of agent through the nfsagent install script is *not* supported on clusters. If you want the agent to monitor a Cluster and/or Oracle RAC, you must use the agent deployment with cluster options.

6.3.3 Deinstalling the NFSAgent

If the nfsagent you want to deinstall is the *only* Oracle product installed on the host, you must check the `/etc/oraInst.loc` directory for the inventory location and perform the following steps to deinstall the agent:

1. Stop the agent using the following command:

   ```
   <EMSTATE DIR>/bin/emctl stop agent
   ```

2. On Microsoft Windows, you must delete the agent service by executing the following command:

   ```
   nmesrvops delete <service name>
   ```

3. Execute `rm -rf <inventory_location>`
4. Execute `rm -rf <EMSTATE Dir>`

If the nfsagent you want to deinstall is *not* the only Oracle product installed on the host, then go to the master agent Oracle home (using the mounted path) and perform the following steps to deinstall the agent:

1. Stop the agent using the following command:

   ```
   <EMSTATE DIR>/bin/emctl stop agent
   ```

2. On Microsoft Windows, you must delete the agent service by executing the following command:

   ```
   nmesrvops delete <service name>
   ```

3. Execute the following command from the master agent Oracle home:

   ```
   <master agent home>/oui/bin/runInstaller -detachHome ORACLE_HOME=<master agent
   ```

```
home>
```

4. Execute `rm -rf <EMSTATE Dir>`

6.4 Installing the Agent Using the agentDownload Script

This installation type makes use of the `agentDownload` script that is fully functional and self-documenting. The downloadable Agent software contains a sample script called `agentDownload`. This script provides a means for installing Management Agents that can be customized for specific environments using a silent, scripted installation.

6.4.1 About agentDownload Script

The `agentDownload` script uses the *pull* technology for agent installations. That is, though the script is not required to exist on a local file system, it must always be executed from the target host computer. You must be logged in to the target host to run the script. Files are not pushed from a central location to a list of target hosts. Instead, files are pulled to the local `$ORACLE_HOME` from the staged product installation location.

This means that the `agentDownload` script needs to be launched from each target host where you want to install the Management Agent. As the installation is scripted, it is possible to use a wrapper script, Linux `cron` job, `rdist`, or a combination of operating system features to fully automate this process for mass deployments.

Note: Use the `agentDownload` script to perform an agent installation on a cluster environment. See Section 6.4.4.1, "Cluster Installation" for more information.

6.4.2 Benefits of the agentDownload Script

The download script deploys the standard Management Agent installation with some additional benefits:

- Can be modified for specific user environments.
- Noninteractive, silent, installations.
- Output is text-only (nongraphical).
- Management Agents installed using the script are identical to Management Agents installed with the Oracle Universal Installer graphical installation.
- Simplifies deploying Management Agents in secure Web environments that are configured to provide HTTP access.
- Provides useful installation options using the command line (including the ability to control target autodiscovery, autostarting of the agent, and so on).
- Allows installation onto clustered environments.

6.4.3 Obtaining the agentDownload Script

The downloadable Agent software for the operating system of the Management Service platform is available on the platform-specific CD from which the Management Service was installed, and from the Oracle Technology Network Web site under Mass Agent Deployment at

http://www.oracle.com/technology/software/products/oem/htdocs/agentsoft.html

See Section 6.4.5, "Downloading 10.2.0.3.0 Agent Installation Software for Different Platforms" for more information on obtaining agent installables for different platforms.

6.4.4 Using the agentDownload Script

The `agentDownload` script is downloaded to a target node and executed to initiate a silent Oracle Universal Installer session. The agent files are copied from the staging area in the Management Service home to the target node through HTTP.

To deploy multiple Management Agents using the `agentDownload` script, you must do the following:

1. Install Oracle Management Service.

   Install the Management Service using Oracle Universal Installer. See Section 3.3.3, "Installing an Additional Management Service" for more information.

   > **See Also:** *Oracle Enterprise Manager Advanced Configuration* for more information about the directory structure of a typical Management Service installation

2. The download stage for the Management Service platform is installed with the Management Service. For example, for Linux operating systems, the download stage can be found in:

   `OMS_HOME/sysman/agent_download/<version>/linux`

   - The `agentDownload` script is located at `OMS_HOME/sysman/agent_download/<version>/linux`

     For example, for Enterprise Manager 10*g* R2, the `<version>` value in the preceding syntax will be 10.2.0.2.0

   - The response file is located at `OMS_HOME/sysman/agent_download/<version>`

     > **Caution:** If the Management Service is using a load balancer, you must modify the `s_omsHost` and `s_omsPort` values in the `<OMS_HOME>/sysman/agent_download/<version>/agentdownload.rsp` file to reflect the load balancer host and port before using the `agentDownload` script.

     > **Note:** For Enterprise Manager 10*g* R2, the `<version>` value in the preceding syntax will be `10.2.0.2.0`.

   - The readme file is available at `OMS_HOME/sysman/agent_download`.

3. Download the `agentDownload` script to the target host from the Management Service URL.

   The Management Service installation creates a Web server alias called `agent_download` that maps to a physical directory in the Oracle Application Server home directory where the Management Service is installed and deployed. For

example, if you installed the Management Service on a host named mgmthost27.acme.com, you could access the following URL from a browser:

```
http://mgmthost27.acme.com:4889/agent_download/10.2.0.2.0/<platform>
```

> **Note:** The default port for Grid Control is 4889. This should be available after you install the Management Service.

Using this Web server alias, you can download the script to the target host computer using the following URL. Save the script locally as `agentDownload`.

```
http://mgmthost27.acme.com:4889/agent_
download/10.2.0.2.0/<platform>/agentDownload.<OS>
```

The `<OS>` argument represents the operating system platform. For example, for Linux operating systems, the script is named `agentDownload.linux`. For Windows operating systems, the script is named `agentDownload.vbs`.

On Microsoft Windows, the URL to download the script would be as follows:

```
http://mgmthost27.acme.com:4889/agent_
download/10.2.0.2.0/win32/agentDownload.vbs
```

> **Note:** You can also access the `agentDownload` script from the command line by executing the following command:
>
> ```
> wget http://mgmthost27.acme.com:4889/agent_
> download/10.2.0.2.0/<platform>/agentDownload.<OS>
> ```
>
> or
>
> ```
> wget http://mgmthost27.acme.com:4889/agent_
> download/10.2.0.2.0/win32/agentDownload.vbs
> ```

Any method of retrieving the file is acceptable: cp, rcp, scp, FTP, and so on. The script can also be retrieved by opening a browser window on the target machine and saving the link to a local file.

> **Note:** If you want to download using a file-based protocol rather than HTTP, you need to modify the `$AgentDownload` URL variable to access the file system on the Management Server host instead of a URL.
>
> The URL is the following:
>
> ```
> http://${OMShost}:${httpPort}/agent_download/
> ```
>
> is a Web alias for:
>
> ```
> $OMS_HOME/sysman/agent_download/
> ```

4. Execute the `agentDownload` script on the target host.

   Before launching the script, ensure the following:

- The execute binary is set and the script file has the proper file protection settings (use `chmod` to ensure the file has the correct privileges).
- The base directory is specified at the command line. This will be the location of the Management Agent home on the target host. If the directory does not exist, it is created during the installation. If it exists, ensure it is empty. If the variable is not set, the script exits with an error.

  Note: The base directory for the agent installation must be specified using the `-b` option. For example, if you specified the parent directory to be `agent_download` (`/scratch/agent_download`), then the command to be specified is:

  ```
  -b /scratch/agent_download
  ```

  The agent Oracle home (`agent10g`) is created as a subdirectory under this parent directory.

- The `wget` (or other file transfer mechanism) has been defined in the script. The script checks for the existence of `wget` in `/usr/local/bin/wget`, followed by `/usr/bin/wget`. If wget is not found in either of those locations, then it must be included in the `$PATH` or the script will exit with an error.
- The `$AGENT_INSTALL_PASSWORD` environment variable is set in the environment if the Management Agent is uploading to a secure and locked Management Service.

  Caution: The agent that you are installing is not secure by default. If you want to secure the agent, you must specify the password using the AGENT_INSTALL_PASSWORD environment variable, or by executing the following command after the installation is complete:

  ```
  <Agent_Home>/bin/emctl secure agent
  ```

  Note: For Enterprise Manager 10.2.0.3.0, if the `agent_download.rsp` file does not contain the encrypted registration password or the AGENT_INSTALL_PASSWORD environment variable is not set, the agentDownload script in UNIX will prompt for the Agent Registration password which is used for securing the agent. Provide the password to secure the agent. If you do not want to secure the agent, continue running the agentDownload script by pressing **Enter**.

  See Also: *Oracle Enterprise Manager Advanced Configuration* for more information on enabling security for Enterprise Manager components

- The script user has the necessary file access permissions for the Management Agent home directory.

5. After the Management Agent installation is complete, change the directory to the Agent home directory and run the `root.sh` script (on UNIX machines only) as the `root` user.

   For example:

```
$PROMPT>su root
Password: root_password
#./root.sh
#exit
$PROMPT>
```

The `root.sh` script must be run as `root`; otherwise, the Enterprise Manager job system will not be accessible to the user. The job system is required for some Enterprise Manager features, such as hardware and software configuration tasks and configuring managed database targets.

6.4.4.1 Cluster Installation

The `agentDownload` script can be used to install Management Agents onto clustered environments. In order to perform this type of installation, the command-line options to be used are listed in Table 6–2.

Table 6–2 Command-Line Options for Cluster Installation

Options	Description
-c	This option is followed by a comma-separated list of the nodes in the cluster. It is possible to install a standalone agent that will still discover cluster targets by not specifying this option, while still specifying the cluster name with the `-n` option.
-n	This option is followed by the name of the cluster. This option is required for Oracle9*i* clusters; for Oracle Database 10*g* clusters, if this option is not specified, the default cluster name from the `targets.xml` file will be used.
-l	This option specifies that the installation should be done just on the local node of the cluster.

For example, to use the `agentDownload` script to install a Management Agent on just the local node of a cluster that consists of nodes *host1*, *host2*, and *host3*, with cluster name *myCRS*, you must execute the following:

```
./agentDownload.<platform> -b <name of the Oracle Homes> -m <fully-qualified
Oracle Management Service host name> -r <Oracle Management Service ports> -c
"host1,host2,host3" -n myCRS -l
```

For example for Linux operating system, the command would be as follows:

```
./agentdownload.linux - b /oracle/agentinstall -m foo.us.oracle.com -r 4889 -c
"host1,host2,host3" -n myCRS -l
```

6.4.4.2 Script Details

The `agentDownload` script performs the following actions:

- Creates home directories for the Management Agent and Oracle Universal Installer if they do not exist, based on the `$ORACLE_HOME` path specified through the command line.
- Downloads the `agent_download.rsp` response file from the Management Service Web server.

  The Management Service instantiates the response file with the name and port number of the Management Service. As a result, the Management Agent you install is configured to use the Management Service from which the response file was downloaded.

- Downloads an Oracle Universal Installer JAR file for the target operating system from the Management Service Web server (for UNIX only).
- Extracts Oracle Universal Installer and points it to the product definition file (`products.xml`) hosted by the Management Service Web server.
- Starts Oracle Universal Installer in silent mode from the local machine; Universal Installer pulls files from the Web server to the target machine via HTTP.

> **Note:** This script uses the `-ignoresysPrereqs` flag to bypass prerequisite check messages for operating system-specific patches during installation; prerequisite checks are still performed and saved to the installer logs. While this makes the Management Agent easier to deploy, check the logs to make sure the target machines on which you are installing Management Agents are properly configured for successful installation.

- The resulting installation and configuration, including the automatic discovery of managed targets on the Management Agent host, is identical to that provided by the Management Agent installation on the Enterprise Manager DVD set.
- The `agentDownload` script creates a log file in the base directory that is specified using the `-b` option.
- At the end of a successful installation, the Agent starts and should begin successfully uploading to the Management Service, presuming automatic discovery and automatic start were not disabled at the command line.

To run the script, use the following command:

```
./agentDownload.<platform> [-bcdhilmnoprtuxN]
```

For Linux operating system, the command would be as follows:

```
./agentDownload.linux [-bcdhilmnoprtuxN]
```

The descriptions of the script options are listed in Table 6–3.

Table 6–3 AgentDownload Script Options

Option	Description
-b	To specify base directory of the Agent Oracle home.
-c	To specify the cluster nodes (CLUSTER_NODES) Note that there should not be any spaces between the entries in the comma-separated nodes list.
-d	Do not automatically discover targets during installation. Host target will be created as needed.
-h	To display and describe the options that can be used with this script.
-i	To specify the inventory pointer location file: Can be used to point the installer to a nondefault inventory. (For advanced users only.)
-l	To specify as local host (pass -local to runInstaller)
-m	To specify the Oracle Management Service host name for downloading the agent install.
-n	To specify the cluster name.

Table 6–3 (Cont.) AgentDownload Script Options

Option	Description
-o	To specify the OLD_ORACLE_HOME during upgrade
-p	To specify static port list file.
-r	To specify the port for connecting to the Oracle Management Service host name.
-t	Do not automatically start the agent at the end of the installation.
-u	To upgrade.
-x	To debug output: Turns on shell debugging.
-N	Do not prompt for Agent Registration Password.

6.4.4.3 Customizing the agentDownload Script

You can edit the contents of the `agentDownload` script so it uses a specific tool for transferring files from the Management Service Web server. The contents of the file contain instructions for doing so, as shown in the following example:

```
WGET="/usr/local/bin/wget --dot-style=mega --verbose --tries=5"
InstallerDownloadCmd=$WGET
# Define the command to be used to download the jarred installer from
# the web server hosting the OMS.
# Other download possibilities: ftp; cp/scp; use local browser to save the
# link to a file on the target machine.
# This example uses wget, a GNU tool for http and ftp file transfers.
# If the products.xml referenced by the Oracle Installer is a URL, then the
# Installer will download its files via http. This greatly facilitates
# performing installs in a secure environment that may include firewalls
# and servers with limited access (no ftp server, NFS mounts not available,
# etc.).
# Enterprise Manager version number. This is used to construct the
# home name used by the installer
```

`GNU wget` is available for most platforms and can be downloaded from the following location:

```
http://www.gnu.org/software/wget/wget.html
```

6.4.5 Downloading 10.2.0.3.0 Agent Installation Software for Different Platforms

To obtain the agent download for other platforms, you must complete the following steps to make the Management Agent installable from the Management Service Oracle home.

To Obtain agentDownload for Unix

Follow the instructions below to download the agent installation software for Unix:

1. Download the `<platform>_Grid_Control_agent_download_10_2_0_3.zip` file from OTN:

   `http://www.oracle.com/technology/software/products/oem/htdocs/agentsoft.html`

2. Copy the downloaded file to the `<OMS_HOME>/sysman/agent_download/10.2.0.3.0` directory.

> **Note:** Create the `<OMS_HOME>/sysman/agent_download/10.2.0.3.0` directory, if it does not exist.

3. Go to this directory by executing the following:

   ```
   cd <OMS_HOME>/sysman/agent_download/10.2.0.3.0
   ```

   When you are here, confirm that the size and checksum calculation of the downloaded file match the information specified on the OTN download page.

4. Execute the following command:

   ```
   unzip <platform>_Grid_Control_agent_download_10_2_0_3.zip
   ```

5. If the agent_download.rsp file does not exist in the `<OMS_HOME>/sysman/agent_download/10.2.0.3.0` directory, do the following:

   1. Execute `mv agent_download.rsp.bak agent_download.rsp`
   2. Edit agent_download.rsp and modify `s_OMSHost="REPLACE_WITH_OMS_HOST"` and `s_OMSPort="REPLACE_WITH_OMS_PORT"` variables with the correct OMSHost and OMSPort values. For example:

      ```
      s_OMSHost="foo.us.oracle.com"
      s_OMSPort="4889"
      ```

      > **Note:** Even if you are specifying a secure Management Service, you must still enter the non-secure port number here.

6. Download the `agentDownload` script by using cp, rcp, scp, FTP, or wget utility.

   An example of using `wget` is as follows:

   ```
   wget http://foo:4889/agent_download/10.2.0.3.0/linux/agentDownload.linux
   ```

7. Run the following command:

   ```
   chmod +x agentDownload.linux
   ./agentDownload.linux -b <name of the Oracle Homes> -m <fully-qualified Oracle
   Management Service host name> -r <Oracle Management Service ports>
   ```

   For example:

   ```
   ./agentdownload.linux - b /oracle/agentinstall -m foo.us.oracle.com -r 4889
   ```

   For clusters, use the following command:

   ```
   ./agentdownload.linux - b /oracle/agentinstall -m foo.us.oracle.com -r 4889 -c
   "host1,host2,host3" -n myCRS -l
   ```

   To view more options, use the `./agentdownload.linux -h` command.

To obtain agentdownload for Windows:

Follow the instructions below, to download the agent installation software for Windows:

1. Download the `Win32_Grid_Control_agent_download_10_2_0_3.zip` file from OTN:

   ```
   http://www.oracle.com/technology/software/products/oem/htdocs/agentsoft.html
   ```

2. Copy the downloaded file to the `<OMS_HOME>/sysman/agent_download/10.2.0.3.0` directory.

   Note: Create the `<OMS_HOME>/sysman/agent_download/10.2.0.3.0` directory, if it does not exist.

3. Go to this directory by executing the following:

   ```
   cd <OMS_HOME>/sysman/agent_download/10.2.0.3.0
   ```

   When you are here, confirm that the size and checksum calculation of the downloaded file match the information specified on the OTN download page.

4. Unzip this file by executing the following:

   ```
   unzip Win32_Grid_Control_agent_download_10_2_0_3.zip
   ```

5. After unzipping, the `agentdownload.vbs` will be available at `<OMSHOME>/sysman/agent_download/10.2.0.3.0/win32/agentdownload.vbs`.

6. Download the `agentDownload.vbs` by using cp, rcp, scp, FTP, or wget utility on the machine where you want to install the Management Agent.

   Note: To download `agentDownload` script using `wget` utility, ensure that the `wget` utility exists on the Windows path variable

   Note: Before executing the `agentDownload.vbs` script, ensure *Windows Script Host version 5.6* is installed on the target agent host. This is required for the script to be executed successfully.

7. Run `agentDownload.vbs` by executing the following:

   ```
   cscript.exe agentDownload.vbs -b /oracle/agentinstall -m foo.us.oracle.com -r
   4889
   ```

   For clusters, use the following command:

   ```
   cscript.exe agentdownload.vbs - b /oracle/agentinstall -m foo.us.oracle.com -r
   4889 -c "host1,host2,host3" -n myCRS -l
   ```

7

Postinstallation Configuration Tasks

This chapter identifies postinstallation configuration tasks you must complete after installation. The following topics are covered in this chapter:

- Running root.sh to Complete the Installation Process (UNIX Only)
- Checking Database Settings
- Accessing the OracleMetaLink Web Site
- Configuring Database and ASM Targets for Monitoring
- Agent Reconfiguration and Rediscovery

7.1 Running root.sh to Complete the Installation Process (UNIX Only)

If you have performed any of the following silent installations, you must run the `allroot.sh` script to complete the installation:

- Enterprise Manager Using New Database

  If you have selected this installation option, you must execute the `allroot.sh` script from the database Oracle home (`db10g`). For example:

  ```
  /scratch/OracleHomes/db10g/allroot.sh
  ```

- Enterprise Manager Using Existing Database

  If you have selected this installation option, execute the `allroot.sh` script from the Management Service Oracle home (`oms10g`). For example:

  ```
  /scratch/OracleHomes/oms10g/allroot.sh
  ```

- Additional Management Service

  If you have selected this installation option, execute the `allroot.sh` script from the Management Service Oracle home (`oms10g`). For example:

  ```
  /scratch/OracleHomes/oms10g/allroot.sh
  ```

Execute the `root.sh` script from the agent Oracle home if you have performed a silent installation of only the Management Agent.

This script finishes the postinstallation steps for the Management Agent, Management Service, and Management Repository database. If you used interactive mode to install Enterprise Manager, you are prompted to run `allroot.sh` or root.sh (depending on the installation type selected) before completing your installation.

On the Management Service machine, run the `root.sh` script as the `root` user from the `$ORACLE_HOME` directory.

Note: For a cluster installation, you must run the `root.sh` script on each host of the cluster on which you installed a Management Agent.

7.2 Checking Database Settings

You may want to check the following settings for your Management Repository database to make sure they are set correctly.

7.2.1 UNDO Tablespace and Temporary Tablespace

Oracle recommends that the Management Repository database have the Tablespace and the Temporary Tablespace set to `UNDO` and `AUTOEXTEND ON`, respectively.

See Also: Managing the UNDO Tablespace chapter of the *Oracle Database Administrator's Guide* for more information.

7.2.2 Archive Logging

Oracle recommends that the Management Repository database have archive logging turned on for any environment where continuity of data is important. Regular backups are also recommended.

7.2.3 Ensure the Database is Not in QUIESCE Mode

Oracle recommends that you do not put the Management Repository database in `QUIESCE` mode. Check your Resource Plan for `INTERNAL_QUIESCE`.

1. Navigate to the Database Home page of your Management Repository.
2. On the Administration property screen, under Resource Manager, click **Resource Plans.**
3. Make sure `INTERNAL_QUIESCE` has not been selected.

In `QUIESCE` mode, only DBA transactions are processed; all other transactions are suspended. Putting the Management Repository database in the `QUIESCE` mode suspends Enterprise Manager transactions.

7.3 Accessing the Oracle*MetaLink* Web Site

You can search Oracle*MetaLink* for Oracle software patches and patchsets, and download these patches or patch sets to an appropriate location in the Management Service Oracle home of Enterprise Manager.

To locate the required patches or patch sets in *MetaLink*:

1. Go to `http://metalink.oracle.com` and navigate to the Patches and Updates screen.
2. Here, you can either perform a simple search with limited parameters, or click **Advanced Search** to perform a more granular (detailed) search. On this screen, you can search for updates based on the patch type (patches or patch sets), product name, platform, patch number, and so on.
3. Specify `emgrid` and click **Search.** The search results display all the patch or patch sets that match the parameters you have specified.

4. Select the appropriate patch or patch set and download it to the Management Service Oracle home location.

7.3.1 Accessing Management Packs

Oracle offers a number of management packs for Oracle Database and Oracle Application Server. For example, management packs available with the Oracle Enterprise Manager 10*g* Release 2 include: Database Change Management Pack, Database Configuration Pack, Database Diagnostics Pack, and Database Tuning Pack. Oracle Application Server supports the following packs: Application Server Configuration Pack and Application Server Diagnostics Pack.

Each pack has several premium features bundled as part of that pack.

The licensable targets (also called parent targets) that are granted access to the packs propagate that access to their dependent targets. For example, all packs that are granted to a database propagate to the host on which the database resides.

For example, if databases D1, D2, and D3 reside on host H1, and the user has access to the Database Tuning pack for database D1, then not only is the D1 database granted access to the Database Tuning pack, but the host H1 is granted access to this pack as well.

You can manage, that is grant and revoke, access to packs for various databases and application servers in your Enterprise Manager repository by using the Management Pack Access option available from the Setup screen. This Management Pack Access function is available only for super administrators.

7.3.1.1 Impact of Management Packs on Targets

Whether a target has access to a pack or not has a very significant impact on the user experience. The corresponding links related to the target, which need the pack, are enabled or disabled accordingly.

To know what packs a screen needs, as well as the links in that screen, click Show Management Pack Information in the screen footer.

When the access to a pack is removed from a target, all corresponding links that need this pack are disabled.

Identifying the Features that Can Be Accessed in Enterprise Manager

When one or more packs on a target monitored by Enterprise Manager are not licensed, access to premium functions for that target is disabled.

For example, the **Blackout** button located on a Target home page (which you can use to move the target to the *blackout* state), is enabled only when either the Oracle Database Diagnostics Pack or the Oracle Application Server Diagnostics Pack is licensed for that target.

To determine the packs used by the current screen and to know what packs need to be licensed for any link on that screen to be enabled, click Show Management Pack Information in the footer of the Enterprise Manager Home page. Enterprise Manager displays this information for all pages you navigate to during that session.

For more information on working with Management Packs, refer to the Enterprise Manager online Help.

7.3.2 Optional Configurations

You can perform the following configuration activities, if required:

7.3.2.1 Specifying the OracleMetaLink Credentials

Enterprise Manager uses Oracle*MetaLink* credentials to search for and download *MetaLink* patches. If you did not specify your Oracle*MetaLink* credentials during installation, you can do the following:

1. On the Enterprise Manager Grid Control Home page, click **Setup.**
2. On the Setup screen, click **Patching Setup.**
3. Specify your Oracle*MetaLink* user name and password in the fields provided.

The URL (`http://updates.oracle.com`) to access the Oracle*MetaLink* Web site appears in the Patch Search URL field on this screen.

Access Oracle*MetaLink* directly by going to the following Web site:

```
http://metalink.oracle.com
```

From this screen, Oracle licensees can register for an account or log in with an existing account. Once logged in, you can search for and download patches.

7.3.2.2 Setting Up Proxy Configuration for the Management Service

If your firewall prevents you from accessing Web sites without the use of an HTTP proxy, then you must set the proxy settings for Enterprise Manager to access Oracle*MetaLink*.

> **See Also:** *Oracle Enterprise Manager Advanced Configuration* for information on configuring Enterprise Manager components, such as Management Agents and Beacons, for use in a firewall environment

If Enterprise Manager is using a proxy server for external access, the following properties must be properly set in the `<OMS_HOME>/sysman/config/emoms.properties` file:

```
proxyHost=www-fooproxy.here.com
proxyPort=80
dontProxyFor=here.com
```

> **See Also:** *Oracle Enterprise Manager Advanced Configuration* for more information on configuring the Management Service properties file

You can also specify domain names that cover all hosts with those domains. For example:

```
dontProxyFor=us.mycompany.com, uk.mycompany.com
```

If the proxy properties are set incorrectly or not set at all, and you try to search for a patch, you receive an error message indicating that Enterprise Manager cannot access the Oracle*MetaLink* Web site.

7.4 Configuring Database and ASM Targets for Monitoring

When you first view the Database Home page for an Oracle Database 10*g* target, the Database Home page may display no monitoring data and the status of the database may indicate that there is a metric collection error. This is because the DBSNMP password has not been configured, or has been locked due to unsuccessful login attempts.

Similarly, the first time you display the home page for an Automatic Storage Management (ASM) target, the status of the ASM instance may be unknown or unavailable, and the home page may indicate that the Management Agent is unavailable (down). Again, this is because you need to supply the ASM SYS password.

> **Note:** You may first need to unlock the DBSNMP user account before setting the monitoring credentials. If the account is not locked, skip Section 10.3.6, "Unlock the DBSNMP User Account" in the next chapter and proceed to Section 10.3.7, "Set Monitoring Credentials" for instructions.

To fix this problem for an Oracle Database target, do the following from the Grid Control console:

1. Unlock the DBSNMP User Account (if necessary).
2. Set Monitoring Credentials.

7.5 Agent Reconfiguration and Rediscovery

The Agent Configuration Assistant (`agentca`) script is used to reconfigure the agent and rediscover the targets on the machine. This script is useful when you want to rediscover a newly added target on the machine or to convert a standalone agent to a Oracle RAC Agent.

You can make use of the following options in the `agentca` script.

Table 7–1 Agent Configuration Assistant Script Options

Option	Description
-n	Specify the cluster name (CLUSTER_NAME).
-c	Specify a comma-separated cluster node list.
-t	Do not start the agent after reconfiguration or target rediscovery.
-d	Rediscover targets.
-f	Reconfigure agents.
-i	Specify the `oraInst.loc` (oracle inventory location). This is required when the Oracle home does not exist in the central inventory.
-h	Get information on all the available options.

> **Note:** You must specify either the `-f` or `-d` option when executing this script. Using one of these two options is mandatory.

> **Caution:** Do not use the `agentca -f` option to reconfigure any upgraded agent (standalone and RAC).

7.5.1 Rediscover and Reconfigure Targets on Standalone Agents

An agent automatically discovers all targets that are installed before the agent installation. Typically, rediscovering of targets is performed when you have installed new targets after an agent installation.

To rediscover new targets, execute `agentca`. The usage is as follows:

```
<Agent_Home>/bin/agentca -d [ -t -i oraInstloc ]
```

7.5.2 Reconfiguring a Standalone Agent to an Oracle RAC Agent

Reconfiguration of a standalone agent occurs when you want to configure this agent (with standalone configurations) as a Oracle RAC agent.

To reconfigure a standalone agent as a Oracle RAC agent, you must execute the `agentca` script with the following options:

```
<Agent_Home>/bin/agentca -f -c "node1,node2…." [-t -i oraInstloc -n CLUSTER_NAME ]
```

Note: The `-c` option must comprise all the nodes (including the local machine) to update the inventory.

7.5.3 Reconfiguring an Existing RAC Agent

If you have added new nodes to an existing Oracle RAC, you can invoke the `agentca` script to automatically reconfigure the existing Oracle RAC agent. The `agentca` script updates the central inventory to add the new nodes information, and also discovers the new targets (if any).

When this script is executed, it takes a back-up of the `EMSTATE` directory on the local machine and creates a new `EMSTATE` directory.

Note: You must run this script on only one node at a time.

To reconfigure an existing Oracle RAC agent, execute `agentca` as follows:

```
prompt> <Agent_Home>/bin/agentca -f  -c "node1,node2,node3....." [-t -i
oraInst.loc -n CLUSTER_NAME]
```

Note: The `-c` option must comprise all the nodes (including the local machine) to update the inventory.

7.5.4 Rediscovering Targets on a Oracle RAC Agent

You can rediscover the new targets that have been installed on Oracle RAC nodes by running the agent configuration assistant with the following options.

```
prompt> <Agent_Home>/bin/agentca -d  -c "node1,node2,node3....." [-t -i
oraInst.loc -n CLUSTER_NAME]
```

Note: The `-c` option must comprise all the nodes (including the local machine) to update the inventory.

Caution: You run this script on only one node at a time.

8

Deploying Cluster Agent

In Enterprise Manager Grid Control 10*g* Release 2 (10.2.0.2), the agent installation is supported both on Oracle Clusterware as well as 9.2 clusters. The Management Agent can be installed as a standalone agent on each node of a cluster individually, or can be installed on multiple nodes in one single installation by choosing the cluster option.

> **Caution:** The agent Oracle home cannot be installed in an Oracle Cluster Shared File System (OCFS) drive, but is supported on a NAS (Network Attached Storage) drive.

8.1 Installing the Agent on a Release 9.2 Cluster

You can choose to either install a standalone agent on each node individually, or perform a cluster installation of the agent. The following sections discuss the various deployment methods for both options.

8.1.1 Installing a Standalone Agent on a Release 9.2 Cluster Node

You can perform a standalone agent installation using the following deployment methods:

8.1.1.1 Installing a Standalone Agent Using the agentDownload Script

The agent can be installed by executing the `agentDownload` script on one node at a time using the correct arguments. If you want to discover the cluster targets, then you must set the `CLUSTER_NAME` environment variable prior to executing the `agentDownload` script, or pass the cluster name to the `agentDownload` script as `agentDownload -n <clustername>`.

```
agentDownload -b <Oracle Base Directory location> -n <clustername>
```

> **Note:** If the `CLUSTER_NAME` environment variable is not set, the agent cannot discover any cluster targets.

8.1.1.2 Installing a Standalone Agent Using the Agent Deploy Application

To perform a standalone agent installation on a cluster node, you must select the appropriate node of that cluster. If you want to discover the cluster targets, you must specify the correct cluster name in the Cluster Name text box. See Section 6.2.3.1, "Fresh Installation of the Management Agent" for detailed instructions.

Note: Ensure the nodes that you select for the agent installation are part of the cluster that you have specified in the Cluster Name text box. Otherwise, the targets are not discovered.

8.1.1.3 Installing a Standalone Agent Using Oracle Universal Installer

You can perform this installation by invoking the installer using Oracle Universal Installer (OUI). The Interactive type is typically a one-node installation.

If the agent is installed as a standalone agent on a release 9.2 cluster, then you can set the `CLUSTER_NAME` environment variable to the name of the cluster that you want to use for the cluster targets before invoking the `runInstaller` script. If this variable is not set, the agent cannot discover any cluster targets.

8.1.2 Installing a Cluster Agent on a Release 9.2 Cluster

You can perform a cluster agent installation using the following deployment methods:

8.1.2.1 Installing a Cluster Agent Using the agentDownload Script

You can perform a cluster agent installation through this script by using the `-c` option (for example, `-c "node1,node2,..."`). This option helps install the cluster agent on all the nodes that you specify here.

If you want to override the cluster name that appears in `targets.xml`, then you must set the `CLUSTER_NAME` environment variable prior to executing the `agentDownload` script, or pass the cluster name to the `agentDownload` script as `agentDownload -b <Oracle Base Directory location> -n <clustername> -c "node1,node2,node3"`.

8.1.2.2 Installing a Cluster Agent Using the Agent Deploy Application

To perform a cluster agent installation using the Agent Deploy application, you must select the Cluster Install option and specify all the nodes of that cluster. If you want to discover the cluster targets, you must specify the correct cluster name in the Cluster Name text box. See Section 6.2.3.1, "Fresh Installation of the Management Agent" for detailed instructions.

8.1.2.3 Installing a Cluster Agent Using the Interactive Installer

To install an agent on a release 9.2 cluster that is on multiple nodes at a time, you must pass the `CLUSTER_NODES` variable when starting executing the `runinstaller` script as:

```
./runInstaller CLUSTER_NODES="{node1,node2}"
```

If the `CLUSTER_NODES` variable is not passed, the installer cannot detect the nodes and cannot perform the cluster install.

If you want to set the cluster name that appears in the `targets.xml` file, you must set the `CLUSTER_NAME` environment variable before invoking the `runInstaller`. If this variable is not set, the agent uses the first node as the cluster name.

8.2 Installing the Agent on Oracle Clusterware

You can choose to either install a standalone agent on each Oracle Clusterware node individually, or perform a cluster installation of the agent. The following sections discuss the various deployment methods for both options.

8.2.1 Installing a Standalone Agent on Oracle Clusterware

You can perform a standalone agent installation on Oracle Clusterware using the following deployment methods:

8.2.1.1 Installing a Standalone Agent Using agentDownload Script

The agent can be installed by executing the `agentDownload` script on one node at a time using the correct arguments. If you want to override the cluster name to be used in `targets.xml` file, you must set the `CLUSTER_NAME` environment variable prior to executing the `agentDownload` script, or pass the cluster name to the `agentDownload` script as `agentDownload -n <clustername>`.

```
agentDownload -b <Oracle Base Directory location> -n <clustername>
```

> **Note:** If the `CLUSTER_NAME` environment variable is not set or passed, the agent uses the cluster name that was specified during the Oracle Clusterware installation.

8.2.1.2 Installing a Standalone Agent Using the Agent Deploy Application

To perform a standalone agent installation on a cluster node, you must select the Cluster Install option, and specify the appropriate cluster node names. The cluster name that you specify here overrides the corresponding value in the `targets.xml` file. See Section 6.2.3.1, "Fresh Installation of the Management Agent" for detailed instructions.

8.2.1.3 Installing a Standalone Agent Using Oracle Universal Installer

You can perform this installation by invoking the installer using Oracle Universal Installer (OUI).

If you want to set the cluster name that will appear in `targets.xml` file, then you must set the `CLUSTER_NAME` environment variable before invoking the `runInstaller`. If this variable is not set, the agent uses the cluster name that was specified during the Oracle Clusterware installation.

8.2.2 Installing a Cluster Agent on Oracle Clusterware

You can perform a cluster agent installation using the following deployment methods:

8.2.2.1 Installing a Cluster Agent Using the agentDownload Script

You can perform a cluster agent installation through this script by using the `-c` option (for example, `-c "node1,node2,..."`). This option helps install the cluster agent on all the nodes that you specify here.

If you want to override the cluster name that appears in `targets.xml` file, then you must set the `CLUSTER_NAME` environment variable prior to executing the `agentDownload` script, or pass the cluster name to the `agentDownload` script as `agentDownload -b <Oracle Base Directory location> -n <clustername> -c "node1,node2,node3"`.

> **Note:** If the `CLUSTER_NAME` variable is not set or passed, the agent uses the cluster name that was specified during the Oracle Clusterware installation.

8.2.2.2 Installing a Cluster Agent Using the Agent Deploy Application

To perform a cluster agent installation using the Agent Deploy application, you must select the **Cluster Install** option and specify all the nodes of that cluster. If you want to override the cluster name that appears in `targets.xml` file, you must specify the appropriate cluster name in the application. See Section 6.2.3.1, "Fresh Installation of the Management Agent" for detailed instructions.

8.2.2.3 Installing a Cluster Agent Using Oracle Universal Installer

When you execute the `runInstaller` script, it automatically detects all the cluster nodes. You can then choose the nodes on which you want to perform the cluster agent installation.

If you want to override the Cluster name that appears in targets.xml, you must set the `CLUSTER_NAME` environment variable before invoking the `runInstaller`. If this variable is not set, the agent uses the cluster name that was specified during the Oracle Clusterware installation.

8.2.3 Installing Oracle RAC Agent on Windows

When you are performing an Oracle RAC agent installation on the Microsoft Windows platform, only the host and cluster targets will be discovered during the installation.

To discover all other targets, you must execute the following on each node of that cluster:

```
Agent Home>/bin/agentca -d -n <Cluster Name> -c <node name>
```

9

Management Agent Cloning

If you have a master agent installation, you can use this installed agent and clone it on multiple destination Oracle homes.

To clone a Management Agent, perform the following steps:

1. Install the Agent on a host using any of the deployment methods discussed in this chapter.
2. Zip the agent Oracle home that you want to clone (for example, `agent.zip`).
3. Perform a file transfer (FTP) of this zipped Oracle home onto the destination host (for example, `ftp agent.zip`).
4. In the destination host, unzip the agent Oracle home.
5. Go to `$ORACLE_HOME/oui/bin/` directory and execute the following command:

   ```
   ./runInstaller  -clone -forceClone ORACLE_HOME=<full path of Oracle home>
   ORACLE_HOME_NAME=<Oracle home name> -noconfig -silent
   ```

   > **Note:** The cloned agent is not in the secure mode by default. You must manually secure the agent by executing `<Oracle_Home>/bin/emctl secure agent`.

6. Execute the following script to run the Agent Configuration Assistant (`agentca`):

   ```
   $ORACLE_HOME/bin/agentca -f
   ```

   > **Caution:** After the cloning process is complete, you must execute the `root.sh` script from the destination agent Oracle homes.

Part III

Postinstallation Configuration

This part discusses the postinstallation configurations that you must complete after successful installation. It also provides information on the ready-to-use Enterprise Manager configurations, along with the instructions to customize your grid environment.

Part 3 contains the following chapters:

- Chapter 7, "Postinstallation Configuration Tasks"
- Chapter 10, "Getting Started with Enterprise Manager"

10

Getting Started with Enterprise Manager

After the Enterprise Manager installation, the Management Service and Grid Control are automatically started. You can immediately log in to Grid Control with the SYSMAN account and begin using Enterprise Manager.

This chapter describes Enterprise Manager's ready-to-use configuration, recommends the tasks to be performed after installation to begin customizing Enterprise Manager for your particular environment, and contains information on how to configure the Management Agent and Management Service. The following topics are covered in this chapter:

- Enterprise Manager's Ready-To-Use Configuration
- Using the Enterprise Manager Grid Control Console for the First Time
- Controlling the Management Repository, Service, and Agent

10.1 Enterprise Manager's Ready-To-Use Configuration

At install time, the following tasks are automatically performed, with no user interaction required:

- The default super administrator SYSMAN account is created with the password you specified.
- The SYSMAN account is automatically configured to receive e-mail notifications if you provided the e-mail notification settings at installation time.
- E-mail notifications are set up with default Notification Rules for the critical conditions.
- Supported targets located on the same host machine as the Management Agent are automatically discovered.

10.1.1 Default Super Administrator: SYSMAN

A default super administrator account, SYSMAN, is created with the password you specified during the installation. After installation, you can immediately log in to the Grid Control Console with this user name and password to perform management tasks. The SYSMAN account owns the database schema containing the Management Repository.

> **See Also:** *Setting Up Enterprise Manager for Your Environment* chapter of *Oracle Enterprise Manager Concepts* to learn more about the SYSMAN user account

10.1.2 E-mail Notifications

The SYSMAN account is automatically configured to receive e-mail notifications from Enterprise Manager if, during installation, you specified the Outgoing (SMTP) Mail Server and SYSMAN e-mail address. Also, as part of the self-monitoring feature, a script is created that enables the user to be notified by e-mail in the event that Enterprise Manager stops unexpectedly.

> **Note:** If you do not specify the mail server, there will be no notification. If you specify the mail server, but not the e-mail address, the system is set up to send e-mail notifications, but the SYSMAN account does not receive any notifications. If you did not specify the information during installation, you can set up e-mail notification afterwards using Enterprise Manager Grid Control.

10.1.3 Notification Rules

E-mail notifications are set up with default Notification Rules for the critical conditions that could occur for all supported target types. For example, for the database target type, a rule is created such that e-mail notifications are sent when any database becomes unavailable, or if any of its key performance metrics (Datafile Usage percentage, Archiver Hung Error Stack, Tablespace Space Used%, and others) becomes critical. The e-mail notifications are sent to the e-mail address associated with the SYSMAN account. These rules are public; when other administrators are created, they can subscribe to them later.

> **See Also:** For more information on the notification rules, in Enterprise Manager, click **Preferences,** then **Rules.** Click **Help** on that page.

10.1.4 Automatic Discovery

The first time the Management Agent is started, most supported targets that are located on the same host machine as the Management Agent are automatically discovered, and default monitoring levels and data collections are automatically enabled.

All targets, such as Oracle Collaboration Suite targets, Web applications, clusters, and Beacons are discovered automatically during the installation phase itself. But, you must manually discover the targets that have been installed after the Management Agent installation.

> **Caution:** If you are performing an Oracle RAC agent installation on Microsoft Windows, only the host and cluster targets are discovered (automatically) during the installation phase. To discover all other targets, you must execute the following command on each node:
>
> ```
> <AGENT_HOME>/bin/agentca -d
> ```

See Also:

- Section 1.4.2.4, "Certified Enterprise Manager Targets" for a list of certified targets for Enterprise Manager Grid Control
- *Managing Oracle Collaboration Suite* available on Oracle Technology Network, for instructions on discovering Oracle Collaboration Suite targets
- Adding Targets to Be Monitored and Administered by Enterprise Manager in the Oracle Enterprise Manager online Help for information on manual discovery

10.1.4.1 Troubleshooting Issues Concerning Target Discovery

If you are unable to discover targets on a Management Agent host, check for the following problems.

When the Management Agent is installed, an automatic discovery is performed to detect any existing Oracle9*i* Application Server release 9.0.2 or 9.0.3 instances. If the 9.0.2 or 9.0.3 Oracle9*i*AS instances were installed by a different OS user than the user that installs the Management Agent, then the file protections on `targets.xml` file within that Oracle9*i* Application Server installation may prevent the Management Agent from reading the file. This prevents the discovery of that Oracle9*i* Application Server instance.

To confirm that this is the problem, check the Management Agent logs located at `AGENT_HOME/sysman/log/` for *permission denied* errors, where `AGENT_HOME` is the Oracle home for the Management Agent. To correct the problem, set the file permissions so that it can be read by the user who installed the Management Agent.

This problem does not occur when discovering other existing Oracle Application Server versions on a machine.

See Also: Section 7.4, "Configuring Database and ASM Targets for Monitoring" for more information, if you encounter problems monitoring Oracle Database 10*g* or ASM targets

10.2 Using the Enterprise Manager Grid Control Console for the First Time

Enterprise Manager Grid Control provides a Web-based console for managing your entire enterprise.

The first column describes actions that you may want to perform; the second contains considerations and reasons for performing the action; the third helps you navigate to the appropriate online Help page in Enterprise Manager.

All Help topics are contained within the Setting Up Enterprise Manager directory of the online Help.

10.2.1 Enabling or Disabling the Licensed Function

Before you begin using Enterprise Manager Grid Control, you must first set the access levels according to your licensing agreement with Oracle. To do this, perform the following steps using a super administrator account, such as SYSMAN.

1. After you log in using SYSMAN, in the Grid Control console, click **Setup,** then **Management Pack Access.**

2. Select **Grant Access** or **Remove Access** for each pack, according to the terms of your licensing agreement.
3. Click **Apply** to save your changes. Once access is removed, the function associated with the selected pack is no longer available for any targets managed by Enterprise Manager Grid Control.

10.3 Controlling the Management Repository, Service, and Agent

The Management Service and the Grid Control console are automatically started after the Enterprise Manager installation. This section provides information on how to manipulate the Management Agent and Management Service after installation.

See Also:

- *Understanding the Directory Structure* section of *Oracle Enterprise Manager Advanced Configuration* for information on Enterprise Manager's directory structure
- *Oracle Enterprise Manager Advanced Configuration* for information on configuring Enterprise Manager components, such as Management Agents and Beacons for use in a firewall environment

10.3.1 Starting the Management Repository Database

If you need to start the Management Repository database, use SQL*Plus to connect to Oracle as SYSDBA, and then issue the `STARTUP` command.

Caution: During a restart of a machine, the repository database startup script runs automatically only if you have performed the Enterprise Manager installation using a new database.

For all other Enterprise Manager installation types, you will have to manually start the repository database on reboot.

See Also:

- *Maintaining and Troubleshooting the Enterprise Repository* chapter of *Oracle Enterprise Manager Advanced Configuration* for instructions on managing the repository database, such as how to drop the repository schema
- *Starting Up and Shutting Down* chapter in the *Oracle Database Administrator's Guide* for detailed instructions on starting up a database

10.3.2 Starting and Stopping the Management Service

The relevant `emctl` commands are listed in Table 10.1.

You must be in the `OMS_HOME/bin` directory to issue the `emctl` commands, where `OMS_HOME` is the Oracle Application Server home directory in which the Management Service is installed and deployed.

Note: To execute the `opmnctl` commands, you must be in the `OMS_HOME/opmn/bin` directory.

Table 10–1 Commands to Start and Stop Management Service

If you want to	Enter the following command
Start the Management Service	`emctl start oms`
Stop the Management Service	`emctl stop oms`
Verify status of the Management Service	`emctl status oms`
Verify status of all OPMN processes	`opmnctl status`
Start all components of Oracle Application Server, including Management Service and Web Cache	`opmnctl startall`
Stop all components of Oracle Application Server, including Management Service and Web Cache	`opmnctl stopall`

Note: Use the same `emctl` commands on Microsoft Windows as well, to perform the above-mentioned actions. Optionally, you can use `emctl.bat` and `opmnctl.bat` on Microsoft Windows, though the extension is not mandatory.

Caution: During a reboot of a machine, the Management Service startup script runs automatically to start the OMS only if you have performed the Enterprise Manager installation using a new database. In this case, you do not have to manually start the OMS.

For all other Enterprise Manager installation types, you will have to manually start the OMS on reboot.

See Also: Starting and Stopping Enterprise Manager Components section of the *Introduction to Enterprise Manager Advanced Configuration* chapter of *Oracle Enterprise Manager Advanced Configuration* at

`http://otn.oracle.com/documentation/oem.html`

10.3.3 Starting and Stopping the Management Agent

The relevant `emctl` commands for UNIX are listed in Table 10.2.

You must be in the `<AGENT_HOME>/bin` directory to issue the `emctl` commands, where AGENT_HOME is the Oracle home directory for your Management Agent. Note that this directory is different than the `<AS_HOME>/bin` directory, which is for the Oracle Application Server Control Agent.

Table 10–2 Commands to Start and Stop Management Agent

If you want to	Enter the following command
Start the Management Agent	`emctl start agent`

Table 10–2 (Cont.) Commands to Start and Stop Management Agent

If you want to	Enter the following command
Stop the Management Agent	`emctl stop agent`
Verify status of the Management Agent	`emctl status agent`

Note: On Microsoft Windows, the services are started automatically by the operating system.

Caution: During a restart of a machine, the agent startup script runs automatically to start the Management Agent only if you have performed the Enterprise Manager installation using a new database, or have installed only the Management Agent.

For all other Enterprise Manager installation types, you will have to manually start the agent when you restart the machine.

See Also: Starting and Stopping Enterprise Manager Components section of the *Introduction to Enterprise Manager Advanced Configuration* chapter of *Oracle Enterprise Manager Advanced Configuration* at:

`http://otn.oracle.com/documentation/oem.html`

10.3.4 Starting the Oracle Application Server Console

Oracle Application Server Control console is the Web-based management tool for Oracle Application Server and is used to monitor the Enterprise Manager targets.

After successful Enterprise Manager installation, you must manually start the Application Server console before starting the Enterprise Manager console.

To start the Application Server console, go to the Management Service Oracle home and execute the `start iasconsole` command. The usage is as follows:

```
<OMS_HOME>/bin/emctl start iasconsole
```

10.3.5 Accessing Enterprise Manager Grid Control

The Enterprise Manager Grid Control console is the primary tool for managing your Oracle environment.

Use the following URL to log in to the Grid Control console:

```
http://<oms_hostname>.<domain>:<port>/em
```

or

```
https://<oms_hostname>.<domain>:<port>/em
```

If you are uncertain about the port number, you can refer to one of the following files:

- `ORACLE_HOME/install/setupinfo.txt` as displayed by Oracle Universal Installer at the end of the installation
- `ORACLE_HOME/install/portlist.ini` on the Management Service machine

- `<OMS Home>/sysman/config/emoms.properties`

  Here, check the `properties` `oracle.sysman.emSDK.svlt.ConsoleServerPort` and `oracle.sysman.emSDK.svlt.ConsoleServerHTTPSPort` for unsecure and secure ports respectively.

When the login dialog box appears, enter the user name and password for the super administrator SYSMAN.

See Also:

- *Enterprise Manager Security* chapter of *Oracle Enterprise Manager Advanced Configuration* for more information on Grid Control security
- Viewing a Summary of the Ports Assigned During the Application Server Installation section of the *Configuring Firewalls* chapter of *Oracle Enterprise Manager Advanced Configuration* for more information on port settings
- *Viewing and Modifying Application Server Port Assignments* in the Enterprise Manager online Help.

10.3.6 Unlock the DBSNMP User Account

To unlock the DBSNMP user account:

1. From the Grid Control console, navigate to the Database Home page and click **Administration** to display the list of administration functions.
2. Under Users and Privileges, click **Users** to display the list of all user accounts. If you are prompted to log in to the database, make sure to use a database user account with DBA privileges such as SYSTEM.
3. Find and select the DBSNMP user account, select **Unlock User** from the Actions menu, and click **Go** to confirm your choice.
4. Set the DBSNMP password as described in the Section 10.3.7, "Set Monitoring Credentials" section. Once the password is set, monitoring can begin.

10.3.7 Set Monitoring Credentials

You must reset the monitoring credentials for database and ASM targets if the passwords you specified during installation were different from the defaults that Enterprise Manager expects. If you change a password at any time, make sure to update all components using that password as well.

This section contains the following subsections:

- Setting Monitoring Credentials for Database Targets
- Setting Monitoring Credentials for ASM Targets

10.3.7.1 Setting Monitoring Credentials for Database Targets

To set the monitoring credentials for a single-instance or cluster Oracle Database 10*g* target:

1. From the Grid Control console, navigate to the Configure Database: Properties page:
   a. On the **Targets** tab, click **Databases** to display the list of database targets.
   b. Find and select the database target and click **Monitoring Configuration.**

Enterprise Manager displays the Configure Database: Properties page.

2. Enter the correct password for the DBSNMP user in the **Monitor Password** field and click **Test Connection** to verify the monitoring credentials.
3. If the connection is successful, click **Next,** then click **Submit.**

You should now be able to view the complete Database Home page for the Oracle Database 10*g* target. For more information, see *Specifying New Target Monitoring Credentials* in *Oracle Enterprise Manager Advanced Configuration*.

10.3.7.2 Setting Monitoring Credentials for ASM Targets

Note: You must ensure the DBSNMP password that is required to monitor database targets is correctly set, before proceeding to set the monitoring credentials for the Automatic Storage Management targets.

To set the monitoring credentials for an ASM target:

1. From the Grid Control console, click **All Targets** on the **Targets** tab to display a list of all managed targets.
2. Find and select the ASM target that you want to modify.
3. Click **Configure** to display the ASM Monitoring Configuration page.
4. Enter the ASM SYS password in the **Password** field and click **OK.**

You should now be able to view the complete home page for the ASM target without any Management Agent or collection errors. For more information, see *Specifying New Target Monitoring Credentials* in *Oracle Enterprise Manager Advanced Configuration*.

Part IV

Enterprise Manager Upgrade

This part provides the requirements and step-by-step instructions on the Enterprise Manager upgrade process.

Part 4 contains the following chapter:

- Chapter 11, "Upgrading Enterprise Manager Grid Control"

11

Upgrading Enterprise Manager Grid Control

Oracle recommends reading this chapter to get a better understanding of the requirements for an Enterprise Manager upgrade.

Oracle Enterprise Manager Grid Control consists of three major components:

- Repository Database
- Management Service
- Management Agent

With the option of deploying the Grid Control environment across the enterprise and in any number of permutations, upgrading the entire environment becomes a very complex activity involving updating of software and configurations in different levels (tiers) located in different machines.

The Enterprise Manager Upgrade process aims at simplifying this entire operation and rendering it as seamless and error-free as possible.

The following topics are covered in this chapter:

- Software Prerequisites
- Checks to Be Performed Before Starting the Upgrade
- Upgrade Scenarios
- Enterprise Manager Upgrade

11.1 Software Prerequisites

Grid Control release 10.2 installer only upgrades the corresponding Enterprise Manager release 10.1 components. Table 11.1 lists the supported component versions:

Table 11–1 Supported Component Versions that Correspond to the Installation Type

Installation Type	Management Service Version	Database Version
Enterprise Manager Using New Database	10.1.0.4 and later (with Application server 9.0.4)	9.0.1.5
Enterprise Manager Using Existing Database	10.1.0.4 and later (with Application server 9.0.4)	9.2.0.6 or higher
Additional Management Service	10.1.0.4 and later (with Application server 9.0.4)	containing the 10.1.0.4 or higher Management Service schema
Additional Management Agent[1]	Not Applicable	Not Applicable

[1] The supported Management Agent version is 10.1.0.3 and later.

11.2 Checks to Be Performed Before Starting the Upgrade

This section lists the checks that you must perform before starting any of the Enterprise Manager release 10.2 upgrade scenarios discussed in the following sections.

11.2.1 Shut Down Enterprise Manager Before Upgrade

You must ensure that the existing Enterprise Manager processes are shut down before starting the upgrade process.

To shut down Enterprise Manager, execute the following commands:

```
<OMS Oracle_Home>/opmn/bin/opmnctl stopall
<AGENT_HOME>/bin/emctl stop agent
<OMS Oracle_Home>/bin/emctl stop em
```

> **Note:** Ensure you shut down all instances of the Management Service that are uploading to the same repository.

These commands usually successfully shut down all Enterprise Manager processes that are running. However, there may be instances where some processes might still be left running. Such instances may cause the upgrade to fail. To avoid this, you must ensure the following processes are not running before attempting to start the upgrade process:

- OPMN
- DCM

> **Note:** Ensure that all Management Service instances uploading to the same repository are shut down before the upgrade. Such Management Service instances must be upgraded simultaneously.

11.2.2 Check for Symbolic Links

The `<Oracle_Home>/Apache/<component>` configuration files must be examined to ensure only hard links (and *no symbolic links*) were referenced.

As part of the Enterprise Manager 10*g* Release 2 (10.2) Upgrade from 10.1, the underlying Oracle9*i*AS release 9.0.4 stack is also upgraded. During this phase, the upgrade utility attempts to replace the 10*g* Release 1 Oracle home path that is referenced in these configuration files with the new Enterprise Manager 10*g* Release 2 `ORACLE_HOME` path.

If you have customized the Oracle9*i*AS release 9.0.4 stack using symbolic links to the Oracle home, then the configuration files may also contain these references as symbolic links, instead of the complete path of the Oracle home.

For example, `<Oracle_Home>/Apache/modplsql/conf/plsq.conf` contains references to the `plsql_module`. If this path is a symbolic link, you must modify this path to be a hard link.

11.2.3 Customizations and User Permissions

If there have been any middle-tier customizations files that cannot be accessed using the upgrade user's credentials, ensure such customizations are removed or

commented out before starting the upgrade. You can reapply these customizations after the upgrade is successfully completed.

Also ensure you (use performing the upgrade) have read and write permissions on `/temp/em`.

11.2.4 Recompile EMD_MAINTENANCE for Manually Upgraded Databases

If you have previously upgraded the database (from 9*i* to 10*g*) manually, you must recompile the `EMD_MAINTENANCE` package. To do this:

1. Shut down the Management Service that is associated with the database.
2. Execute SQLPLUS into the upgraded database as SYSMAN.
3. Execute alter package EMD_MAINTENANCE COMPILE BODY; ensure this package has been recompiled successfully.
4. Now, start the management Service.

11.2.5 Verify Inventory.xml for Oracle Home Path

Ensure the `<Oracle_Inventory>/ContentsXML/inventory.xml` file to make sure the Oracle home path is the same as the components that you are upgrading.

Note: These paths must always be hardlinks.

11.2.6 Select an Agent that Is Not Secure

During the upgrade process, you can choose not to specify the Agent Registration password. This leaves the upgraded agent unsecure. The installer displays an error message when the agent's `REPOSITORY_URL` does not match with that of the OMS, indicating the agent is not bound to the Management Service.

This can happen if multiple OMSs are grouped together through a load balancer, and the agent is using this load balancer to communicate with the Management Service.

You can also choose to secure the upgraded agent manually after the agent has been upgraded.

11.2.7 Shut Down Database Listener (UNIX Only)

If the current Enterprise Manger installation (10*g* Release 1) was performed using a new database, the 10*g* Release 2 (10.2) upgrade process will first attempt to upgrade Oracle Database if it has not already been upgraded manually.

In an Enterprise Manager Grid Control 10*g* Release 1 (10.1) installation using a new database, the installer performs a release 9.0.1.5 Oracle Database installation along with the other Enterprise Manager components. When you upgrade Enterprise Manager release 10.1 to release 10.2, the database instance is upgraded to a release 10.1.0.4 before the Enterprise Manager migration configuration is performed.

To successfully migrate your existing Enterprise Manager to release 10.2, the new 10.1.0.4 database listener has to be started. To do this, you must simply stop the old (release 9.0.1.5) database listener **just prior** to executing the `allRoot.sh` script.

After you stop the old listener and execute the `allRoot.sh` script, the release 10.1.0.4 listener will be started automatically.

WARNING: Do not shut down the database listener if you are attempting to upgrade an Enterprise Manager installation that was performed using an existing database. The upgrade will fail if the database listener is shut down.

Note: On *Microsoft Windows*, you must modify the start-up type value of the old listener to *Disable*, and the start-up type value of the new listener to *Automatic* after the upgrade process is complete.

11.2.7.1 Impact on Firewall Ports and Software Load Balancers

During an Enterprise Manager upgrade from 10g R1 to 10g R2, there will be some modifications to the default port values.

For example, port 1158 will no longer be used for communications between the Management Service and the agent. similarly, the default port for the Management Service and agent communications will now (in 10*g* R2) be 3872 and not 1830 (as in 10*g* R1) though the 1830 port will still be valid.

The Enterprise Manager upgrade operation will preserve the ports that were being used in the original deployment. Hence, additional ports will not be required even if Enterprise Manager was originally deployed with a firewall.

Similarly, you will not have to perform any modifications to the software load balancer (SLB) configurations after the Enterprise Manager upgrade.

11.3 Manual Configuration to Be Performed For Upgrade

The following sections explain the configuration tasks to be performed for upgrade from Enterprise Manager 10.1.0.4 or higher to 10.2.0.1 (Linux) or 10.2.0.2 (Windows) or higher. Also explained are tasks to be performed before upgrading from Enterprise Manager 10.2.0.1 (Linux) to 10.2.0.2 (Linux) or 10.2.0.3.0.

11.3.1 Tasks to be Performed Before Upgrading from 10.1.0.4 to 10.2.0.1 or 10.2.0.2

The following steps outline the pre-upgrade tasks for manual upgrade from Enterprise Manager 10.1.0.4 or higher to Enterprise Manager 10.2.0.1 (Linux) or 10.2.0.2 (Windows) or higher in addition to the tasks mentioned above.

1. Ensure that there is a successful database backup for 24 hours before performing upgrade.
2. Shutdown all OPMN processes and agents.
3. Perform Enterprise Manager partition cleanup. To do this, log into the database using SQLPLUS with SYSMAN credentials. At the SQL> prompt, execute the following command:

   ```
   SQL>exec emd_maintenance.partition_maintenance;
   ```

4. Apply fix for index/constraint issues. To do this, log into the database using SQLPLUS with SYSMAN credentials. At the SQL> prompt, execute the following commands:

   ```
   SQL>Alter table MGMT_JOB_TYPE_INFO disable constraint PK_JOB_TYPE_INFO cascade
   drop index;
   SQL>Alter table MGMT_JOB_PARAMETER disable constraint PK_MGMT_JOB_PARAM cascade
   ```

```
drop index;
SQL>Alter table MGMT_TARGET_PROP_DEFS  disable constraint MGMT_TARGET_PROP_
DEFS_PK cascade drop index;
SQL> Alter table mgmt_license_definitions  disable constraint mgmt_license_
definitions_pk cascade drop index;
SQL> ALTER TABLE mgmt_annotation DISABLE CONSTRAINT mgmt_annotation_pk cascade
drop index;
```

5. Check and enable the queue `MGMT_NOTIFY_Q` if it is not enabled. To do this, log into the database using SQLPLUS with SYSMAN credentials. At the SQL> prompt, execute the following commands:

```
SQL> select OWNER, NAME, ENQUEUE_ENABLED from dba_queues where name='MGMT_
NOTIFY_Q';
If ENQUENE_ENABLED is NOT "YES", then
exec dbms_aqadm.start_queue(queue_name => 'SYSMAN.MGMT_NOTIFY_Q');
```

11.3.2 Tasks to be Performed For Upgrading from 10.1.0.4 to 10.2.0.1 or 10.2.0.2

To upgrade from Enterprise Manager 10.1.0.4 or higher to Enterprise Manager 10.2.0.1 (Linux) or 10.2.0.2 (Windows) or higher, do the following:

1. Using the shiphome, invoke OUI with `-noconfig` option as follows:

```
./runInstaller -noconfig
```

2. When prompted for upgrade options, choose both Oracle Management Service and Agent for upgrade. Enter valid input values for the installation. OUI will perform a software only install.
3. After the software only install, replace `$ORACLE_HOME/sysman/admin/emdrep/sql/core/v102020/pre_post_creation.sql` with `/net/stadv48/scratch/BUG566424/10.2.0.1/pre_post_creation.sql`.
4. Execute the command to launch the Configuration tool to complete the upgrade. If the older Oracle Management Service was a "No seed or additional Oracle Management Service" installation, run the following command:

```
$NEW_OMS_HOME/oui/bin/runConfig.sh ORACLE_HOME=<OMS HOME> MODE=perform
ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

   If the older Oracle Management Service was a seed installation, run the following command:

```
$NEW_OMS_HOME/oui/bin/runConfig.sh ORACLE_HOME=<OMS HOME> MODE=perform
ACTION=configure COMPONENT_XML={encap_emseed.1_0_0_0_0.xml}
```

11.3.3 Tasks to be Performed Before Upgrading from 10.2.0.1 to 10.2.0.2 or 10.2.0.3.0

To upgrade from Enterprise Manager 10.2.0.1 or 10.2.0.2 to Enterprise Manager 10.2.0.2 or 10.2.0.3.0 respectively, the following manual tasks need to performed before the upgrade:

1. Using the Oracle Management Service patchset, invoke OUI with `-noconfig` option as follows:

```
./runInstaller -noconfig
```

   OUI will perform a software only install.

2. After the software only install, replace `$ORACLE_HOME/sysman/admin/emdrep/sql/core/10.2.0.2/pre_data_upgrade.sql` with `/net/stadv48/scratch/BUG566424/10.2.0.2/pre_data_upgrade.sql`.
3. Execute the command to launch the Configuration tool to complete the upgrade as follows:

```
OMS_HOME/oui/bin/runConfig.sh ORACLE_HOME=<OMS_HOME> ACTION=patchsetConfigure
MODE=perform RERUN=true COMPONENT_XML={oracle.sysman.top.oms.10_2_0_2_0.xml}
```

11.3.4 Tasks to be Performed For Upgrading from 10.2.0.1 to 10.2.0.2 or 10.2.0.3.0

For upgrading from Enterprise Manager 10.2.0.1 to 10.2.0.2 or 10.2.0.3.0 using OUI, follow the steps outlined in Section 11.5.1, "Enterprise Manager Upgrade Using Oracle Universal Installer".

11.4 Upgrade Scenarios

The following upgrade scenarios are discussed in this section:

- Upgrading Oracle Management Service that Is Installed Using a New Database
- Upgrading Management Service that Is Installed Using an Existing Database
- Upgrading the Oracle Management Service
- Upgrading the Management Agent

> **Caution:** During the upgrade process, you must ensure the monitoring agent is also upgraded along with the OMS and repository database.

11.4.1 Upgrading Oracle Management Service that Is Installed Using a New Database

If the Enterprise Manager 10*g* Release 1 (10.1) was of this installation type, then the 10*g* Release 2 (10.2) installer performs an out-of-place upgrade of the release 10.1 Management Service (OMS), the repository database, and the agent Oracle homes. During the upgrade, the installer creates a new Oracle home for the management Service, Repository Database, and Management Agent. The upgrade assistants upgrade the datafiles and `SYSMAN` schema, and then configure the new Oracle homes.

> **Caution:** Before you start the upgrade process on Microsoft Windows, ensure the parameter `SQLNET.AUTHENTICATION_SERVICES` value is NTS (`SQLNET.AUTHENTICATION_SERVICES=NTS`). If this is not done, the Database Upgrade Assistant will fail.
>
> You must also ensure that the listener is running, and the SQL command (`sqlplus "/as sysdba"`) is connecting to the database.

11.4.2 Upgrading Management Service that Is Installed Using an Existing Database

If the earlier Enterprise Manager installation was done using an existing database, the 10*g* Release 2 installer automatically checks the remote database version (must be release 9.2.0.6 or later). If the minimum database version requirement is met, the

installer not only performs an upgrade of the Management Service but also upgrades the `SYSMAN` schema in the remote database.

> **Note:** If the database version is lower than release 9.2.0.6, this database is not upgraded as part of the Enterprise Manager upgrade process. You are required to upgrade the database separately, before proceeding with the Management Service upgrade process.

> **Caution:** If you are upgrading an Enterprise Manager target (for example, database) using an upgrade mechanism other than Oracle Universal Installer, the agent you have selected must also be part of the same installation (is the agent associated with that Management Service). See Section A.4.4, "Monitoring Agent Does Not Discover Upgraded Targets" for more information.

11.4.3 Upgrading the Oracle Management Service

If the previous Enterprise Manager installation was for an additional Management Service, the 10*g* Release 2 installer checks the remote database (must be release 9.2.0.6 or later). If this minimum database release requirement is met, the installer performs the Management upgrade.

If you are upgrading only the Management Service to 10*g* Release 2 (10.2) without upgrading the monitoring agent (agent associated with that Management Service), you may encounter a metric collection error. To resolve this issue, you must upgrade the monitoring agent to 10*g* Release 2 as well.

Oracle recommends upgrading the Management Service and the associated (monitoring) agent at the same time.

> **Caution:** Ensure you shut down the Management Service that you are going to upgrade, and its associated (monitoring) agent before starting the upgrade process.

> **Note:** If the database release is earlier than 9.2.0.6, this database is not upgraded as part of the Enterprise Manager upgrade process. You are required to upgrade the database separately, before proceeding with the Management Service upgrade process.

> **Caution:** After successfully upgrading the 10*g* Release 1 (10.1.0.4) Management Service to release 10.2, the 10.1.0.4 agents that are uploading data to this Management Service may show an incorrect Management Service version when you execute `./emctl status agent`.
>
> To resolve this issue, you must stop the 10.1.0.4 agents (`./emctl stop agent`) and restart them (`./emctl start agent`).

11.4.4 Upgrading the Management Agent

All agent Oracle homes that need to be upgraded are detected and displayed in the Select Install or Upgrade screen of the installer. You can select the agent Oracle homes that you want to upgrade and proceed with the process.

> **Note:** The agent Oracle homes that are installed as part of the first two installation types are not upgraded automatically along with the Management Service (OMS) Oracle homes. You must select the agent home that you want to upgrade. This agent home can be independent of the Management Service home.

11.4.4.1 Upgrading 10.1.0.4 Agents that Monitor User-Defined Metrics

Because the Management Agent upgrade process is an out-of-place[1] installation, upgrading an agent will create a new agent Oracle home directory. If you are using OS-based user-defined metrics that are referencing scripts located in an agent Oracle home, then such scripts will not be copied over during the upgrade process. Specifically, if a release 10.1.0.4 agent is being upgraded to release 10.2 agent, any user-defined metric scripts that may have existed in the 10.1.0.4 agent Oracle home will not be copied into the new 10.2 agent Oracle home.

In order to ensure the user-defined metrics continue to work the same, you must manually copy all user-defined metrics scripts into another directory (outside any Oracle home), and then update the user-defined metric definitions to reflect the new script location.

For example, if the user-defined script is called `myScript.sh` and is located in the 10.1.0.4 agent Oracle home (for example, `/u1/oracle/sysman/admin/scripts` directory), copy this script over to a new directory (for example, `/u1/scripts`). Now, in the definition of the user-defined metric, you must change the command line from `/u1/oracle/sysman/admin/scripts/myScript.sh` to `/u1/scripts/myScript.sh`.

> **Note:** Ensure you do not delete the original Oracle home (that is 10.1.0.4 Oracle home in the preceding example) until you have changed the user-defined metric script location.

11.5 Enterprise Manager Upgrade

When you invoke Oracle Universal Installer to perform an upgrade, it automatically detects the existing Enterprise Manager installation type of the target Oracle homes and displays the components that need to be upgraded. You can select the component that you want to upgrade and proceed with the process.

> **Caution:** Oracle recommends that you perform a backup of the repository before starting the upgrade process.

[1] Out-of-place upgrade refers to the process of installing the software in a new Oracle home. All the data and configuration files from an existing Oracle home are retrieved and migrated to the new Oracle home. After the upgrade is complete, the old Oracle home is discarded and the software can be started from the new Oracle home.

11.5.1 Enterprise Manager Upgrade Using Oracle Universal Installer

Follow these steps to perform an Enterprise Manager upgrade.

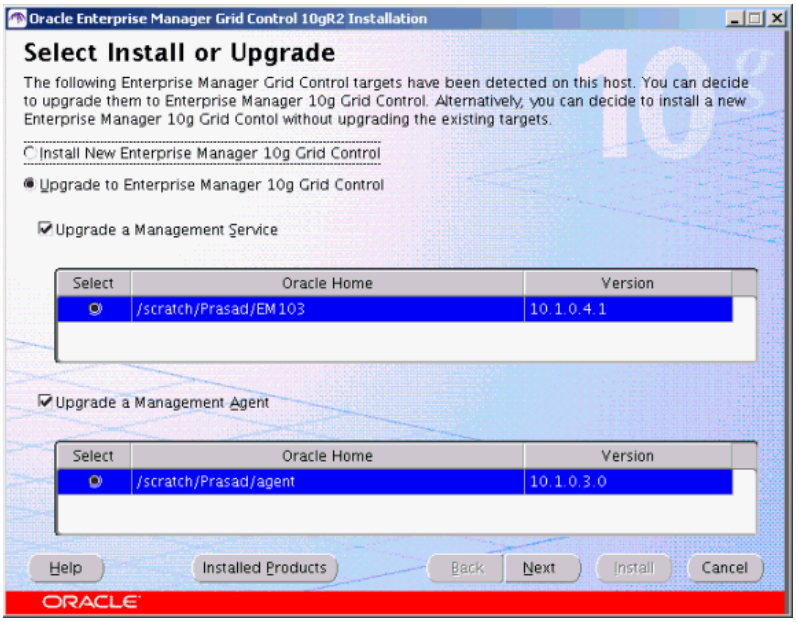
1. Start Oracle Universal Installer by running the `runInstaller` script in Linux (go to the top-level folder in the contents copied from the DVD and execute `./runInstaller` or `setup.exe` on Microsoft Windows) from the top directory of Disk1.
2. When you invoke Oracle Universal Installer, you will be presented with two choices:
   a. Perform a New Enterprise Manager Installation

      See Section 3.3, "Enterprise Manager Installation Types" for more information.

   b. Products Upgrade

      Select this option to continue with the upgrade process.
3. Click **Products Upgrade**. The Select Install or Upgrade screen appears.

Figure 11–1 Select Install or Upgrade



4. The installer automatically detects the Grid Control components that require an upgrade and lists them in this screen.
5. Here, you can choose to perform the following upgrades:
   a. Management Service and the associated (monitoring) Management Agent
   b. Only the Management Service
   c. Only the Management Agent

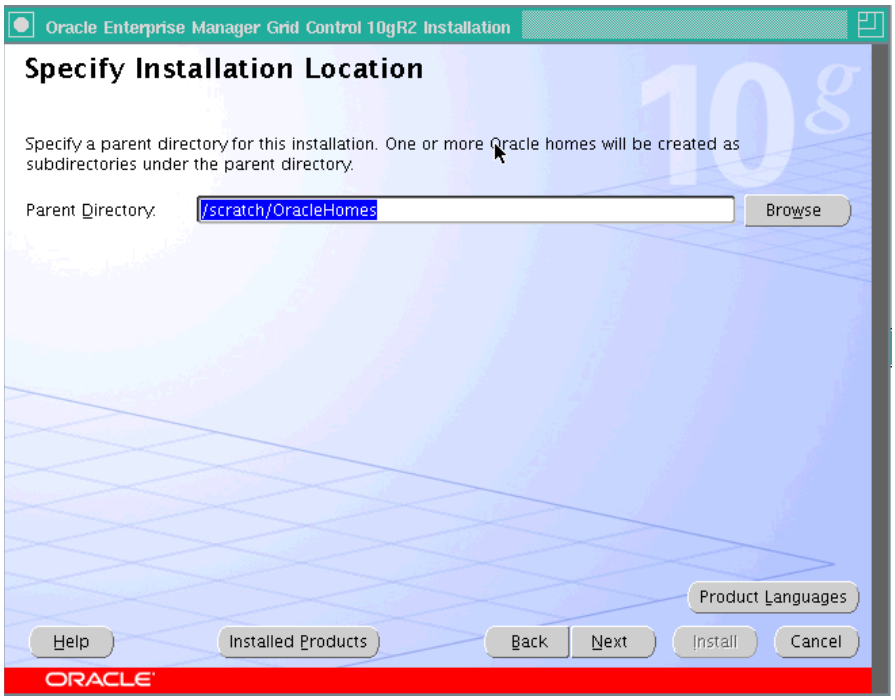
Caution: If you are upgrading both Management Service and Agent (which is part of a chain agent installation), ensure the agent you have selected is the one that is communicating with selected Management Service.

Also, ensure you shut down the agent and the Management Service that you are going to upgrade, before starting the process.

---

6. Select the Oracle homes that you want to upgrade and click **Next**. The Specify Installation Location screen appears.

Figure 11–2 Specify Installation Location

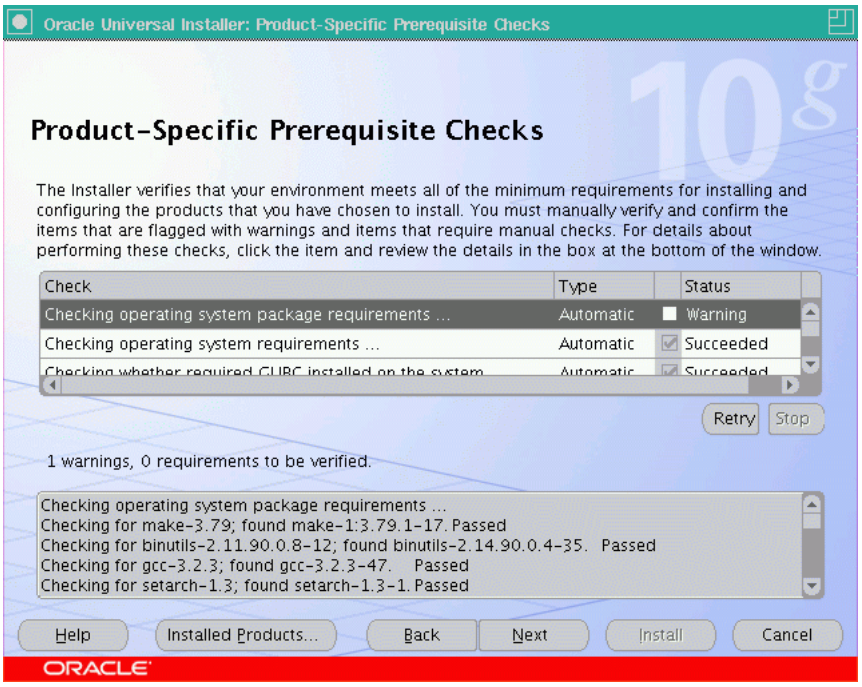


Here, specify a parent directory (base directory), for example, `/scratch/OracleHomes`, for the new installation. because the installer is going to perform an out-of-place[2] upgrade, all the Oracle homes created during the upgrade will be placed as subdirectories under this parent directory.

7. Click **Next**. The Product-Specific Prerequisite Checks screen appears.

[2] Out-of-place upgrade refers to the process of installing the software in a new Oracle home. All the data and configuration files from an existing Oracle home are retrieved and migrated to the new Oracle home. After the upgrade is complete, the old Oracle home is discarded and the software can be started from the new Oracle home.

Figure 11–3 Product-Specific Prerequisite Checks



a. At this point, the installer runs some prerequisite checks to verify whether or not the environment meets the minimum requirements for a successful Enterprise Manager installation.

   Early detection of problems with the system setup reduces the chances of you encountering problems during installation; for instance, problems with insufficient disk space, missing patches, inappropriate hardware, and so on.

   This page displays the check name, type, and status for all prerequisite checks designed for the installation. Automatic checks are run first, followed by optional and manual checks.

   Depending on the status of the automatic checks, you must verify all warning and manual checks. At some point, if you have stopped the prerequisite check and want to rerun these checks, select the checks that you want to rerun and click **Retry**. As each check runs, a progress bar is shown, and test details (expected results, actual results, error messages, instructions) are displayed in the details section, at the bottom of the page.

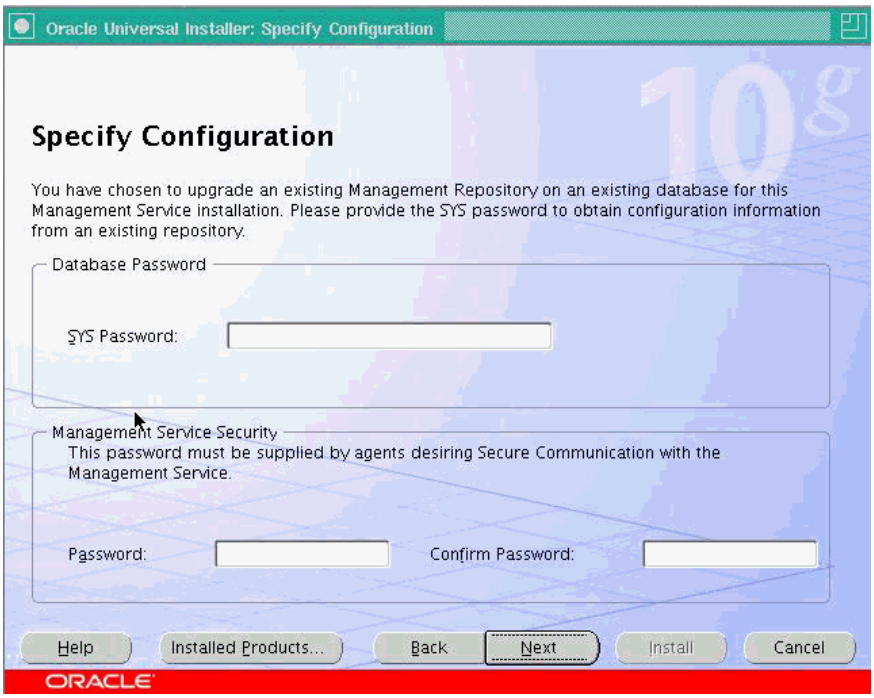
b. To stop all prerequisite checks, click **Stop**. At any point of time, click a prerequisite check to view its corresponding details, including the recommended user actions.

   Note: You must manually verify and confirm all checks that were flagged with a warning, skipped (stopped by user), or failed.

c. To continue with the installation without retrying, click **Next**.

8. The Specify Configuration screen appears.

Figure 11–4 Specify Configuration



a. Here, you must specify the existing Database and Secure Management Service passwords. The Database Password (SYS) is required to access the configuration files of the existing database repository that is associated with the Management Service that you have selected for upgrade.

b. In the Database password section, specify the SYS Password (the default super administrator account) for the existing database repository that is associated with the selected Management Service.

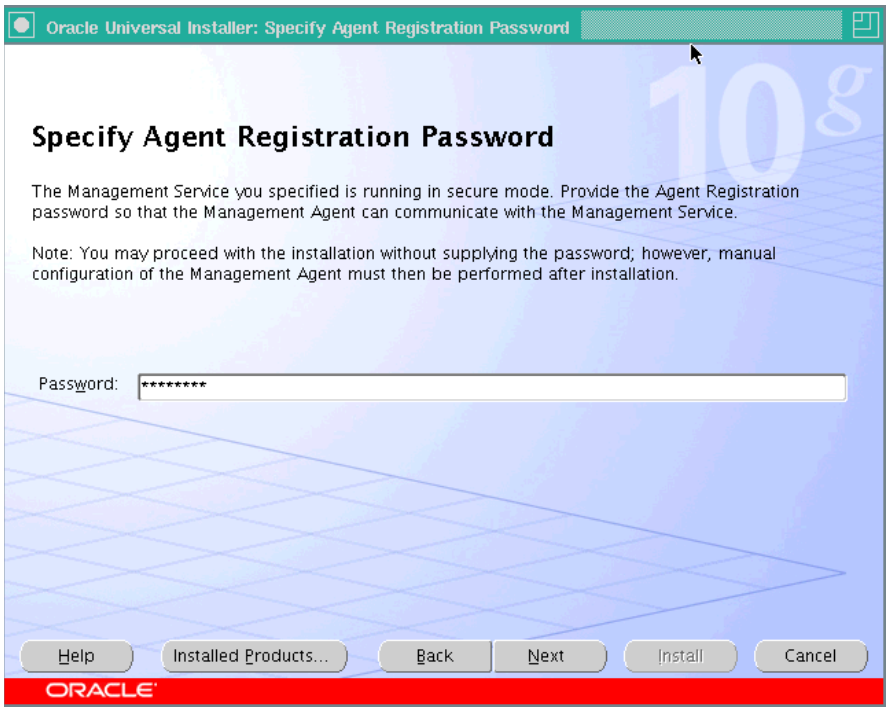
c. In the Management Service Security section, specify a password that will be used to secure the communications between the Management Service and its agents.

Note: Management Service Security: This section is enabled only when the existing Management Service that you are upgrading is not secure.

---

9. Click **Next.** If you are upgrading both Management Service and Agent, but only the existing Management Service is secure and locked, then the Agent Registration Password screen appears. Here, you must provide the correct password to enable communications between the secure Management Service and the agent that you are upgrading.

Figure 11–5 Specify Agent Registration Password



Note: This screen appears only if the base (existing) agent installation is not secure.

Caution: If you do not know the password and choose to leave the Password field blank, you must do the following after installation, to enable secure communication between the agent and Management Service:

1. Find out the correct password for the secure Management Service environment. If you do not know the password, obtain it from the user who configured the Management Service for SSL.
2. In the Agent's <ORACLE_HOME>/bin directory, execute the following command:

   ```
   <AGENT_HOME>/bin/emctl secure agent -reg_passwd <password>
   ```

   The <passwd> argument must be replaced with the Agent Registration Password.

10. The Summary screen appears. This screen displays all the Oracle homes that will be created. Depending on the type of upgrade you have selected, this page will display any of the following details:
    - Global Settings
    - Product Languages
    - Space Requirements
    - New Installations

11. Verify the choices that you have made, and click **Install** to start the upgrade.

11.5.1.1 Upgrade Logs

During the Management Service (OMS) upgrade, the following log files are created:

- `iasua.log`

  The Oracle Application Server stack is upgraded by the OMS Upgrade Plugin. This is performed by invoking the IASUA utility. the iasua.log file is created at the following location:

  ```
  <NEW_OMS_HOME>/upgrade/log/iasua.log
  ```

- `emrepmgr.log.<pid>`

  This log is created during the schema upgrade. The upgrade output log file is located at:

  ```
  <NEW_OMS_HOME>/sysman/log/emrepmgr.log.<pid>
  ```

11.5.1.2 Post-Upgrade Configuration

Perform the following configuration tasks after the upgrade is complete.

11.5.1.2.1 For Oracle Management Service After the Oracle Management Service upgrade is complete, you must do the following:

- Check the `<OMS_HOME>/sysman/log/emrepmgr.log.<pid>` log file and verify whether or not there were any errors.

  > **Note:** There may be more than one `emrepmgr.log.<pid>` file present in the OMS home. Ensure you select the files that were updated most recently.

  In the log files, examine the last line to see whether or not it indicates Repository Upgrade as successfully completed or as having ended in a failure.

  If it shows a failed upgrade, search for any "ORA-" or "compilation" errors.

- After OMS upgrade (regardless of whether or not the agent has been upgraded along with it), you must execute `agentca` with discovery options in order to discover CSA targets.
- You can optionally delete the BC4J target of the old OMS home after the OMS upgrade is complete.
- You must reset the `ias_admin` password after the Management Service upgrade. The `ias_admin` password is set as `welcome1` by default, during the upgrade process.
- If in the Patch Advisories page on the Grid Control console, the patch advisories and affected homes count is showing 0 (zero), do ne of the following:
  - Execute the following SQL as `sysman` and then run the `RefreshFromMetalink` job. This must be done just once after the upgrade process.

    ```
    BEGIN
    MGMT_POLICY.AUTO_ENABLE_EXISTING_TARGETS(
      p_target_type => 'host',
        p_policy_name => 'Critical Patch Advisories for Oracle Homes' );
    ```

```
END;
```

– Go to the Targets tab in the console and click **Hosts.** On this page, click the **Metric and Policy Settings** link for a host. Now, go to the Policies tab and click **Add Policy.** Here, select the CPF policy and associate it to the target.

- After the upgrade, if you find the links under the Web Application tasks tab (under Monitoring Configuration) in the console disabled, it means that the Application Server diagnostics pack is disabled after the upgrade. To work around this issue, do the following:
  1. Identify the system associated with the Web Application Enterprise Manager Web site.
  2. Add the new Application Server target as a member of this system.
  3. Mark the new Application Server target as a key component of the Web Application Enterprise Manager Web site.
- After the upgrade, if the performance graph is missing, do the following:
  1. Go to the Performance Metrics page under Monitoring Configuration.
  2. Add the metric and select the performance graph to be displayed on the home page. Perform similar tasks for the Usage Metrics also.
- You may fin some of the Web site targets in a broken state after the upgrade. They will show up in the All Targets page under the **Targets Not Configured** list. This does not affect their monitoring in any way. Even though the target is in a "non-configured" state, the availability is still computed and al functions remain in working order.

  To prevent these targets from showing up in that list, the user has to run the query provided below, to update a table in the repository. This query must be run after the OMS upgrade is complete.

```
UPDATE MGMT_TARGETS SET broken_reason = 0, broken_str = NULL, emd_url = NULL,
host_name = NULL
  WHERE target_guid IN (SELECT t.target_guid
                          FROM MGMT_TARGET_PROPERTIES p,
                               MGMT_TARGETS t
                         WHERE t.target_guid = p.target_guid
                           AND t.target_type = 'website'
                           AND t.broken_reason != 0
                           AND p.property_name = 'Upgraded'
                           AND p.property_value = '1');

COMMIT;
```

  After this query completes, the targets will not show up in the **Targets Not Configured** list.

11.5.1.2.2 For Oracle Database Upgrade After the Oracle Database upgrade is complete, you must do the following:

- On Microsoft Windows, if you have performed an upgrade on an installation of the type Enterprise Manager Using a New Database, you must manually modify the Listener services to make sure that the old Listener's startup type is set to `Disable`, and the new Listener's startup type is set to `Automatic`.

- There may be instances where the Enterprise Manager Using a New database installation and its subsequent upgrade encounters an abnormal growth of the `ons.log`. This can potentially take up a lot of disk space relatively quickly.

  In such circumstances, you must check whether or not the `ons.log` contains repeated messages such as the following:

  ```
  Local connection 0,127.0.0.1,6100 missing form factor
  ```

  If such an error message is observed in the `ons.log`, perform the following steps:

  1. In the Database Oracle home, rename the $ORACLE_HOME/opmn/conf/ons.config file (in order for the Listener not to find the database to sue it). For example,

     ```
     cd $ORACLE_HOME/opmn/conf
     mv ons.config ons.config.orig
     ```

  2. Restart the Listener.

11.5.1.2.3 For Management Agent After the Oracle Management Agent upgrade is complete, if you find that the Beacon URL Watchlist items do not appear in the collections file, do the following:

1. Go to the Beacon home page.
2. Click **Past Changes.**
3. On this page, click **Sync Beacon.**

11.5.1.3 Enterprise Manager Grid Control Upgrade Diagnostics

This sections details some of the diagnostic checks that you should perform along with their resolutions.

11.5.1.3.1 Management Service Upgrade Stops At IASUA failure Check the appropriate log file to get the facts for this occurrence. The installation dialog and the configuration framework log file is located at:

```
<New_OracleHome>/cfgtoollogs/cfgfw/oracle.sysman.top.oms_#date.log
```

This file will list the SEVERE messages indicating the reason that iASUA (Oracle Application Server Upgrade Assistant) failed to complete successfully. If the message shows that "permission denied" on certain files, that means that the user running the installer may not have the correct privileges to run certain iAS configuration.

To resolve this issue, comments out the iAS configuration that contains these files, and then retry the upgrade again.

11.5.1.3.2 Management Service Upgrade Stops at EMDeploy Failure The most common reasons that EMDeploy would fail are because of some pre-upgrade check list items that were not satisfied. The messages in the log file located at:

```
<New_OracleHome>/cfgtoollogs/cfgfw/oracle.sysman.top.oms_#date.log
```

This file will indicate the reasons for the EMDeploy failures.

You must resolve the issue in accordance with the pre-upgrade check list items, and then retry the upgrade.

11.5.1.3.3 Management Service Upgrade Stops at the Repository Schema Upgrade (RepManager) The most common reason that repository schema upgrade fails is when it is not able to connect to the listener. The log file mentioned below would indicate the reason that repository schema upgrade has failed.

To fix this issue, you must examine whether or not the listener that the OMS connects to is valid and live. If the OMS is of installation type Enterprise Manager Using a New Database, then you should check whether or not the old listener has been stopped, and the new listener has been started. After the listener issue is resolved, you can retry the upgrade process.

The log file is at the following location:

```
$ORACLE_HOME/sysman/log/emrepmgr.log.<pid>
```

You must examine this log file to check whether or not there are any errors.

> **Note:** There may be more than one `emrepmgr.log.<pid>` file present in the OMS home. Ensure you select the files that were updated most recently.

In the log files, examine the last line to see whether or not it indicates Repository Upgrade as successfully completed or as having ended in a failure.

If it shows a failed upgrade, search for any "ORA-" or "compilation" errors.

11.5.2 Upgrading Management Agent Using the Agent Deploy Application

Agent Deploy is a J2EE application that is used for mass deployment of Management Agents.

The Upgrade Agent option in this application will help you upgrade an existing Management Agent installation to a release 10.2 Management Agent.

Accessing the Agent Deploy Application

To access the Agent Deploy application, follow these steps:

1. Log in to the Grid Control console and go to the Deployments page.
2. Click **Install Agent** under the Agent Installation section.
3. In the Agent Deploy Application home page that appears, select the appropriate installation option that you want to perform.

> **Note:** If you want to view the status of an earlier installation/upgrade session, click **Agent Installation Status** in the Deployments page.

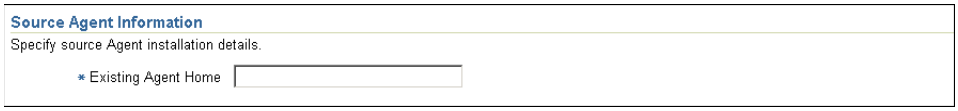
To upgrade the Management Agent using Agent Deploy, follow the instructions documented below:

1. On the Agent Deploy application home page, click **Upgrade Agent** to perform the Management Agent upgrade.
2. The Agent Upgrade: Installation Details page appears.

3. In the Source Agent Information section, specify the full path to an existing agent Oracle home location. This source agent installation will be used to perform the upgrade.

> **Note:** The path of the source agent should be the same on all the remote hosts.

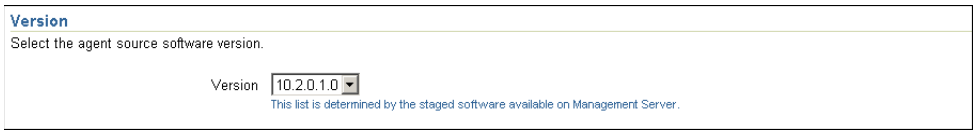
Figure 11–6 Source Agent Information Section of the Installation Details Screen



4. In the Version section of this page, select the appropriate version of the agent software that you want to use for upgrade.

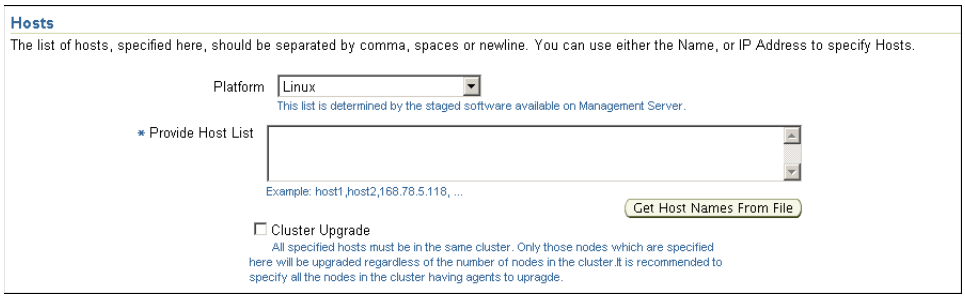
> **Note:** The values in this list will depend on the staged software that are available on the Management Service host.

Figure 11–7 Version Section of the Installation Details Screen



5. In the Hosts section, do the following:

Figure 11–8 Hosts Section of the Installation Details Screen



   a. Select the appropriate platform on which you want to perform this installation.

   b. In the Provide Host List text box, specify all the hosts (host names or IP addresses) on which you want to perform the Agent installation. Alternatively, click **Get Host Names From File** to browse and select the file that contains a list of all the required host names.

WARNING: Do not specify duplicate entries of the host list. If there are duplicate host entries in this list, the application hangs.

Use the same host names for which the SSH has been set.

Note: You can use either a comma (,), white space, or a new line as a separator when specifying multiple hosts.

Caution: The Agent Deploy application picks up only the values in the first column of the Host List file that you specify or select.

Ensure the host list format is appropriate, since the Agent Deploy application does not validate this format on the selected file.

A sample host list format is provided in Table 11–2.

Table 11–2 Sample Host List Format

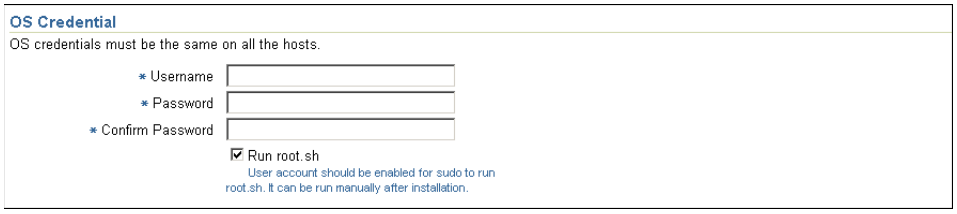
Fully Qualified Host name	Host name	Host IP Address
host1.foo.com	host1	154.87.3.229
host2.foo.com	host2	154.87.3.109
host3.foo.com	host3	154.80.5.218

c. Select **Cluster Upgrade** if you want to upgrade the Management Agent cluster.

Note: The hosts that you specify must belong to the same cluster. Also, note that only the hosts that you specify here will be upgraded, irrespective of the number of hosts in that cluster. For example, if there are 10 hosts in a cluster and you specify only 5 here, Agent Deploy will upgrade only those five hosts in the cluster that you have specified.

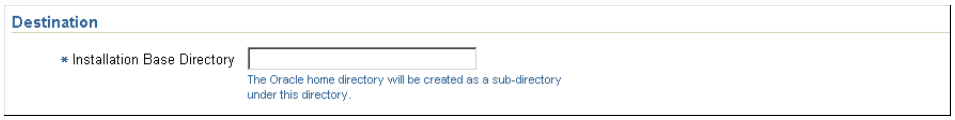
6. In the OS Credential section, specify the appropriate operating system user credentials. Select **Run root.sh** (UNIX platforms only) if you want Agent Deploy to execute this script. Agent Deploy will use `sudo` to run this script. You must specify the *invoking user's password* here. You must also ensure that the `targetpw` variable is not set in the `/etc/sudoers` file.

Figure 11–9 OS Credential Section of the Installation Details Screen (UNIX Only)



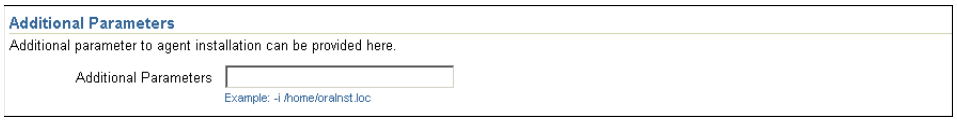
7. In the Destination section, specify the absolute path for the Installation Base Directory. This directory will be created on all the specified hosts, and the Agent Oracle home directory will be created as a subdirectory under this directory.

Figure 11–10 Destination Section of the Installation Details Page



8. In the Additional Parameters text box, specify any additional parameters that you want to pass during installation.

Figure 11–11 Additional Parameters Section of the Installation Details Page



9. In the Additional Scripts section, specify any preinstallation and postinstallation scripts that you want to execute.
10. Click **Continue** to start the installation process.

Click **Help**, in the Agent Deploy application for more information.

11.5.2.1 Possible Parameters that You Can Specify During Agent Upgrade

The important parameters for Agent Upgrade are `-o`, `-b` and optionally `-i`, `-t`.

Table 11–3 lists all the possible parameters that you can specify.

Table 11–3 Possible Parameters that You Can Specify During Agent Upgrade

Parameters	Description
-t	Do NOT start the Agent after installation/upgrade. No value required.
-b	Specify installation Base Dir location. For example, `-b /home/OracleHomes/agent/`
-d	Do not initiate automatic target discovery. No value required.
-i	Specify inventory pointer location file. For example, `-i /etc/oraInst.loc`
-o	Specify existing agent home to upgrade. For example, `-o /home/OracleHomes/oldAgent/`
-p	Specify file location for static port for Agent. For example, `-p /home/config/staticports.ini`
-z	Specify the timezone environment variable value (`-z <timezone>`). For example, `-z PST8PDT`.

> **Note:** If the parameters that you specify here are also specified independently through command-line options, the value of the parameters that you specify here will take precedence over the others. For example, if installation Base Dir has been specified independently, and the -b option is specified here, the value of the latter (`-b`) will be used during the upgrade.

11.5.3 Upgrading Management Agent Using agentDownload Script

To upgrade Management Agent using the `agentDownload` Script, follow the instructions documented below:

1. Invoke the `agendDownload` script using `-u` option.

   The `OLD_ORACLE_HOME` that you want to upgrade should be specified either by passing the `-o` option, or setting the `OLD_ORACLE_HOME` environment variable.

   Invoke the agentdownload script using the following command:

   ```
   ./agentDownload.linux -u -o <OLD_ORACLE_HOME_PATH>
   ```

   For Microsoft Windows, invoke the `agentDownload` script using the following command:

   ```
   ./agentDownload.vbs -u -o <OLD_ORACLE_HOME_PATH>
   ```

   > **Note:** The first two options (`-u` and `-o`) are mandatory. The `-b` option can be skipped if this has already been specified in the response files.

2. To construct the new Oracle home name, either pass the `-b` option, or specify these values for `BASEDIR` in the `agent_download.rsp` file.

   > **Note:** You can specify these options in the command-line even though they are present in the response file. The command-line options will have a higher precedence over the ones in response file.

3. If the base agent that you are upgrading is not secure, the script will prompt you to specify the Agent Registration Password.

You can use the options listed in Table 11–4 to execute the `agentDownload` script.

Table 11–4 Options that You Can Use To Execute the agentDownload Script

Options	Description
-b	baseDirectory of the Agent Oracle home
-l	local (pass -local to runInstaller)
-n	Cluster name
-o	OLD_ORACLE_HOME during Upgrade
-u	Upgrade
-c	CLUSTER_NODES (to specify the cluster nodes)
-p	`staticports.ini` file

Table 11–4 (Cont.) Options that You Can Use To Execute the agentDownload Script

Options	Description
-s	Installer stage directory
-t	Do NOT start the Agent
-i	Inventory pointer location file
-d	Do NOT initiate automatic target discovery

Note: When performing an Management Agent upgrade using the `agentDownload` script, ensure you are using the `agentDownload script` from the Oracle home of the pointing Management Service (OMS).

For example, if you are upgrading `agent1` that is pointing to OMS `A`, then you must use the `agentDownload` script that is located in the OMS `A` Oracle home only.

Caution: If you are upgrading a non-secure agent to a secure mode, the script will prompt you to specify the Agent Registration Password. Specify the correct password to secure the upgraded agent.

11.5.4 General System Installation Requirements for Real Application Clusters

Each node that is going to be part of your Oracle Real Application Clusters (Oracle RAC) installation must meet the following hardware and software requirements. You will perform step-by-step tasks for hardware and software verification for the platform-specific preinstallation procedures.

11.5.4.1 Hardware Requirements for Real Application Clusters Setup

Each node in a cluster requires the following hardware:

- External shared disks for storing the Oracle Clusterware files.

  Refer to the respective Oracle RAC installation guides for information on the disk configuration options that are available. Review these options before you decide which storage option to use in your Oracle RAC environment.

- One private internet protocol (IP) address for each node to serve as the private interconnect. The following must be true for each private IP address:

  – It must be separate from the public network.

  – It must be accessible on the same network interface on each node.

  – It must have a unique address on each node.

  The private interconnect is used for internode communication by both Oracle Clusterware and Oracle RAC. If the private address is available from a domain name server (DNS), then you can use that name. Otherwise, the private IP address must be available in each node's `/etc/hosts` file.

  On Microsoft Windows, this IP address must be available at the following location on each node:

  ```
  C:/Windows/<system drive>/etc/hosts file
  ```

During Oracle Clusterware installation, the information you enter as the private IP address determines which private interconnects are used by Oracle RAC database instances. They must all be in an up state, just as if their IP addresses were specified in the initialization parameter, `CLUSTER_INTERCONNECTS`. Oracle Real Application Clusters does not fail over between cluster interconnects; if one is down, then the instances using them will not start.

Oracle recommends that you use a logical IP address that is available across all private networks, and that you take advantage of any available operating system-based failover mechanism by configuring it according to your third-party vendor's instructions for using their product to support failover.

- One public IP address for each node, to be used as the Virtual IP address for client connections and for connection failover.

  This public Virtual IP address must be associated with the same interface name on every node that is part of your cluster. In addition, the IP addresses that you use for all of the nodes that are part of a cluster must be from the same subnet. If you have a domain name server (DNS), then register the host names for the Virtual IP with the DNS. The Virtual IP address should not be in use at the time of the installation, because this is a Virtual IP address that Oracle manages.

- One public fixed hostname address for each node, typically assigned by the system administrator during operating system installation. If you have a DNS, then register both the fixed IP and the VIP address with the DNS. If you do not have a DNS, then you must make sure that both public IP addresses are in the node host file.

11.5.4.2 Software Requirements for Real Application Clusters Setup

Each node in a cluster requires a supported interconnect software protocol to support Cache Fusion, and to support Oracle Clusterware polling. Your interconnect must be certified by Oracle for your platform. You should also have a Web browser, both to enable Oracle Enterprise Manager, and to view online documentation. For Oracle Database 10*g* requirements, Oracle Clusterware provides the same functions as third-party vendor clusterware. Using Oracle Clusterware also reduces installation and support complications. However, you may require third-party vendor clusterware if you use a non-ethernet interconnect, or if you have deployed clusterware-dependent applications on the same cluster where you deploy Real Application Clusters.

See Chapter 5, "Prerequisites for Installing Enterprise Manager on Oracle RAC" for more information on the preinstallation tasks.

Caution: If you are upgrading a 10.1.0.*n* agent to 10.2.0.2 release, you must execute the following command before starting the upgraded agent:

```
emctl resetTZ agent
```

This command is required to correct the agent time zone.

This command will correct the agent-side time zone, and specify an additional command to be run against the repository to correct the value there.

Note: Before you change the timezone, check if there are any blackouts that are currently running or scheduled to run on any of the targets that are monitored by the upgraded agent. Do the following to check this:

1. In the Grid Control console, go to the All Targets page under Targets and locate the Agent in the list of targets. Click the agent name link. The Agent home page appears.
2. The targets monitored by the agent will be listed in the *Monitored Targets* section.
3. For each target in the list, click the target name to view the target home page.
4. In the Related Links section, click **Blackouts** to check any blackouts that are currently running or may be scheduled to run in the future.
5. If such blackouts exist, you must stop all the blackouts that are running on all the targets monitored by this agent.
6. From the console, stop all the targets that are scheduled to run on any of these monitored targets.
7. Now, run the following command from the agent home to reset the timezone;

   ```
   emctl resetTZ agent
   ```

8. After the timezone is reset, you can create new blackouts on the targets.

Part V

Appendixes

Part 5 contains the following appendixes:

- Appendix A, "Troubleshooting Enterprise Manager"
- Appendix B, "Platform-Specific Package and Kernel Requirements"
- Appendix C, "Agent Deploy Application - Installation Prerequisites"
- Appendix D, "Additional Parameters for Agent Deploy"
- Appendix G, "Oracle Reserved Words"

A

Troubleshooting Enterprise Manager

This appendix describes solutions to common problems and scenarios that you might encounter when installing or upgrading Enterprise Manager.

A.1 Installation Issues

This section lists some of the most commonly encountered installation issues, and their resolutions.

A.1.1 Installation Fails with an Abnormal Termination

If there is a daily `cron` job that is running on the system where you are installing Grid Control that cleans up the `/tmp/` directory, the installation might fail with an abnormal termination and the `installActions.err` file will log the following error: `java.lang.UnsatisfiedLinkError: no nio in java.library.path`.

The workaround is to set the `TMP` and `TEMP` environment variables to a directory other than the default `/tmp` and execute the `./runInstaller`.

A.1.2 PERL Environment Variable is Forced on the environment During an Enterprise Manager 10*g* R2 (10.2.0.2) Installation

In a Microsoft Windows environment, if you have an existing `PERL5LIB` environment variable, the Enterprise Manager Grid Control installation will forcible overwrite this variable, in turn, forcing other applications on this host to use the new Perl version that get installed during the Management Service installation.

To work around this issue, rename the existing Perl variable as `PERL5LIB_TMP` before the Management Service installation starts. You can later (after the installation is complete) change the `PERL5LIB_TMP` variable to `PERL5LIB`

Note: If the Perl environment variable is not set, remove this variable from the Environment Variables. To do this, from the **Control Panel**, go to **Environment Variable** under **Systems**.

A.1.3 Management Agent Installation Fails

If the Management Agent installation fails, look into the emctl status log to diagnose the reason for installation failure. You can view this log by executing the following command:

```
<AGENT_HOME>/bin/emctl status agent
```

A sample log file follows and shows some of the typical problem areas shown in bold.

```
Oracle Enterprise Manager 10g Release 10.2.0.0.0.
Copyright (c) 1996, 2005 Oracle Corporation.  All rights reserved.
-------------------------------------------------------------
Agent Version     : 10.2.0.2.0
OMS Version       : 10.2.0.2.0
Protocol Version  : 10.2.0.2.0
Agent Home        : /scratch/OracleHomes2/agent10g
Agent binaries    : /scratch/OracleHomes2/agent10g
Agent Process ID  : 9985
Parent Process ID : 29893
Agent URL         : https://foo.abc.com:1831/emd/main/
Repository URL    : https://foo.abc.com:1159/em/upload
Started at        : 2005-09-25 21:31:00
Started by user   : pjohn
Last Reload       : 2005-09-25 21:31:00
Last successful upload                       : (none)
Last attempted upload                        : (none)
Total Megabytes of XML files uploaded so far :     0.00
Number of XML files pending upload           :     2434
Size of XML files pending upload(MB)         :    21.31
Available disk space on upload filesystem    :    17.78%
Last attempted heartbeat to OMS              : 2005-09-26 02:40:40
Last successful heartbeat to OMS             : unknown
-------------------------------------------------------------
Agent is Running and Ready
```

A.1.3.1 Prerequisite Check Fails with Directories Not Empty Error During Retry

During an agent installation using Agent Deploy, the installation fails abruptly, displaying the Failure page. On clicking **Retry**, the installation fails again at the Prerequisite Check phase with an error stating the directories are not empty.

This could be because Oracle Universal Installer (OUI) is still running though the SSH connection that is closed on the remote host.

To resolve this issue, on the remote host, check if OUI is still running. Execute the following command to verify this:

```
ps -aef | grep -i ora
```

If OUI is still running, wait till OUI processes are complete and restart the SSH daemon. Now, you can click **Retry** to perform the installation.

Note: For more information on running the prerequisite checks in standalone mode, see Section 1.5, "Running the Prerequisite Check in Standalone Mode".

A.1.3.2 Agent Deployment on Linux Oracle RAC 10.2 Cluster Fails

Agent deployment on a 10.2 release of an Oracle RAC cluster may fail due to a lost SSH connection during the installation process.

This can happen if the `LoginGraceTime` value in the `sshd_config` file is 0 (zero). The zero value gives an indefinite time for SSH authentication.

To resolve this issue, modify the `LoginGraceTime` value in the `/etc/ssh/sshd_config` file be a higher value. The default value is 120 seconds. This means that the server will disconnect after this time if you have not successfully logged in.

To resolve this issue, modify the `LoginGraceTime` value in the `/etc/ssh/sshd_config` file to be a higher value. If the value is set to 0 (zero), there is no definite time limit for authentication.

A.1.3.3 SSH User Equivalence Verification Fails During Agent Installation

The most common reasons for SSH User Equivalence Verification to fail are the following:

- The server settings in `/etc/sshd/sshd_config file` do not allow `ssh` for user `$USER`.
- The server may have disabled the public key-based authentication.
- The client public key on the server may be outdated.
- You may not have passed the `-shared` option for shared remote users, or may have passed this option for non-shared remote users.

Verify the server setting and rerun the script to set up SSH User Equivalence successfully.

> **Note:** For more information on how to set up SSH, see Section C.1.2, "Set Up SSH (Secure Shell) User Equivalence".

A.1.3.3.1 Sample sshd_config File

The following `sshd_config` file sample is a server-wide configuration file with all the variables.

```
#$OpenBSD: sshd_config,v 1.59 2002/09/25 11:17:16 markus Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default values where
# possible, but leave them commented out.  Uncommented options change a
# default value.

#Port 22
#Protocol 2,1
#ListenAddress 0.0.0.0
#ListenAddress ::

# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 3600
#ServerKeyBits 768

# Logging
#obsoletes QuietMode
#SyslogFacility AUTH
```

```
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 120
#PermitRootLogin yes
#StrictModes yes

#RSAAuthentication yes
#PubkeyAuthentication yes
#AuthorizedKeysFile.ssh/authorized_keys

# rhosts authentication should not be used
#RhostsAuthentication no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no
# similar for protocol version 2
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
#IgnoreUserKnownHosts no

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes

#AFSTokenPassing no

# Kerberos TGT Passing only works with the AFS kaserver
#KerberosTgtPassing no

# Set this to 'yes' to enable PAM keyboard-interactive authentication
# Warning: enabling this may bypass the setting of 'PasswordAuthentication'
#PAMAuthenticationViaKbdInt no

#X11Forwarding no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PrintMotd yes
#PrintLastLog yes
#KeepAlive yes
#UseLogin no
#UsePrivilegeSeparation yes
#PermitUserEnvironment no
#Compression yes

#MaxStartups 10
# no default banner path
```

```
#Banner /some/path
#VerifyReverseMapping no
#ShowPatchLevel no

# override default of no subsystems
Subsystemsftp/usr/libexec/openssh/sftp-server
```

A.1.3.4 SSH Setup Fails with "Invalid Port Number" Error

The SSH User Equivalence script when executed, is built to automatically verify the setup at the end, by executing the following command:

```
ssh -l <user> <remotemachine> 'date'
```

At the time of verification, you may encounter an "Invalid Port Error" indicating that the SSH setup was not successful.

This can happen if the `ssh.exe` (`sshUserSetupNT.sh` script) is not being invoked from the `cygwin` home directory.

To resolve this issue, ensure the `sshUserSetupNT.sh` script on the local OMS machine is being executed from within the `cygwin` (BASH) shell only. The script will fail to execute if done from outside this location.

If there are multiple Cygwin installations, and you want to find out which ssh.exe is being invoked, execute the following command:

```
C:\Cygwin\bin\which ssh
```

For example, when you execute the previously mentioned command, and it returns a result that is similar to the following:

```
\cygdrive\c\WINDOWS\ssh
```

This indicates that the `ssh.exe` file from Cygwin is not being invoked as there is `C:\windows` that is present before `C:\Cygwin\bin` in the PATH environment variable.

To resolve this issue, rename this ssh.exe as follows:

```
-C:\cygwin>move c:\WINDOWS\ssh.exe c:\WINDOWS\ssh.exe1
         1 file(s) moved.
```

Now, execute the `C:\Cygwin which ssh` command again.

The result should be similar to `"\usr\bin\ssh"`.

This verifies that `ssh.exe` file is being invoked from the correct location (that is, from your `C:\Cygwin\bin` folder).

Note: You must ensure `C:\cygwin` is the default installation directory for the Cygwin binaries.

If you install `Cygwin` at a location other than `c:\cygwin` (default location), it can cause the SSH setup to fail, and in turn, the agent installation will fail too.

To work around this issue, you must either install `Cygwin` in the default directory (`c:\cygwin`), or update the `ssPaths_msplats.properties` file with the correct path to the `Cygwin` binaries.

You can look into the following remote registry key to find out the correct `Cygwin` path:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cygnus Solutions\Cygwin\mounts v2\
```

Note: For more information on how to set up SSH, see Section C.1.2, "Set Up SSH (Secure Shell) User Equivalence".

A.1.3.5 sshConnectivity.sh Script Fails

If you are executing the `sshConnectivity.sh` script on *Cygwin version 5.2*, the script may fail and result in the following error:

```
"JAVA.LANG.NOCLASSDEFFOUNDERROR"
```

To workaround this issue, ensure the Oracle home in the *Cygwin style path* is defined as follows:

```
ORACLE_HOME="c:/oraclehomes/oms10g/oracle"
```

You can find out the currently installed Cygwin version by executing the `uname` command on the Cygwin window.

Note: For more information on using the sshConnectivity.sh script, see Section C.1.2.1, "Setting Up SSH User Equivalence Using sshConnectivity.sh".

A.1.3.6 Troubleshooting the "command cygrunsrv not found" Error.

During the SSH daemon setup, you may encounter a "`command cygrunsrv not found`" error. This can occur due to one of the following two reasons:

- The sshd service is not running.
- The Cygwin installation was not successful.

A.1.3.6.1 If SSHD Service Is Not Running

Create the sshd service, and then start a new sshd service from the `cygwin` directory.

To create the SSHD service, you must execute the following command:

```
ssh-host-config
```

The Cygwin script that runs when this command is executed will prompt you to answer several questions. Specify **yes** for the following questions:

- privilege separation
- install sshd as a service

Specify **no** when the script prompts you to answer whether or not to "create local user sshd".

When the script prompts you to specify a value for Cygwin, type `ntsec` (`CYGWIN="binmode tty ntsec"`).

Now that the SSHD service is created, you can start the service by executing the following command:

```
cygrunsrv -start sshd
```

A.1.3.6.2 If Your Cygwin Installation Was Unsuccessful

If restarting the SSHD service does not resolve the error, then you must reinstall Cygwin. To do this:

1. Remove the Keys and Subkeys under Cygnus Solutions using `regedit`.
2. Remove the Cygwin directory (`C:\cygwin`), and all Cygwin icons.
3. Remove the `.ssh` directory from the Documents and Settings folder of the domain user.
4. Reinstall Cygwin.

   For detailed instructions on Cygwin installation, see Section C.1.2.3, "Setting Up SSH Server (SSHD) on Microsoft Windows"
5. Execute the following command to start SSH daemon:

   ```
   cygrunsrv -start sshd
   ```

A.1.3.7 SSH Setup Verification Fails with "Read from socket failed: Connection reset by peer." Error

After the SSH setup is complete, the script automatically executes the following verification command:

```
ssh -l <user> <remotemachine> 'date'
```

If this command returns an error stating "Read from socket failed: Connection reset by peer", this means SSH was incorrectly set up. To resolve this issue, go to the remote machine where you attempted to set up user equivalence and do the following:

1. Stop the SSHD service (`cygrunsrv -stop sshd`).
2. Go to the `etc` directory (`cd /etc`).
3. Change the SSH file owner to the appropriate system (`chown <SYSTEM> ssh*`).
4. Go to the Cygwin command prompt and execute the following:

   ```
   chmod 644 /etc/ssh*
   chmod 755 /var/empty
   chmod 644 /var/log/sshd.log
   ```

5. Now, execute the verification command from the Management Service (OMS) machine (`ssh -l <user> <remote machine> 'date'`). This should display the date correctly, suggesting the SSH setup was successful.
6. Finally, start the SSHD service (from `/usr/bin/sshd`), or by executing `cygrunsrv -start sshd`.

7. Now, execute the verification command again from the OMS machine (`ssh -l <user> <remote machine> 'date'`). This should display the date correctly, suggesting the SSH setup was successful.

A.1.3.8 SSHD Service Fails to Start

During SSHD configuration, the SSHD service is created for the local account by default. When you log in as a domain user, this account is not recognized by the service, and does not start up.

To resolve this issue, you must change the SSHD service "`Log On As`" value from `LocalSystem` to the domain user. To do this, complete the following steps:

1. Right-click on My Computer and select **Manage.**
2. In the Computer Management dialog box that appears, click **Services** under Services and Applications.
3. In the right pane, select the Cygwin SSHD service, right-click and go to Properties.
4. In the Cygwin SSHD Properties window that appears, select **This Account**.
5. Now, specify the appropriate domain name and user (in the form of `domain\user`, for example, `FOO-US\pjohn`).
6. Specify the password for this user, and click **Apply.**
7. Now, go to the Cygwin command prompt and execute the following:

```
chmod 644 /etc/ssh*
chmod 755 /var/empty
chmod 644 /var/log/sshd.log
```

8. Start SSHD by executing the following command:

```
/usr/sbin/sshd
```

A.1.3.9 Timezone Prerequisite Check Fails

The timezone prerequisite check (`timezone_check`) will fail if the TZ environment variable is not set on the SSH daemon of the remote host.

To resolve this issue, you must set the TZ environment variable on the SSH daemon of the remote host. See Section C.1.2.5, "Setting Up the Timezone Variable on Remote Hosts" for more information.

Alternatively, you do the following:

- If you are installing or upgrading the agent from the default software location, set the timezone environment variable by specifying the following in the Additional Parameters section of the Agent Deploy application:

```
-z <timezone>
For example, -z PST8PDT
```

- If you are installing the agent from a nondefault software location, you must specify the timezone environment variable using the following command:

```
s_timeZone=<timezone>
For example, s_timezone=PST8PDT
```

A.1.3.10 OMS Version Is Not Displayed

If the OMS version is not displayed in the log file, it could mean that the installed agent is not registered with a secure and locked Management Service (OMS).

You can verify this by executing the following commands:

```
emctl status oms
emctl status agent
```

To resolve this issue, you must manually secure the Management Agent by executing the following command:

```
<AGENT_HOME>/bin/emctl secure agent -reg_passwd <password>
```

A.1.3.11 Discrepancy Between Agent and Repository URL Protocols

If the agent installation is successful, the protocol for both agent and the repository URLs are the same. That is, both URLs start with the `https` protocol (meaning both are secure).

If the protocol for the agent URL is displayed as `http` instead of `https`, this means that the agent is not secure.

To resolve this issue, you must secure the agent manually by executing the following command:

```
<AGENT_HOME>/bin/emctl secure agent -reg_passwd <password>
```

A.1.3.12 Last Successful Upload Does Not Have a Time Stamp

If there is no time stamp against this parameter in the log (displays `Null`), it means that the agent is unable to upload any data.

To resolve this issue, you must perform a manual upload of the data by executing the following command, and then check the log again:

```
<AGENT_HOME>/bin emctl upload
```

A.1.3.13 emctl status Log File is Empty

If the agent is not ready and running, the `emctl status` log displays only the copyright information. None of the parameters listed in the sample log is displayed.

The issue can occur due to any of the following reasons:

- Agent is not secure: To manually secure the agent, execute the following command:

  ```
  <AGENT_HOME>/bin emctl secure agent -reg_passwd <password>
  ```

- Agent is not running: Check if the agent is running. If not, you can start the agent manually by executing the following command:

  ```
  <AGENT_HOME>/bin emctl start agent
  ```

- Agent port is not correct: Verify whether the agent is connecting to the correct port. To verify the port, look into the `sysman/config/emd.properties` file:

  You must also ensure the following are correctly set in the `emd.properties` file:

  a. REPOSITORY_URL: Verify this URL (`http://<hostname>:port/em/upload`). Here, ensure the host name and port are correct.

  b. emdWalletSrcURL: Verify if the host name and port are correct in this URL (`http://<hostname>:port/em/wallets/emd`).

  c. agentTZRegion: Ensure the time zone that is configured is correct.

A.2 Configuration Issues

This section lists some of the most commonly encountered configuration issues, and their resolutions.

A.2.1 Configuration Assistants Fail During Enterprise Manager Installation

During the installation, if any of the configuration assistants fails to run successfully, you can choose to run the configuration assistants in standalone mode.

Note: The individual log files for each configuration tool are available at the following directory:

```
ORACLE_HOME/cfgtoollogs/cfgfw
```

Besides the individual configuration logs, this directory also contains `cfmLogger_timestamp.log` (The timestamp depends on the local time and has a format such as `cfmLogger_2005_08_19_01-27-05-AM.log`.). This log file contains all the configuration tool logs.

For more information about the installation logs that are created and their locations, see Appendix A, "Troubleshooting Enterprise Manager".

Also see Section 3.4, "Executing the runConfig Tool from the Command Line" to understand using the runconfig tool. This tool is used for running configuration assistants as explained below.

A.2.1.1 Invoking the One-Off Patches Configuration Assistant in Standalone Mode

During the installation process, this configuration assistant is executed before the Management Service Configuration Assistant is run.

This configuration assistant applies the one-off patches that are required for a successful Enterprise Manager 10*g* Release 2 installation.

To run this configuration assistant in standalone mode, you must execute the following command from the Management Service Oracle home:

```
<OMS_HOME>/perl/bin/perl <OMS_HOME>/install/oneoffs/applyOneoffs.pl
```

A.2.1.2 Invoking the Database Configuration Assistant in Standalone Mode

To run the Database Configuration Assistant, you must invoke the `runConfig.sh` script as:

```
<DB_Home>/oui/bin/runConfig.sh ORACLE_HOME=<DB_HOME> ACTION=Configure MODE=Perform
```

On Microsoft Windows, replace `runConfig.sh` with `runConfig.bat` in the previously mentioned command.

A.2.1.3 Invoking the OMS Configuration Assistant in Standalone Mode

To run the OMSConfig Assistant, you must invoke the runConfig.sh as the following:

```
<OMS_Home>/oui/bin/runConfig.sh ORACLE_HOME=<OMS_HOME> ACTION=Configure
MODE=Perform
```

On Microsoft Windows, replace `runConfig.sh` with `runConfig.bat` in the previously mentioned command.

A.2.1.4 Invoking the Agent Configuration Assistant in Standalone Mode

To run the AgentConfig Assistant, you must invoke the `runConfig.sh` as the following:

```
<Agent_Home>/oui/bin/runConfig.sh ORACLE_HOME=<AGENT_HOME> ACTION=Configure
MODE=Perform
```

On Microsoft Windows, replace `runConfig.sh` with `runConfig.bat` in the above-mentioned command.

Note: While the preceding command can be used to execute the `agentca` script, Oracle recommends you execute the following command to invoke the configuration assistant:

```
Agent_Home/bin/agentca -f
```

If you want to run the `agentca` script on a Oracle RAC, you must execute the following command on each of the cluster nodes:

```
Agent_Home/bin/agentca -f -c "node1,node2,node3,...."
```

See Section 7.5, "Agent Reconfiguration and Rediscovery" for more information.

A.2.1.5 Invoking the OC4J Configuration Assistant in Standalone Mode

If you want to deploy only the Rules Manager, execute the following commands:

```
/scratch/OracleHomes/oms10g/jdk/bin/java -Xmx512M
-DemLocOverride=/scratch/OracleHomes/oms10g -classpath
/scratch/OracleHomes/oms10g/dcm/lib/dcm.jar:/scratch/OracleHomes/oms10g/jlib/e
mConfigInstall.jar:/scratch/OracleHomes/oms10g/lib/classes12.zip:/scratch/Orac
leHomes/oms10g/lib/dms.jar:/scratch/OracleHomes/oms10g/j2ee/home/oc4j.jar:/scr
atch/OracleHomes/oms10g/lib/xschema.jar:/scratch/OracleHomes/oms10g/lib/xmlpar
serv2.jar:/scratch/OracleHomes/oms10g/opmn/lib/ons.jar:/scratch/OracleHomes/om
s10g/dcm/lib/oc4j_deploy_tools.jar oracle.j2ee.tools.deploy.Oc4jDeploy
-oraclehome /scratch/OracleHomes/oms10g -verbose -inifile
/scratch/OracleHomes/oms10g/j2ee/deploy.master -redeploy
```

On Microsoft Windows, replace `runConfig.sh` with `runConfig.bat` in the previously mentioned command.

A.2.1.6 Enterprise Manager Deployment Fails

Enterprise Manager deployment may fail due to the Rules Manager deployment failure.

To resolve this issue, redeploy Enterprise Manager by following these steps:

1. Move `OH/j2ee/deploy.master` to `OH/j2ee/deploy.master.bak`.
2. Execute the `OH/bin/EMDeploy script`.
3. Restore the `OH/j2ee/deploy.master`. That is, `execute mv OH/j2ee/deploy.master.bak OH/j2ee/deploy.master`

A.2.2 Oracle Management Service Configuration Fails

Oracle Management Service configuration may fail due the following reasons.

A.2.2.1 Oracle Management Service Fails While Deploying Enterprise Manager AgentPush Application

The cfgfw logs display the following error:

```
Redeploying application 'EMAgentPush' to OC4J instance 'OC4J_EMPROV'. FAILED!
ERROR: Caught exception while deploying 'EMAgentPush' to 'OC4J_
EMPROV':java.lang.reflect.InvocationTargetException at
sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
```

This error is due to Ipv6 entries in `/etc/hosts` file. When prompted to execute root.sh or when configuration fails, do the following:

1. In `<OMS Home>/sysman/install/EMDeployTool.pm`, include `"-Djava.net.preferIPv4Stack=true"` in the command executed in deployEmEar ().
2. In `<OMS Home>/opmn/conf/opmn.xml`, include `"-Djava.net.preferIPv4Stack=true"` in java-options of all OC4J processes.

A.2.2.2 In 'Enterprise Manager with new Database' Install, Oracle Management Service Configuration Fails While Unlocking Passwords

The `cfgfw` logs display the following error:

```
Failed to initialize JDBC Connection
```

This is caused when listener does not start during NetCA execution and the following error will be present in the `installActions` log:

```
Listener start failed. Listener may already be running.
```

To rectify this error, add the following line in `<DB Home>/network/admin/listener.ora`:

```
SUBSCRIBE_FOR_NODE_DOWN_EVENT_<listener_name>=OFF
```

Then, restart the listener.

A.2.2.3 Dropping of Repository Hangs If SYSMAN Sessions are Active

While installing Enterprise Manager using existing database, Oracle Management Service configuration hangs while dropping the repository. This is due to active SYSMAN sessions connected to the database.

To resolve this issue, shutdown any existing Enterprise Manager sessions (both Grid Control and Database Control) or other SQLPLUS SYSMAN sessions.

A.2.2.4 If Oracle Management Service Configuration is Retried, oracle.sysman.emSDK.svlt.ConsoleServerHost and oracle.sysman.emSDK.svlt.ConsoleServerName in emoms.properties are Swapped and There is an Extra Underscore in ConsoleServerHost

This problem only occurs with 10.2.0.1.0 Additional Oracle Management Server installation.

To resolve this issue, swap the values and remove the extra underscore in ConsoleServerName in `emoms.properties` present in `<OMS_ORACLE_HOME>/sysman/config` directory.

A.3 Enterprise Manager Upgrade and Recovery Issues

The Enterprise Manager 10*g* Release 2 upgrade is an out-of-place upgrade, meaning that Enterprise Manager 10*g* Release 2 Oracle homes are separate from the old homes. If you decide to abort the upgrade process during the copying phase (copying of the binaries), you can simply revert to your old 10*g* Release 1 installation.

The upgrade process creates a new OMS home and a new database home. The Upgrade assistants upgrade the datafiles and `SYSMAN` schema, and then configure the new Oracle homes.

Caution: Do not abort the upgrade process during the configuration phase, as this will corrupt the installation. You will not be able to revert to the old 10*g* Release 1 installation either.

A.3.1 Agent Upgrade Issues

This section lists some of the issues that you may encounter during an agent upgrade.

A.3.1.1 Agent Does Not Start Up After Upgrade

During an agent upgrade from 10.1.0.*n* to 10.2.0.2, the agent may fail to start up after upgrade if the time zone that is configured for the upgraded agent is different from the originally configured agent.

You can correct this issue by changing the time zone. To do this, execute the following command from the upgraded agent home:

```
emctl resetTZ agent
```

This command will correct the agent-side time zone, and specify an additional command to be run against the repository to correct the value there.

Caution: Before you change the time zone, check if there are any blackouts that are currently running or scheduled to run on any of the targets that are monitored by the upgraded agent. Do the following to check this:

1. In the Grid Control console, go to the All Targets page under Targets and locate the Agent in the list of targets. Click the agent name link. The Agent home page appears.
2. The list of targets monitored by the agent will be listed in the *Monitored Targets* section.
3. For each target in the list, click the target name to view the target home page.
4. Here, in the Related Links section, click **Blackouts** to check any blackouts that are currently running or may be scheduled to run in the future.
5. If such blackouts exist, you must stop all the blackouts that are running on all the targets monitored by this agent.
6. From the console, stop all the targets that are scheduled to run on any of these monitored targets.
7. Now, run the following command from the agent home to reset the time zone;

   ```
   emctl resetTZ agent
   ```

8. After the time zone is reset, you can create new blackouts on the targets.

A.3.1.2 Missing Directories When Upgrading Agent from 10.1.0.5 to 10.2.0.1

In a Windows NT RAC agent upgrade scenario, after the AgentOnly shiphome installer has completed installation, the utility `<Upgrade AOH>/oui/bin/upgrade` has to be executed on every single node in the RAC to complete the agent upgrade.

A.3.2 Enterprise Manager Recovery

This sections provides the instructions to be followed to perform an Enterprise Manager recovery.

A.3.2.1 Steps to Follow for Agent Recovery

Use the following instructions to perform an agent recovery:

1. After exiting the installer, you must open a new window and change the directory to the `<New_AgentHome>/bin`.
2. Execute the script `./upgrade_recover`.
3. You can then start the old agent and continue using it. If you want to remove the installed binaries of the new agent home, use the Remove Productions function of the installer.

A.3.2.2 Steps to Follow for OMS Recovery

If the schema has been upgraded or the upgrade was incomplete, you must manually restore the database to the backup that was taken prior to executing the OMS upgrade.

You can determine the status of the repository upgrade by looking into the log file at `<New_OMSHome>/sysman/log/emrepmgr.log.<proc_id>`. The last line of the log file provides the status of the upgrade. If the upgrade was completed without

errors, it reads *Repository Upgrade Successful*. If not, the message *Repository Upgrade has errors…* is displayed.

Follow these instructions to perform an OMS recovery:

Note: Before you attempt to restore the database, you must exit the Upgrade wizard. You must also ensure there are no OMS processes that are running. See Section 11.2.1, "Shut Down Enterprise Manager Before Upgrade" for more information on shutting down the Enterprise Manager processes.

Caution: Ensure all OMS processes are completely shut down. If not, the system may become unstable after the upgrade.

---

1. Restore the database to the backup. See Oracle Database Administrator's Guide for more information.
2. After the database is restored, start the database and listener to ensure successful restoration.
3. Open a new window and change the directory to the `<New_OMSHome>/bin`.
4. Now, execute the `./upgrade_recover`.

Start the old OMS and continue to use it. If you want to remove the binaries of the newly installed OMS home, use the Remove Productions function in the installer.

A.3.2.3 Steps to Re-create the Repository

If the Management Service configuration plugin fails due to the repository creation failure, rerunning the configuration tool from Oracle Universal Installer drops the repository and re-creates it. However, if you want to manually drop the repository, complete the following steps:

A.3.2.3.1 Dropping the Repository

1. Stop the OPMN processes (`<OMSHOME>/bin/opmnctl stopall`), Management Service (`<OMS_HOME>/bin/emctl stop oms`), and Agent (`<AGENT_HOME>/bin/emctl stop agent`) before dropping the repository.
2. Set ORACLE_HOME to `OMS_OracleHome`
3. Execute `OMS_Home/sysman/admin/emdrep/RepManager <hostname> <port> <SID> -action drop -output_file <log_file>`

A.3.2.3.2 Creating the Repository

1. Set ORACLE_HOME to `OMS_OracleHome`.
2. Execute `OMS_Home/sysman/admin/emdrep/RepManager <hostname> <port> <SID> -action create -output_file <log_file>`.

Note: After recreating the repository, you must run the following command on all the Management Service Oracle homes to reconfigure the `emkey`:

```
emctl config emkey -repos -force
```

This command overwrites the `emkey.ora` file with the newly generated `emkey`.

Caution: While recreating the repository using `./Repmanager -action create` command, you may encounter the following error message:

```
java.sql.SQLExecution: ORA-28000: the account is locked during
recreation of repository.
```

Workaround

This error may occur if there are processes or multiple Management Services that are trying to connect to the database with incorrect SYSMAN credentials. If there are multiple login failures, the database becomes locked up and shuts down the monitoring agent.

You can resolve this issue by shutting down all the Management Services connected to the database, along with the monitoring agent.

A.3.3 Repository Creation Fails

When installing Enterprise Manager using an existing database, the repository creation fails.

This may happen if the profile of the Password Verification resource name in the database has a value that is other than *Default*. To resolve this issue:

1. Change the Password Verification profile value to *Default*.
2. Create the repository using RepManager command.

A.3.4 Collection Errors After Upgrade

If you upgrade only the Management Service to 10*g* Release 2 without upgrading the monitoring agent, you may encounter the following collection errors:

- Target Management Services and Repository
- Type OMS and Repository
- Metric Response
- Collection Timestamp <session_time_stamp>
- Error Type Collection Failure
- Message Target is in Broken State. Reason - Target deleted from agent

To resolve this issue, upgrade the monitoring agent along with the Management Service to 10*g* Release 2.

A.4 Oracle Management Service Upgrade Issues

You may encounter problems during Management Service upgrade where the upgrade process aborts due to the following reasons.

A.4.1 OMS Upgrade Stops at OracleAS Upgrade Assistant Failure

The installation dialog box and the configuration framework log file (located at`<New_OracleHome>/cfgtoollogs/cfgfw/oracle.sysman.top.oms_#date.log`) lists `SEVERE` messages indicating the reason the Oracle Application Server Upgrade Assistant fails.

If the message displays *permission denied* on certain files, it means that the user running the installer may not have the correct permissions to run certain iAS configurations.

To resolve this issue, comment out the OracleAS configuration that contains these files and then retry the upgrade again. You can reapply the configurations after the upgrade is successfully completed.

A.4.2 OMS Configuration Stops at EMDeploy Failure

The most common reasons for EMDeploy to fail are if:

- All Enterprise Manager processes are not shut down completely.

  To shut down Enterprise Manager, execute the following commands:

  ```
  <Oracle_Home>/opmn/bin/opmnctl stopall
  <Oracle_Home>/bin/emctl stop em
  ```

  See Section 11.2.1, "Shut Down Enterprise Manager Before Upgrade" for more information.

- Symbolic links have been used instead of hard links

  The `<Oracle_Home>/Apache/<component>` configuration files must be examined to ensure only hard links (and no symbolic links) were referenced. See Section 11.2.2, "Check for Symbolic Links" for more information.

After you have successfully resolved these issues, perform the redeploy steps manually and click **Retry** on the Upgrade wizard.

A.4.3 OMS Configuration Stops at Repository Schema Failure (RepManager)

The most common reason the repository schema configuration fails is when it is not able to connect to the listener. The configuration framework log file (`<New_OracleHome>/cfgtoollogs/cfgfw/oracle.sysman.top.oms_#date.log`) indicates the reason for the repository schema upgrade failure.

To resolve this issue, you must verify whether or not the listener connecting to the OMS is valid and active.

Also, if you have installed the OMS using the *Install Enterprise Manager Using New Database* installation type, ensure there are no symbolic links being referenced. After you have successfully established the listener connections, click **Retry** on the Upgrade wizard.

A.4.4 Monitoring Agent Does Not Discover Upgraded Targets

If you have upgraded an Enterprise Manager Grid Control target (for example, database) independently (that is using a regular upgrade mechanism other than the

Oracle Universal Installer), the monitoring agent may fail to discover this upgraded target.

This can happen if you have specified a different Oracle home value for the upgraded target other than the one that already existed.

To resolve this issue, you must manually configure the `targets.xml`file of the monitoring agent to update the configuration details of the upgraded Oracle home information, or log in to the Enterprise Manager console, select the appropriate target, and modify its configuration parameters to reflect the upgraded target parameters.

A.4.5 CSA Collector Is Not Discovered During Agent Upgrade

When a 10*g* Release 1 Management Service and its associated (monitoring) agent are upgraded at the same time, the agent upgrade does not discover the CSA Collector target.

To discover this target, you must run the agent configuration assistant (the `agentca` script) using the rediscovery option. See Section 7.5.1, "Rediscover and Reconfigure Targets on Standalone Agents" for more information.

A.4.6 ias_admin Password Is Set To welcome1 After Upgrade

To resolve this issue, run the following command:

```
<New OMS Home>/bin/emctl set password welcome1 <New Password>
```

A.4.7 Oracle Management Service Upgrade Fails If Older Listener Is Running On A Port Other Than 1521

To resolve this issue, do the following:

1. Stop the older listener when prompted to execute `allroot.sh`. The Oracle Management Service upgrade will fail.
2. Set the listener from the new database to run from the same non-1521 port.
3. Run the upgrade again.

A.5 Network Issues

This section lists network issues you may encounter during Enterprise Manager installation and configuration.

A.5.1 Incorrect Format For Entries In /etc/hosts File

This will cause the installation to hang and OUI-25031 or OUI-10104 errors in log files.

Entries in the `/etc/hosts` file should be in the following format:

```
IP_Address Canonical_Hostname Aliases
```

For example:

```
11.22.33.441 abc.xyz.com abc1 xyz2
```

When creating the `/etc/hosts` file, follow these rules:

- Host name may contain only alphanumeric characters, hyphen, and period. The name must begin with an alphabetic character and end with an alphanumeric character.

- Lines cannot start with a blank or tab character.
- Fields can have any number of blanks or tab characters separating them.
- Comments are allowed and designated by a pound sign (#) preceding the comment text.
- Trailing blank and tab characters are allowed.
- Blank line entries are allowed.
- Only one host entry per line is allowed.

Forward lookup is finding IP address given the hostname. Reverse lookup is finding hostname given the IP address. Results of forward and reverse lookups should be the same. It is usually different because of case difference (upper/lower) in hostnames and aliases.

For 10.2.0.1 Enterprise Manager installations, if a host name contains an upper case letter, securing of Agent will fail.

A.5.2 Enterprise Manager Installation on Computers With Multiple Addresses

While installing Enterprise Manager or related components on Multi-homed (Multi-IP) machines, that is, a machine having multiple IP addresses, hostname will be derived from `ORACLE_HOSTNAME` environment variable if it is set; else the first name in `/etc/hosts` will be considered for installation purposes.

A.5.3 Agent Configuration Fails on A Non-Network Computer

To resolve this error, Oracle Management Service and target host where the Agent needs to be installed should be pingable.

A.5.4 Loopback Adapter On Windows and Related Known Issues

If installing Enterprise Manager or related components on a DHCP host, one needs to install a loopback adapter to assign a local IP address to that computer.

Note: Refer to section 2.4.5 Installing a Loopback Adapter of the *Oracle® Database Installation Guide 10g Release 2 (10.2) for Microsoft Windows (32-Bit) Part Number B14316-02* for more information.

Ensure that the following conditions are met:

- The `/etc/hosts` file should contain the following entry:

  ```
  <lopback IP Address><hostname.domainname> <hostname>
  ```

  For example:

  ```
  127.0.0.1 localhost.localdomain localhost
  ```

- Ensure that the IP address specified in `/etc/hosts` is correct otherwise allocation of ports will fail

A.6 Other Installation and Configuration Issues

This section lists some of the generic errors that you may encounter during Enterprise Manager installation and configuration.

A.6.1 Storage Data Has Metric Collection Errors

The following Enterprise Manager collection error message may appear from agents installed through silent or `agentdownload` install mechanisms:

```
snmhsutl.c:executable nmhs should have root suid enabled.
```

Perform the required root install actions (using `root.sh` script on UNIX platforms only) to resolve this issue. It may take up to 24 hours before the resolution is reflected.

A.6.2 Cannot Add Systems to Grid Environment from the Grid Control Console

You cannot add new targets to your grid environment if you do not have an agent already installed.

To install the agent from your Grid Control console:

1. Log in to the Grid Control console and go to the Deployments page.
2. Click **Install Agent** under the Agent Installation section.
3. In the Agent Deploy home page that appears, select the appropriate installation option that you want to perform. See Section 6.2.1, "Agent Deploy Installation Prerequisites" for more information.

A.7 Error During Deinstallation of Grid Control Targets

After deinstalling certain Grid Control targets, when you try to remove the same targets from the Grid Control console, you may encounter an exception with a message similar to the following:

```
java.sql.SQLException: ORA-20242: Target <target name> is monitoring other
targets. It cannot be deleted.
```

To resolve this issue, deinstall the Grid Contol targets and wait for at least 15 minutes before you attempt to remove the targets from the Grid Control console using the Hosts page. This time is required for the deinstallation information to propagate to the Management Repository.

A.8 Need More Help

If this appendix does not solve the problem you encountered, try these other sources:

- Oracle Enterprise Manager Release Notes, available on the Oracle Technology Network Web site (`http://www.oracle.com/technology/documentation`).
- Oracle

  (`http://metalink.oracle.com`).

If you do not find a solution for your problem, log a service request.

B

Platform-Specific Package and Kernel Requirements

This appendix lists the recommended software packages and kernel parameters required for a successful Enterprise Manager Grid Control installation on each of the supported platforms. For the most current list of supported operating system-specific software, refer to OracleMetaLink at http://metalink.oracle.com.

This appendix has the following sections:

- Package Requirements
  - Required Packages on Linux
  - Required Packages on Solaris
  - Required Packages on HP-UX
  - Required Packages on AIX
- Kernel Parameter Requirements
  - Kernel Parameter Requirements on Linux
  - Kernel Parameter Requirements on Solaris
  - Kernel Parameter Requirements on HP-UX
  - Configure Shell Limits and System Configuration Parameters on AIX

B.1 Package Requirements

The following sections list the package requirements for each platform.

B.1.1 Required Packages on Linux

The following (or later) packages must be running on your Linux systems.

Red Hat Enterprise Linux 3.0

- glibc-2.2.4-31.7
- make-3.79
- binutils-2.11.90.0.8-12
- gcc-2.96
- openmotif21-2.1.30-9

Red Hat Enterprise Linux 4.0

- glibc-2.3.4-2.9
- make-3.79
- binutils-2.15.92.0.2-13
- gcc-3.4.3-22.1
- libaio-0.3.96
- glibc-common-2.3.4-2.9
- setarch-1.6-1
- pdksh-5.2.14-30
- openmotif21-2.1.30-11
- sysstat-5.0.5-1
- gnome-libs-1.4.1.2.90-44.1
- libstdc++-3.4.3-22.1
- libstdc++devel-3.4.3-22.1
- compat-libstdc++-296-2.96-132.7.2
- compat-db-4.1.25-9
- control-center-2.8.0-12
- xscreensaver-4.18-5.rhel4.2

SUSE Linux Enterprise Server 9

- glibc-2.2.4-31.7
- make-3.79
- binutils-2.11.90.0.8-12
- gcc-2.96
- openmotif21-2.1.30-11

Note: To check if the required operating system packages have been installed on your system, enter the following command:

```
rpm -qa | grep <package name>
```

B.1.2 Required Packages on Solaris

The following (or later) package versions must be running on your Solaris systems:

- SUNWarc
- SUNWbtool
- SUNWhea
- SUNWlibm
- SUNWlibms
- SUNWsprot
- SUNWsprox

- SUNWtoo
- SUNWi1of
- SUNWxwfnt

To check if the required operating system packages have been installed on your system, enter the following command:

```
prompt> pkginfo SUNWarc SUNWbtool SUNWhea SUNWlibm SUNWlibms SUNWsprot SUNWsprox
SUNWtoo SUNWi1 of SUNWxwfnt
```

Note: If any packages are missing, contact your system administrator.

B.1.2.1 Checking for 32-Bit and 64-Bit Application Support

Check whether or not your system is configured to support 32-bit and 64-bit applications by entering the following command:

```
prompt> /usr/bin/isainfo -v
```

B.1.2.2 Required Patches

The patches required for the different Solaris versions are the following:

Solaris 8

- 108652-74 or later: X11 6.4.1: Xsun patch
- 108921-18 or later: CDE 1.4: dtwm patch
- 108940-57 or later: Motif 1.2.7 and 2.1.1: Runtime library patch
- 108773-18 or later: IIIM and X input and output method patch
- 111310-01 or later: /usr/lib/libdhcpagent.so.1 patch
- 109147-26 or later: Linker patch
- 111308-04 or later: /usr/lib/libmtmalloc.so.1 patch
- 111111-03 or later: /usr/bin/nawk patch
- 112396-02 or later: /usr/bin/fgrep patch
- 110386-03 or later: RBAC feature patch
- 111023-02 or later: /kernel/fs/mntfs and /kernel/fs/sparcv9/mntfs patch
- 108987-13 or later: Patch for patchadd and patchrm
- 108528-26 or later: Kernel update patch
- 108989-02 or later: /usr/kernel/sys/acctctl and /usr/kernel/sys/exacctsys patch
- 108993-45 or later: LDAP2 client, libc, libthread and libnsl libraries patch
- 111023-02 or later: Unable to load fontset ... iso-1 or iso-15

Solaris 9

- 113096-03 or later: X11 6.6.1: OWconfig patch
- 112785-35 or later: X11 6.6.1: Xsun patch

Solaris 10

- 113096-03 or later: X11 6.6.1: OWconfig patch
- 112785-35 or later: X11 6.6.1: Xsun patch

B.1.2.3 Checking for Patches

To determine the patches that have been installed on the system, follow these steps:

1. Run the `showrev` command with the `-p` option. The following command saves the sorted output to a file called `patchList`.
2. Enter the following command:

```
prompt> showrev -p | sort > patchList
```

3. Open the file in a text editor and search for the patch numbers.

> **Note:** If the required patches have not been installed, you can download them from http://sunsolve.sun.com.

B.1.3 Required Packages on HP-UX

The following (or later) package versions must be running on your HP-UX systems:

HP-UX 11i V1 (11.1)

- For installation on HP-UX 11.11, the following packages or later versions are required:
  - HP-UX 11i June 2003 Consolidated Quality Patch Bundle
  - Jun03GQPK11i_Aux_Patch
- Make sure that Motif 2.1 Development Environment (X11MotifDevKit.MOTIF21-PRG)B.11.11.01 is installed

  Either install this package or create symbolic links as follows:

  1. Log in as `root`.
  2. Change directory to `/usr/lib` as follows:

     ```
     # cd /usr/lib
     ```

  3. Create the required links:

     ```
     # ln -s libX11.3 libX11.sl
     # ln -s libXIE.2 libXIE.sl
     # ln -s libXext.3 libXext.sl
     # ln -s libXhp11.3 libXhp11.sl
     # ln -s libXi.3 libXi.sl
     # ln -s libXm.4 libXm.sl
     # ln -s libXp.2 libXp.sl
     # ln -s libXt.3 libXt.sl
     # ln -s libXtst.2 libXtst.sl
     ```

- The following patches or later are required:
  - PHCO_28123, cumulative SAM patch
  - PHKL_29198, Psets Enablement Patch
  - PHNE_28476, Cumulative STREAMS Patch

  - PHNE_28923, LAN product cumulative patch
  - PHSS_28871, ld(1) and linker tools cumulative patch
  - PHSS_28880, HP aC++ -AA runtime libraries (aCC A.03.50)
  - PHCO_26331, mountall cumulative patch
  - PHCO_29109, Pthread enhancement and fixes
  - PHKL_25468, eventport (/dev/poll) pseudo driver
  - PHKL_25842, Thread Abort
  - PHKL_25993, thread nostop for NFS, rlimit, Ufalloc fix
  - PHKL_25994, Thread NOSTOP, Psets Enablement, Ufalloc
  - PHKL_25995, eventport syscalls; socket close(2); Ufalloc
  - PHKL_26468, Shared mutex synchronization support patch
  - PHKL_28489, copyin EFAULT, LDCD access type
- To determine whether or not a bundle, a product, or file set is installed, enter a command similar to the following, where *level* refers to the bundle, patch or file set.

```
# /usr/sbin/swlist -l level |more
```

HP-UX 11i V2 (11.23)

- For installation on HP-UX 11.23, the following packages or later versions are required:
  - Patch Bundle for HP-UX 11i V2 (B.11.23), September 2004
  - BUNDLE11i, Revision B.11.23.0409.3
- The following patches or later are required:
  - PHSS_31849:linker + fdp cumulative patch
  - PHSS_31852: aC++ Runtime (PA A.03.61)

B.1.4 Required Packages on AIX

The follwoing packages must be running on your AIX systems:

AIX 5L Version 5.2

The following file sets must be installed and committed:

- bos.adt.base
- bos.adt.lib
- bos.adt.libm
- bos.perf.libperfstat
- bos.perf.perfstat
- bos.perf.proctools

The following Authorized Problem Analysis Reports (APARs) must be installed:

- IY43980: libperfstat.h not ANSI-compliant
- IY44810: DSI IN BMRECYCLE

- IY45462: Definition of isnan() in math.h incorrect
- IY45707: J2 READAAHEAD/CIO INTERACTION
- IY46214: dropping partial connections leaves them on so_q0
- IY46605: exec of 32 bit application can fail on 64 bit kernel
- IY48525: SDK 1.4.1 32-BIT SR1: CA141-20030930
- IY51801: race condition in aio_nwait_timeout
- IY76141: CHILD PROCESS UNABLE TO LOAD A MODULE. (If AIX 5.2 Maintenance Level 07)

AIX 5L Version 5.3

The following file sets must be installed and committed:

- bos.adt.base
- bos.adt.lib
- bos.adt.libm
- bos.perf.libperfstat
- bos.perf.perfstat
- bos.perf.proctools

The following Authorized Problem Analysis Reports (APARs) must be installed:

- IY70159: KRTL relocation problem
- IY66513: Parsing of LDR_CNTRL value fails
- IY68989: write to mapped space hangs
- IY76141: CHILD PROCESS UNABLE TO LOAD A MODULE. (If AIX 5.2 Maintenance Level 07)

B.1.4.1 To Verify Whether the Filesets Are Installed and Committed

To determine whether or not the required file sets are installed and committed, execute the foollowing command:

```
# lslpp -l bos.adt.base bos.adt.lib bos.adt.libm \
bos.perf.perfstat bos.perf.libperfstat
```

> **Note:** If a file set is not installed and committed, you need to install it. Refer to your operating system or software documentation for information on handling file sets.

B.1.4.2 Verify Whether or Not APAR is Installed

To determine whether or not an authorized program analysis report (APAR) is installed, execute the following command:

```
# /usr/sbin/instfix -i -k " IY43980, IY44810,..."
```

Note: If an APAR is not installed, you need to install it. For installing and downloading the APAR, refer to:

`https://techsupport.services.ibm.com/server/aix.fdc`

B.2 Kernel Parameter Requirements

The following sections list the kernel parameter requirements for each platform.

B.2.1 Kernel Parameter Requirements on Linux

The systems must have at least the following recommended kernel parameters:

Red Hat Enterprise Linux 3.0 and **SUSE Linux Enterprise Server 9**

- semmsl = 250
- semmns = 32000
- semopm = 100
- semmni = 128
- shmmax = 2147483648
- shmmni = 4096
- shmall = 2097152
- shmmin = 1
- shmseg = 10
- filemax = 65536

Red Hat Enterprise Linux 4.0

- semmsl = 250
- semmsl2 = 250
- semmns = 32000
- semopm = 100
- semmni = 128
- shmmax = 536870912
- shmmni = 4096
- shmall = 2097152
- filemax = 65536
- ip_local_port_range = 1024 65000
- rmem_default = 262144
- rmem_max = 262144
- wmem_default = 262144
- wmem_max = 262144

To check your kernel parameter settings, run the commands listed in Table B–1.

Table B–1 Execute Commands to Check Kernel parameter Settings

Parameter	Command
semmsl, semmns, semopm, semmni	`# /sbin/sysctl -a | grep sem`[1]
shmall, shmmax, shmmni	`# /sbin/sysctl -a | grep shm`
file-max	`# /sbin/sysctl -a | grep file-max`
ip_local_port_range	`# /sbin/sysctl -a | grep ip_local_port_range`
rmem_default	`# /sbin/sysctl -a | grep rmem_default`
rmem_max	`# /sbin/sysctl -a | grep rmem_max`
wmem_default	`# /sbin/sysctl -a | grep wmem_default`
wmem_max	`# /sbin/sysctl -a | grep wmem_max`

[1] This command displays the value of the four semaphore parameters in the order listed.

To change your kernel parameter settings, use any text editor to create or edit the `/etc/sysctl.conf` file to add or modify the necessary entries. You may need to restart your system after changing kernel parameters.

> **Note:** Include lines only for the kernel parameter values that you want to change. For the semaphore parameters (`kernel.sem`), you must specify all four values in order.
>
> If the current value of any of your system's kernel parameters is higher than the recommended value, keep your current value.

For example, your `/etc/sysctl.conf` file may look like this:

```
kernel.shmall = 2097152
kernel.shmmax = 536870912
kernel.shmmni = 4096
kernel.sem = 250 32000 100 128
fs.file-max = 65536
net.ipv4.ip_local_port_range = 1024 65000
rmem_default = 262144
rmem_max = 262144
wmem_default = 262144
wmem_max = 262144
```

By specifying the values in the `/etc/sysctl.conf` file, they persist when you restart the system.

On SUSE systems only, enter the following command to ensure that the system reads the `/etc/sysctl.conf` file when it restarts:

```
# /sbin/chkconfig boot.sysctl on
```

B.2.2 Kernel Parameter Requirements on Solaris

The system must have at least the following recommended kernel parameters:

Solaris 8 and 9

Verify that the following kernel parameters have been set to a equal to or greater than the value specified in Table B–2.

Table B–2 Recommended Kernel Parameter Values for Solaris 8 and 9

Parameter	Recommended Value
noexec_user_stack	1
semsys:seminfo_semmni	100
semsys:seminfo_semmsl	256
shmsys:shminfo_shmmax	4294967295
shmsys:shminfo_shmmin	1
shmsys_shminfo_shmmni	100
shmsys:shminfo_shmseg	10

Note: The following parameters are obsolete in Solaris 9:

- `semsys:seminfo_semmni`
- `shmsys:shminfo_shmseg`

Solaris 10

On Solaris 10, verify that the kernel parameters shown in Table B–3 are set to values equal to or greater than the recommended values. Table B–3 also lists the resource controls that replace the `/etc/system` file for a specific kernel parameter.

Table B–3 Recommended Kernel Parameter Values for Solaris 10

Parameter	Resource Control	Recommended Values
noexec_user_stack	NA	1
semsys:seminfo_semmni	project.max-sem_ids	100
semsys:seminfo_semmsl	project.max-sem-nsems	256
shmsys:shminfo_shmmax	project.max-shm-memory	4294967295
shmsys:shminfo_shmni	project.max-shm-ids	100

B.2.2.1 View and Change Kernel Parameter Values on Solaris 8 and 9

To view the current values of the kernel parameters, enter the following commands:

```
# grep noexec_user_stack/etc/system
# /usr/sbin/sysdef | grep SEM
# /usr/sbin/sysdef | grep SHM
```

To change any of the current values, follow these steps:

1. Create a backup copy of the `/etc/system` file, by using a command similar to the following:

   ```
   # cp /etc/system/etc/system.orig
   ```

2. Open the `/etc/system` file in any text editor, and if required, add lines similar to the following (edit the lines if the file already contains them):

   ```
   set noexec_user_stack=1
   set semsys:seminfo_semmini=100
   set semsys:seminfo_semmsl=256
   set semsys:seminfo_semvmx=32767
   ```

```
set shmsys:shminfo_shmmax=4292967295
set shmsys:shminfo_shmmin=1
set shmsys:shminfo_shmmni=100
set shmsys:shminfo_shmseg=10
```

3. Enter the following command to restart the system

```
# /usr/sbin/reboot
```

4. After you have restarted the system, log in to the system and switch to the `root` user.

B.2.2.2 View and Change Kernel Parameter Values on Solaris 10

To view the current values of the resource control, enter the following commands:

```
#id -p //to verify the project ID
uid = 0 (Root) gid = 0 (Root) projid = 1 (user.root)
#prctl -n project.max-shm-memory -i project user.root
#prctl -n project.max=sem-ids -i project user.root
```

To change any of the current values, follow these steps:

1. To modify the value of `max-shm-memory` to 6GB:

```
#prctl -n project.max-shm-memory -v 6gb -r -i project user.root
```

2. To modify the value of `max-sem-ids` to 256:

```
#prctl -n project.max-sem-ids -v 256 -r -i project user.root
```

B.2.3 Kernel Parameter Requirements on HP-UX

Verify that the kernel parameters listed in Table B–4 are set to the values greater than or equal to the recommended value shown. The procedure following Table B–4 describes how to verify and set the values.

Table B–4 Recommended Parameter Values for HP-UX

Parameter	Recommended Value
ksi_alloc_max	32768
max_thread_proc	256
maxdsiz	1073741824
maxdsiz_64bit	2147483648
maxssiz	134217728
maxssiz_64bit	1073741824
maxswapchunks	16384
maxuprc	3687
msgmap	4098
msgmni	4096
msgseg	32767
msgtql	4096
ncsize	34816
nfile	63488

Table B–4 (Cont.) Recommended Parameter Values for HP-UX

Parameter	Recommended Value
nflocks	4096
ninode	34816
nkthread	7184
nproc	4096
semmap	4098
semmni	4096
semmns	8192
semmnu	4092
semvmx	32767
shmmax	1073741824
shmmni	512
shmseg	120
vps_ceiling	64

Note: The following parameters are obsolete in HP-UX 11.23:

- `maxswapchunks`
- `semmap`

If the current value of any parameter is higher than the value listed in this table, do not change the value for that parameter.

B.2.3.1 View and Change Kernel Parameter Values

To view the current value of these kernel parameters, and to change them, if necessary, follow these steps:

1. Set the DISPLAY environment variable to specify the display of the local system. This is an optional step.

   Bourne, Bash or Korn shell:

   ```
   $ DISPLAY=localhost:0.0; export DISPLAY
   ```

   C Shell

   ```
   $ setenv DISPLAY localhost:0.0
   ```

2. Start System Administration Manager (SAM)

   # /usr/sbin/sam

3. Choose the Kernel Configuration area and the Configurable Parameters area.
4. Check the value or formula specified for each of these parameters and if necessary, modify that value or formula. Refer to the SAM Online Help for more details.
5. Exit from SAM.
6. If you have modified the value for any of the parameters, you must restart your system.

```
# /sbin/shutdown -r now
```

7. After you have restarted the system, log in and switch to the `root` user if necessary.

B.2.4 Configure Shell Limits and System Configuration Parameters on AIX

On AIX systems, you do not need to configure the kernel parameters. However, Oracle recommends that you set shell limits and system configuration parameters as described in this section.

B.2.4.1 Configuring Shell Limits

Verify that the shell limits shown in Table B–5 are set to the values shown. The procedure following the table describes how to verify and set the values.

Table B–5 Shell Limits

Shell Limit (as shown in smit)	Recommended Value
Soft FILE size	-1 (Unlimited)
Soft CPU size	-1 (Unlimited)
Soft DATA segment	-1 (Unlimited)
Soft STACK size	-1 (Unlimited)

Do the following to view and change the values that are currently specified for these shell limits:

1. Execute the following command:

```
# smit chuser
```

2. In the User Name field, specify the user name of the Oracle software owner, for example `oracle`.
3. Scroll down the list and verify whether the value for the soft limits is `-1`. If not, edit the existing value as recommended in Table B–5.
4. When you have finished making changes, press **F10** to exit.

B.2.4.2 Specifying System Configuration Parameters

Ensure the maximum number of processes allowed per user is set to 2048 or higher. The following procedure describes how to verify and set the value.

To specify the system configuration parameters:

1. Execute the following command:

```
# smit chgsys
```

2. Ensure the value shown for Maximum Number of Processes allowed per user is greater than or equal to 2048. If not, edit the existing value.
3. When you have finished making changes, press **F10** to exit.

C

Agent Deploy Application - Installation Prerequisites

This appendix describes the prerequisites to performing an installation using the Agent Deploy application. It contains the following sections:

- Prerequisites
- Prerequisite Checks Executed by Agent Deploy
- Troubleshooting Failed Prerequisite Checks

C.1 Prerequisites

The following prerequisites must be met before proceeding with the installation:

- Verify if the package requirements for each platform are met. See
- SSH (Secure Shell) User Equivalence is set up
- Validate all command locations
- Modify response file for Big IP host and port
- Verify `oraInventory` permissions on remote hosts
- Verify if user installing the agent is same as the user that installed Oracle Application Server and Oracle Collaboration Suite.
- Verify if the Target Monitor Check and Host Name Check are the same for all platforms.
  - Target Monitor Checks: The agent will not be able to monitor those targets that have been installed by different users.
  - Host Name Check: The name of the host on which the installation is being performed should neither be `localhost.localdomain` nor an IP address. It must be a valid host name.

C.1.1 Check Platform-Specific Package Requirements for Agent Installation

Table C–1 lists the packages and disk space requirements for each platform.

Table C–1 Platform-Specific Packages and Disk Space Requirements

Operating System	Platform	Packages	Disk Space for Installation
Solaris	Solaris 5.8 SPARC	■ SUNWarc ■ SUNWbtool ■ SUNWhea ■ SUNWlibm, ■ SUNWlibms ■ SUNWsprot ■ SUNWsprox ■ SUNWtoo ■ SUNWi1of ■ SUNWxwfnt	0.85 GB
	Solaris 5.9 SPARC	■ SUNWlibm ■ SUNWlibms ■ SUNWsprot ■ SUNWsprox ■ SUNWtoo ■ SUNWi1of ■ SUNWxwfnt	0.85 GB
	Solaris 5.10 SPARC	SUNWbtool	0.85 GB
HP-UX	HP-UX 11.11 PA-RISC2.0	■ X11MotifDevKit version 0.0 ■ X11MotifDevKit.MOTIF21-PRG version 0.0	1.5 GB
	HP-UX 11.23 PA-RISC2.0	BUNDLE11i version B.11.23.0409.3	1.5 GB
IBM-AIX	AIX 5200	bos.perf.proctools version 0.0	1.5 GB
	AIX 5300	bos.perf.proctools version 0.0	1.5 GB
Linux Itanium	Red Hat Enterprise Linux AS/ES 3.0 ia 64	■ GLIBC>=2.3.2-95.27 ■ Make version 3.79 ■ binutils version 2.14 ■ Libaio version 0.3.96	0.75 GB
	Red Hat Enterprise Linux AS/ES 4.0 ia 64	■ GLIBC>=2.3.2-95.27 ■ Make version 3.79 ■ binutils version 2.14 ■ Libaio version 0.3.96 ■ gcc version 3.2	0.75 GB

Table C–1 (Cont.) Platform-Specific Packages and Disk Space Requirements

Operating System	Platform	Packages	Disk Space for Installation
	SUSE Linux Enterprise Server 9 ia 64	■ GLIBC>=2.3.3-98.28 ■ Make version 3.80 ■ binutils version 2.14 ■ Libaio version 0.3.102 ■ gcc version 3.3	0.75 GB

C.1.2 Set Up SSH (Secure Shell) User Equivalence

You must set up SSH (Secure Shell) prior to deploying the Management Agent using the Agent Deploy application. This is required as the Agent Deploy application uses SSH and SCP as modes of communication between nodes. Setting up the user equivalence helps avoid SSH authentication calls during future Agent Deploy operations.

> **Caution:** The SSH User Equivalence must always be set between the target hosts and the OMS, and never among the target hosts.

In order to set up SSH, you must execute the `sshUserSetup.sh` script (`sshUserSetupNT.sh` on Microsoft Windows) that is available at the following location:

```
OMS_HOME/sysman/prov/resources/scripts
```

The SSH connectivity script should be used for 10.2.0.2 Management Agent when establishing connectivity with both Windows and Linux targets.

If 10.2.0.1 Management Agent is in use, then `sshUserSetup.sh` needs to be used for Linux and `sshUserSetupNT.sh` is to be used for Windows hosts. Refer to section 5 of the Agent Best Practice paper available at http://www.oracle.com/technology/products/oem/pdf/10gr2_agent_deploy_bp.pdf.

C.1.2.1 Setting Up SSH User Equivalence Using sshConnectivity.sh

The `sshConnectivity.sh` script is used on UNIX/Microsoft Windows platforms to set up SSH user equivalence from the (local) host on which it is run, to the specified remote hosts. After this script is executed, you can use SSH to run commands on the remote hosts, or copy files between the local and the remote hosts without being prompted for passwords or confirmations.

Before executing this script, you must ensure that the following environment variables are set:

- `ORACLE_HOME`

  Set this to the OMS home as an environment variable using the following command:

  For CSH shell

  ```
  setenv ORACLE_HOME /scratch/OracleHomes/oms10g
  ```

  For BASH shell

```
export ORACLE_HOME= /scratch/OracleHomes/oms10g
```

- SSH_LOC

  You need not specify this if the ORACLE_HOME variable has already been set. If it has not been set, ensure that this value points to the directory that contains the SSH and remote interfaces JARS files (ssh.jar, remoteinterfaces.jar, jsch.jar).

- OUI_JAR

  You need not specify this if the ORACLE_HOME variable has already been set. If this variable has not been set, ensure that this value points to the OUI home directory.

- JAVAHOME

  You need not specify this if the ORACLE_HOME variable has already been set. If this variable has not been set, ensure that this value points to the JAVA home directory.

Note: All these variables can also be passed as command-line variables to the script in the form of var=value.

C.1.2.1.1 sshConnectivity.sh Script Usage The usage of this script is as follows:

```
./sshConnectivity.sh -user <username> -hosts <space separated
hostlist> | -hostfile <absolute path of cluster configuration file>
[-asUser <user for which the setup needs to be done on the local machine, for
example,SYSTEM>
[-asUserGrp <group that the specified asUser belongs to>]
-sshLocalDir <windows style full path of dir where keys should be
generated on the local machine for asUser>] [ -advanced ]
[-usePassphrase] [-logfile <absolute path of logfile> ] [-confirm]
[-shared] [-verify] [-exverify] [-remotePlatform <platform id (linux:46,
solaris:453, msplats:912>] [-obPassword <obfuscated password>] [-silent]
[-localPlatformGrp <unix,win>] [help]
```

Example C–1 Usage of the sshConnectivity.ch Script to Set Up User Equivalence on Local UNIX Platforms (Linux, Solaris, HP-UX, and IBM AIX)

```
./sshConnectivity.sh -user <username> -hosts <space separated
hostlist> | -hostfile <absolute path of cluster configuration file>
[-remotePlatform <platform id (linux:46, solaris:453, msplats:912>]
[-shared] [-confirm]
```

For example,

```
./sshConnectivity.sh -user pjohn -hosts sidtest1
./sshConnectivity.sh -user alhammel -hosts zeke2 -remotePlatform 453
```

Example C–2 Usage of the sshConnectivity.ch Script to Set Up User Equivalence on Local Microsoft Windows Platforms

```
./sshConnectivity.sh -user
<username> -localPlatformGrp win -asUser <user for which the setup needs to
be done on the local machine, for example, SYSTEM> [-asUserGrp <group that the
specified asUser belongs to>] -sshLocalDir <Windows style full
path of dir where keys should be generated on the local machine for
asUser> -hosts <space separated hostlist> | -hostfile <absolute path of
cluster configuration file> [-remotePlatform <platform id (linux:46,
solaris:453, msplats:912>] [-shared] [-confirm]
```

For example,

1. Go to the Cygwin BASH prompt and execute `cd /`
2. Execute `mkdir .ssh`
3. Now, execute the script as follows:

```
./sshConnectivity.sh -user alhammel -localPlatformGrp win -asUser SYSTEM
-asUserGrp root -sshLocalDir C:\cygwin\.ssh -hosts scrat2
```

> **Note:** Specify all the paths in double quotation marks (" ").

Parameter Description

- *-user*

  This is the user on remote hosts.

- *-hosts*

  This specifies space-separated remote hosts list.

- *-hostfile*

  You can specify the host names either through the `-hosts` option, or by specifying the absolute path of a cluster configuration file. A sample of the host file content is as follows:

```
scrat02 scrat02int 10.1.0.0 scrat02v -
scrat06 scrat06int 10.1.0.1 scrat06v -
```

> **Note:** The first column in each row of the host file will be used as the host name.

- *-localPlatformGrp*

  Specify this option if the local platform is Microsoft Windows. The default value of this option is `unix`.

- *-remotePlatform*

  You must specify this option is the remote platform is not the same as the local platform. Here, you must specify the platform ID of the remote platform. You can find the platform IDs of the supported platforms in the `platforminfo.properties` file.

> **Caution:** When you are executing this script on a Microsoft Windows OMS machine, ensure it is executed from within the Cygwin `BASH` shell. This script will fail to execute if run from outside this location.

C.1.2.2 Setting Up SSH on UNIX Using sshUserSetup.sh

Usage of this script is as follows:

```
sshUserSetup.sh -hosts "<hostlist>" -user <user name> [-verify] [-confirm]
[-shared]
```

For example, `sshUserSetup.sh -hosts "host1 host2" -user sjohn`

Description

This script is used to set up SSH user equivalence from the host on which it is run to the specified remote hosts. After this script is run, you can use SSH to execute commands on the remote hosts, or copy files between the local host and the remote hosts without being prompted for passwords or confirmations.

The list of remote hosts and their user names are specified as command-line parameters to the script.

- *-shared*

  In case you have the home directory NFS-mounted or shared across the remote hosts, the script should be used with the `-shared` option.

  To determine whether or not an Oracle Home Directory is Shared or Not Shared, consider a scenario where you want to determine whether the Oracle home directory of *user1* is shared across hosts A, B, and C or not.

  You can determine this by following these instructions:

  1. On host A, `touch ~user1/checkSharedHome.tmp`.
  2. On hosts B and C, execute `ls -al ~user1/checkSharedHome.tmp`.

     If the file is present on hosts B and C in the `~user1` directory and is identical on all nodes, it means that the user's home directory is shared.
  3. On host A, `rm -f ~user1/checkSharedHome.tmp`.

  Note: In the event that you accidentally pass the `-shared` option for nonshared homes or reverse, the SSH equivalence is set up for only a subset of the hosts. You will have to rerun the setup script with the correct option to rectify this issue.

- *-verify*

  The `-verify` option allows you to verify if SSH has been set up. In this case, the script does not set up SSH, but only checks if *SSH user equivalence* has been set up from the local host to the remote hosts. It then runs the date command on each remote host using SSH. In case you are prompted for a password or see a warning message for a particular host, it means the `SSH user equivalence` has not been set up correctly for that host.

  In case the `-verify` option is not specified, the script sets up SSH and then does the verification as well.

- *-confirm*

  The `-confirm` option allows you to set up SSH user equivalence with a forced change in the permissions on remote hosts. This means that the script will not prompt you to confirm the change in permissions, if you execute the script passing the `-confirm` option.

- *-help*

  Use this option to view the readme file for the `sshUserSetup.sh` script. The usage is as follows:

  ```
  sshUserSetup.sh -help
  ```

The following examples provides usage of the previously mentioned options:

```
Local host = Z
Remote Hosts = A, B, and C
Local user = sjohn
Remote users = foo (non-shared)
aime (shared)
./sshUserSetup.sh -user foo -hosts "A B C" -confirm
```

Example C–3 Set Up SSH User Equivalence and Verify the Setup

```
sshUserSetup.sh -hosts "A B C" -user foo
```

This script sets up `user equivalence` from:

- Z to A
- Z to B
- Z to C

Example C–4 Set Up SSH User Equivalence and verify the Setup Without a Confirmation Prompt

```
sshUserSetup.sh -hosts "A B C" -user foo -confirm
```

This sets up SSH between the local host and A, B, C. It also verifies the setup. However, due to the usage of the `-confirm` option, it assumes that users are aware of the changes that would be made on the systems and will not ask for any confirmation.

Example C–5 Verify Existing SSH User Equivalence Setup

```
./sshUserSetup.sh -hosts "A B C" -user foo -verify
```

Because the `-verify` option is specified, the script does not set up the SSH setup, but only verifies the existing setup.

C.1.2.3 Setting Up SSH Server (SSHD) on Microsoft Windows

Before starting with the SSHD setup, ensure you are not using OpenSSH and MKSNT when using the Agent Deploy application. The Agent Deploy application uses the complete Cygwin suite (full collection of the software tools packaged in Cygwin). To get the complete collection of Cygwin, do the following:

1. Ensure `OpenSSH\bin` and `mksnt` are not in your `%PATH%`. If they are, remove them by doing the following:
   a. Right-click on **My Computer** and go to Properties.
   b. In the System Properties window that appears, click **Advanced.**
   c. In this tab, click **Environment Variables.**
   d. Here, search for the Path system variable, select it, and if the `OpenSSH\bin` and `mksnt` are present in the PATH, click **Edit.**
   e. In the Edit System Variable dialog box that appears, delete these two values from the PATH, and click **OK.**
2. Now, stop the SSH Daemon if it is running from OpenSSH. To do this:
   a. Right-click on **My Computer**, and select **Manage.**

b. In the Computer Management window that appears, go to Services under Services and Applications.

c. In the right-pane, select the SSH daemon service and click the **Stop Service** icon.

Note: Ensure you rename the installation directories of `OpenSSH` and `MKSNT`.

---

3. To install the full suite of Cygwin software, go to `http://www.cygwin.com`, and install Cygwin in your `C:\cygwin` directory.

Note: If you are installing Cygwin into another directory than what has been previously mentioned, ensure you update the `$OMS_HOME/sysman/prov/resources/ssPaths_msplats.properties` file with the proper Cygwin binary values after installing Oracle Enterprise Manager Grid Control.

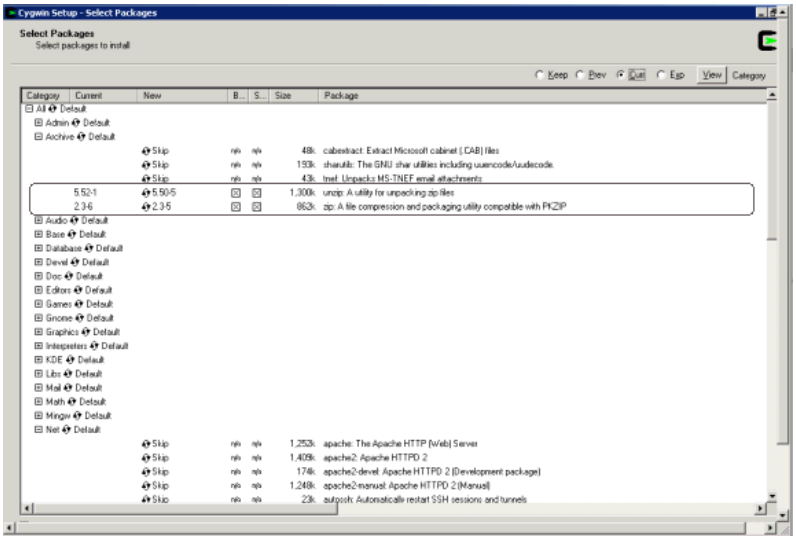
Caution: If you are installing *Cygwin* at a directory that is other than `C:\cygwin` on a remote machine, you must also ensure that Cygwin is installed on the OMS machine at the exact same location.

The Cygwin installation directory should not contain any spaces.

While installing Cygwin, ensure you choose the following binaries:

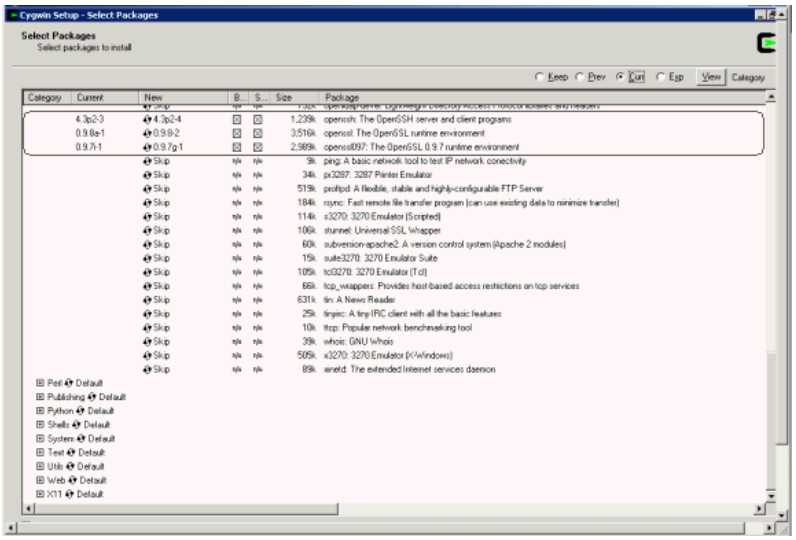
a. Zip, unzip binaries from the Archive package.

Figure C–1 Zip Unzip Binaries



b. OpenSSH and dependencies (automatically selected if you choose OpenSSH) from the Net package.

Figure C–2 Net Packages



4. Modify the `C:\cygwin\cygwin.bat` file to add the following line:

   ```
   set CYGWIN=binmode tty ntsec
   ```

5. Ensure `cygrunsrv` is installed by going to `C:\cygwin\bin` and executing the following:

   ```
   bash
   cygrunsrv -h
   ```

   Note: If you are prompted to provide a Cygwin value, enter `binmode tty ntsec`. If this returns an error message stating "service does not exist", you are on the right track, and can proceed to the next step.

   If you encounter any other error message, (for example, "*command cygrunsrv not found*"), see Section A.1.3.6, "Troubleshooting the "command cygrunsrv not found" Error." for more information on troubleshooting this issue.

6. Open a new command prompt and execute the following:

   ```
   bash
   ssh-host-config
   ```

Note: Enter "*no*" when prompted to create sshd user account (message reads "`sshd user account needs to be created`").

Enter "*yes*" at all other prompts.

When prompted to answer the question "Which value should the environment variable CYGWIN have when sshd starts?", Oracle recommends that you set the value to at least "ntsec" as shown in the following example. This will enable you to change the user context without having to specify the password.

As an answer to the previously mentioned question, specify a value that is similar to the following and press **Enter**:

```
CYGWIN="binmode tty ntsec"
```

7. Now, open the `/etc/passwd` file, and remove only those entries of the user that you will use to connect to the OMS machine.

   For example,

   - If the user that you are employing to connect to the OMS machine is a local user, execute the following:

     ```
     /bin/mkpasswd -l –u <USER> >> /etc/passwd
     ```

   - If the user you are employing to connect to the OMS machine is a domain user, execute the following:

     ```
     /bin/mkpaswd.exe -d -u <USER> >> /etc/passwd
     /bin/mkgroup.exe -d >> /etc/group


     mkdir -p /home/<USER>  (for example, mkdir -p /home/pjohn)
     chown <USER> /home/<USER> (for example, chown pjohn /home/pjohn)
     ```

8. Start the SSH daemon.

   If the user you are employing to connect to the OMS machine is a domain user, do the following:

   a. Right-click on **My Computer**, and select Manage.
   b. In the Computer Management dialog box that appears, go to Services and Applications, and select **CYGWIN sshd**.
   c. Right-click **CYGWIN sshd** and select Properties.
   d. In the Properties dialog box, go to the Log On tab.
   e. Here, specify the domain/username and password. Click **Apply.**
   f. Now, go to the CYGWIN command prompt, and execute the following:

      ```
      chmod 644 /etc/ssh*
         chmod <USERNAME> /var/empty
         chmod 755 /var/empty
         chmod 644 /var/log/sshd.log
      ```

Note: If `/var/log/sshd.log` does not exist, you do not have to execute the following command:

```
chmod 644 /var/log/sshd.log
```

g. Start the SSH daemon by executing:

```
/usr/sbin/sshd
```

Alternatively, from the same BASH prompt, you can also execute:

```
cygrunsrv -S sshd
```

Note: Use `cygrunsrv -E sshd` to stop the SSH daemon.

9. You can now test your `cygwin` setup.

   To do this, go to a different machine (that has the `ssh` client running), and execute the following command:

```
ssh -l <USERNAME> <localhost> 'date'

OR

ssh -l <USERNAME> <this node> 'date'
```

   For example,

```
ssh -l pjohn egal07.db.funds.com 'date'
```

   This command will prompt you to specify the password. When you specify the correct password, the command should return the accurate date.

C.1.2.4 Setting Up SSH on Microsoft WIndows Using sshUserSetupNT.sh

Note: Before executing the `sshUserSetupNT.sh` script, execute the following commands to ensure the home directory has been correctly set:

1. Execute `echo $HOME`

   Ensure this displays the home directory of the current user.

2. If it points to the home directory of another user, execute the following command:

```
export HOME=<Windows style absolute path of homedir>
```

3. Now, execute `echo $HOME` again, to verify the home directory. The `$HOME` value must be the same as that passed to `-homeDir`

This is the script that should be executed to set up user equivalence on Microsoft Windows platforms. The usage of the script is as follows:

```
./sshUserSetupNT.sh -user -asUser -asUserGrp -sshLocalDir -homeDir -hosts
-hostfile
```

For example, `./sshUserSetupNT.sh -user pjohn -asUser SYSTEM -asUserGrp root-sshLocalDir "C:\cygwin\.ssh" -homeDir "C:\Documents and Settings\pjohn" -hosts "host1 host2"`

Note: After the `SSHUserSetupNT.sh` script has been executed, you must verify the successful SSH user setup on all the hosts, individually.

That is, if you have run the script to set up user equivalence on two hosts (host1, and host2), you must run the following command on each host to verify successful SSH setup:

```
ssh -l <username> host1 'date'

and then run:

ssh -l <username> host2 'date'
```

Caution: You must execute the `sshUserSetupNT.sh` script on the local OMS machine from within the `cygwin` (BASH) shell only. The script will fail to execute if done from outside this location.

All the previously mentioned options are mandatory, and should be passed while executing the script.

Note: It is assumed that `C:/cygwin` is the default installation directory for the Cygwin binaries.

If you install `cygwin` at a location other than `c:\cygwin` (default location), it can cause the SSH setup to fail, and in turn, the agent installation will fail.

To work around this issue, you must either install `cygwin` in the default directory (`c:\cygwin`), or update the `ssPaths_msplats.properties` file with the correct path to the `cygwin` binaries.

You can look into the following remote registry key to find out the correct Cygwin path:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cygnus Solutions\Cygwin\mounts v2\/
```

Description

This script is used on Microsoft Windows platforms to set up SSH user equivalence from the host on which it is run to the specified remote hosts. After this script is run, you can use SSH to execute commands on the remote hosts, or copy files between the local host and the remote hosts without being prompted for passwords or confirmations.

The list of remote hosts and their user names are specified as command-line parameters to the script.

- *`-asUser`*

  This is the user of the local machine on which the setup must be performed. For example, SYSTEM.

- *-asuserGrp*

  This is the group to which the specified `asUser` belongs.

- *-sshLocalDir*

  This is the full path to the directory where the keys should be generated for the `asUser` on the local machine.

- *-homeDir*

  This is the full path to the home directory of the current user.

  If the `/home` key (in `regedit`) is seen as a subkey under the Cygnus Solutions key, then the value of the `/home` key must have `/<username>` as a suffix and then be used as `-homeDir`m value.

  If the `/home` key is not found, go to the Cygwin BASH prompt and check the value of `$HOME`. You can now use the same value of `$HOME` as the value for `-homeDir`.

  If `$HOME` does not have any value (is empty), then you must update the `/etc/passwd` file.

  Identifying the Correct Entry in the /etc/passwd File

  If the `/etc/passwd` file has only one entry for the user, you can simply modify that value. In the event that there are multiple entries in this file, you must first identify the correct entry and then modify it.

  To identify the correct entry:

  – Execute the following command if you have specified a local user during SSH setup:

    ```
    /bin/mkpasswd -l -u <username>
    ```

  – Execute the following command if you have specified a domain user during SSH setup:

    ```
    /bin/mkpasswd -d -u <username>
    ```

  Now, match the output with the corresponding entry in the `/etc/passwd` file. This is the entry that you must modify.

  Updating the -homeDir value

  All values for all users are listed as colon (:) separated entries (or fields). To update the user entry that you have identified previously, go to the penultimate value (or field) of that user entry, and modify the value of the home directory for that user.

  Always specify the absolute path needed by Cygwin as value for the home directory. For example, if the path is `C:\Documents and Settings\pjohn`, modify it to:

  ```
  /cygdrive/c/Documents and Settings/pjohn
  ```

  Or, if the path reads `C:\cygwin\pjohn`, modify this to:

  ```
  /cygdrive/c/cygwin/pjohn
  ```

  Now, save the password file and reenter the BASH shell.

Note: If you have used spaces in the `$HOME` value (for example, `/cygdrive/c/Documents and Settings/pjohn`), specify the `$HOME` value in Microsoft Windows style and within double quotation marks (for example, `"C:\ Documents and Settings\pjohn"`).

Note: Specify the full path within double quotation marks (" ").

Caution: You must execute the `sshUserSetupNT.sh` script on the local OMS machine from within the `cygwin` (BASH) shell only. The script will fail to execute if done from outside this location.

C.1.2.5 Setting Up the Timezone Variable on Remote Hosts

This section lists the steps you must follow to set up the timezone environment variable on remote hosts.

To verify if the timezone environment variable (TZ) is accessible by the SSH server on the remote hosts, execute the following command from the OMS host:

```
ssh -l <user_name> -n <remote_node> 'echo $TZ'
```

If this command does not return the TZ environment variable value, you must set the TZ variable and ensure this is accessible by the SSH server. You can set the TZ environment variable on remote hosts in the following sections:

C.1.2.5.1 Set the TZ variable and Restart the SSH Daemon

If the shell being used is BASH, add the following line to the `.bashrc` file in the home directory of the user (being used) for `ssh` access:

```
export TZ=<your machine's timezone>
```

If you are using a CSH shell, then add the following line to the `.cshrc` file in that directory:

```
setenv TZ <your machine's timezone>
```

1. Depending on the shell that is present on the host, set the TZ variable by executing the following command:

   ```
   For a CSH Shell, specify:
   setenv TZ PST8PDT
   ```

2. Restart the SSH daemon by executing:

   ```
   sudo /etc/init.d/sshd restart
   ```

3. Now, execute the following command from the OMS home to verify if the SSH server can access the TZ variable.

   ```
   ssh -l <user_name> -n <node_name> 'echo $TZ'
   ```

C.1.2.5.2 Set the TZ Variable in the "Shell rc" File

The timezone variable must be set in the `rc` file of the shell that the host is using.

For example, if the host is using a BASH shell, go to the user's home directory (`$HOME`) and add the following to the `~/.bashrc` file to set the TZ variable:

```
TZ=PST8PDT; export TZ
```

If the host is using a CSH shell, go to `$HOME` and add the following to the `~/.cshrc` file:

```
setenv TZ PST8PDT
```

Now, execute the following command from the OMS home to verify if the SSH server can access the TZ variable.

```
ssh -l <user_name> -n <node_name> 'echo $TZ'
```

Note: If `sshd` is not set up on remote box for `TZ`, you can pass this variable in the Additional Parameters text box using the `-z` option for default software source location (for install or upgrade) and the `s_timezone=<timezone>` option for a nondefault software location.

Note that this will perform the installation of agents on all remote nodes with the same timezone value that you specify in the Additional Parameters text box. See Appendix D, "Additional Parameters for Agent Deploy" for more information.

C.1.2.6 Dropping SSH Connection

For dropping SSH connection for 10.2.0.1 and 10.2.0.2 release, do the following on the Oracle Management Service machine:

1. For UNIX operating systems, remove the `$HOME/.ssh` folder (use the `rm -rf $HOME/.ssh` command). In the 10.2.0.1 release, $HOME is the home directory of the user who runs sshConnectivity.sh/sshUserSetup.sh.
2. For Windows operating systems, in the cygwin bash prompt, go to `$HOME` folder (use the cd $HOME command).

   Note: If $HOME value has spaces, for example, C:\Documents and Settings\foo\, make sure that you type the value of $HOME in double-quotes. For example:

   ```
   cd "C:\Documents and Settings\foo"
   ```

3. Remove the .ssh folder as follows:

   ```
   rm -rf .ssh
   ```

4. Navigate to `C:\cygwin`, which is the default folder where agentpush assumes you installed cygwin. If cygwin is installed in folder X, go to folder X. Remove the `.ssh` folder.

   Note: The sub-key value of `' SOFTWARE->Cygnus Solutions->Cygwin -> mounts v2->/'` is the installation directory of cygwin, by default. If you have changed it manually, go to that folder and remove the `.ssh` folder.

For Enterprise Manager 10.2.0.3.0 or higher, SSH is setup and dropped by the application itself. Dropping the SSH setup will bring back the previous existing setup, if any.

If SSH was set up by the user, by running `sshConnectivity.sh` and the application has used this existing setup, the user will need to follow the steps explained above for dropping SSH connection for 10.2.0.1 and 10.2.0.2 release. Dropping the SSH setup will not bring back any existing SSH setup.

C.1.2.7 Checking if SSH Connection is Removed

To check if SSH connection is removed, do the following:

1. Run the following command on the Oracle Management Service machine:

   ```
   ssh -l username <remote node> date
   sshConnectivity.sh/sshUserSetup.sh/sshUserSetupNT.sh
   ```

   where username is the value of the `-user` option used while running and remote node is one of the nodes used in the `-hosts` argument while running. For example:

   ```
   sshConnectivity.sh/sshUserSetup.sh/sshUserSetupNT.sh
   This command should NOT show date output. This command must stop for password
   conformation to proceed.
   For Example:
   $ssh -l john mybox.mydomain.com 'date'
   The authenticity of host 'mybox.mydomain.com (111.222.333.444)' can't be
   established.
   RSA key fingerprint is ec:52:5d:63:bc:85:07:ef:fe:5b:74:d3:6b:18:04:1c.
   Are you sure you want to continue connecting (yes/no)?
   ```

The above message ensures that the SSH connection is dropped from the Oracle Management Service to the remote node.

C.1.3 Validate All Command Locations

The properties files located at `<omshome>/sysman/prov/resources/` comprises the default locations of commands that are required for successful execution of certain application programming interfaces (APIs), for example, the `ping` executable.

Such command locations can vary between machines and platforms. Run the `Validatepaths` script to verify whether the command locations in the properties file are correct. This script provides a list of commands that are not found in the default locations.

Run the following command to execute this script:

```
./validatePaths -dirloc oms/sysman/prov/resources/
In the preceding example (of the ping executable), if the executable is present in
/usr/sbin/ping, which is not the default location, you must specify this value in
the userpaths.properties file by specifying PING_PATH=/usr/sbin/ping.
```

The properties files that are loaded by the Agent Deploy application are the following:

- *platforminfo.properties*

  Contains a list of files that need to be loaded for each platform. These files specify the paths for the commands. For example, `/bin/ping`.

  - `Paths.properties`

This file contains the arguments that need to be passed everytime the commands listed in this file are executed.

– `sPaths.properties`

  This is a generic file that contains the paths for all commands that need to be executed, regardless of the platform.

– `ssPaths_<platform>.properties`

  This is a platform-specific file and contains the commands that need to be executed for that platform. For example, `ssPaths_sol.properties`.

Caution: On Microsoft Windows platforms, the path to the `cygwin` binaries is hardcoded in the `ssPaths_msplats.properties` file. If you install `cygwin` at a location other than `c:\cygwin` (default location), it can cause the agent installation to fail.

To work around this issue, you must either install `cygwin` in the default directory (`c:\cygwin`), or update this properties file with the correct path to the `cygwin` binaries.

You can look into the following remote registry key to find out the correct Cygwin path:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cygnus Solutions\Cygwin\mounts v2\/
```

– `userPaths.properties`

  This file lists all the variables that are used to specify the command paths. You must uncomment the variables that you want to use, and specify appropriate values.

Caution: The files that comprise each properties file are loaded in the ascending order of their precedence. This means that values you specify in the last file that is loaded will override the values for the same property in the previous files.

For example, the `platforminfo.properties` file comprises `paths.properties`, `spaths.properties`, `ssPaths.properties`, and `userPaths.properties`.

If the default location for the ping executable in `sPaths.properties` file is `usr/bin/ping`, and you specified an alternative location in the ssPaths.properties file as `usr/sbin/ping`, the value in the latter file takes precedence over the others.

Note: If you want to include other command variables, you can either choose to specify these variables in any of these `s*Paths.properties/userPaths.properties` files, or create another properties file and specify its name in `platforminfo.properties`.

Ensure these files are part of the `platforminfo.properties` file. If they are not, Agent Deploy ignores the paths to the executables that you have specified in these files and attempts to run the executables from their default locations.

Sample property files are provided at the end of this appendix under Sample Properties Files.

- `system.properties`

  This file contains properties that help you control the activity and performance of the application. For example:

  - `oracle.system.prov.threadpoolsize`

    Number of threads that get created in the application and work in parallel to execute commands on remote hosts. The default threadpool size value that is set for Agent Deploy is 32. You can specify an appropriate value for the threadpool size in this property.

    For example `oracle.sysman.prov.threadpoolsize=128`.

  - `oracle.sysman.prov.threadpoolmaxsize`

    Number of threads that can increase dynamically depending on the workload.

    The default value used in the application is 256 (`oracle.sysman.prov.threadpoolmaxsize=256`). You can specify an appropriate maximum value for the threadpool size in this property.

- `ignoreMessages.txt`

  If there are error messages displayed in the error stream that you know can be ignored in the setup, you can update these messages in the `ignoreMessages.txt` file.

  Generally, if the error stream contains data when you execute any command, it is assumed that the command failed. But the data in the error stream may not always correspond to the error. So, to ignore such error messages, you must add these messages (including the banner) to the `ignoreMessages.txt` file.

```
Consider the following example:
When you run /usr.local/bin/sudo on a remote machine, it writes the following
messages on to the error stream:
Administrator. It usually boils down to these two things:
#1) Respect the privacy of others.
#2) Think before you type.

Password:
This essentially, is just a warning to the user and does not constitute the
failure of the executed command.
Such error messages can be added to the ignore_Message.txt file.
```

  Note: The data format for these files mandates only one property per line. You must specify the property values in the format: `variable=value`.

C.1.3.1 Location of Properties File

You can view the following properties files at `<OMS_HOME>/sysman/prov/resources/`:

- platformInfo.properties
- Paths.properties
- sPaths.properties
- ssPaths_sol.properties

- userPaths.properties
- system.properties
- ignoreMessages.txt

C.1.3.2 Location of Installation Logs

See Appendix F, "Installation and Configuration Log File Locations" for more information on the various installation and configuration logs that are created, and their locations.

C.1.4 Modify Response File for Big IP Host and Port

If the Management Service is using a load balancer, you must modify the `s_omsHost` and `s_OMSPort` values in the `<omshome>/sysman/agent_download/10.2.0.2.0/agent_download.rsp` file to reflect the load balancer host and port before using the Agent Deploy application.

C.1.5 Verify oraInventory Permissions on Remote Hosts

Ensure you (or the user performing the agent installation) have read, write, and execute permissions to `oraInventory` on all remote hosts. If you do not have these permissions on the default inventory (typically at `/etc/oraInst.loc`) on any remote host, you can specify the path to an alternative inventory location by using the `-i <location>` option in the Additional Parameters section.

Note: If this is the first installation on a remote host, Oracle Universal Installer automatically creates the `oraInventory` in the user's home directory with read, write, and execute permissions for that user, as well as the OS group to which the user belongs.

C.1.6 Verify User Credentials

Ensure the user installing the agent is the same as the user that has installed Oracle Application Server and/or Oracle Collaboration Suite. You must also ensure the user has `SUDO` privileges that are required to execute the `root.sh` script (UNIX platforms only).

You can either select **Run Root.sh** in Agent Deploy that will automatically execute the `root.sh` script (on UNIX platforms only) at the end of the installation, or choose not to select this option, but manually execute this script at the end of the installation.

This script must be run after the installation is complete in order to discover all the targets.

C.2 Prerequisite Checks Executed by Agent Deploy

The Agent Deploy application runs a local prerequisite check (on the machine running the Management Service) and remote prerequisite checks on all the remote hosts before proceeding with the installation process.

C.2.1 Prerequisite Checks Executed on the Local Host

Table C–2 lists the connectivity prerequisite checks that are run on the local (Oracle Management Service) host.

Table C–2 Connectivity Prerequisite Check

Check if	Description
Nodes are active	Verifies if the remote nodes are accessible.
SSH Server is up	Verifies if there is an SSH Server Daemon running on all remote hosts, since the installation process will require SSH.
SSH user equivalence is set	Verifies if the user name specified in the installation details page has the SSH User Equivalence on all the remote hosts.
Installation directory is writable on the remote hosts	Verifies if the installation base directory that you have specified is writable.

C.2.2 Prerequisite Checks Executed on Remote Hosts

Table C–3 lists the prerequisite checks that are executed by Agent Deploy for each installation type.

Table C–3 Prerequisite Checks for a New Installation of Management Agent

Prerequisite Check for	Description	New Installation	Shared Agent Installation	Upgrade
Certified Versions	Checks if the operating system on remote hosts is certified.	Yes	Yes	Yes
Packages	Checks if the minimum required packages are available on remote hosts	Yes	No	Yes
Disk Space	Checks if the minimum required disk space is available.	Yes	No	Yes
Agent Targets	Checks for targets on remote hosts that cannot be monitored by the agent. Targets that have been installed by another user cannot be monitored by the agent that you are going to install.	Yes	Yes	Yes
Oracle Home Location	Verifies if the specified Oracle home (`<install_base_dir/agent10g>`) is empty.	Yes	Yes	Yes
Existing Agent Installations	Checks for any existing agent installations on the remote hosts.	Yes	No	No
Write Permissions for Base Directory	Checks if the installation base directory on all remote hosts have write permissions.	Yes	No	No
Inventory Check	Checks if the user credentials that you have specified have write permissions on the central inventory of each remote host.	Yes	Yes	Yes

Table C–3 (Cont.) Prerequisite Checks for a New Installation of Management Agent

Prerequisite Check for	Description	New Installation	Shared Agent Installation	Upgrade
Upgrade Agent Existence Check	Determines the existence of an agent (10.1) that can be upgraded on the remote hosts.	No	No	Yes
Write Permissions for Upgrade Agent	Checks if the installation base directory on all remote hosts have write permissions.	No	No	Yes
NFS Agent Existence Check	Checks for any existing agent installations on the remote hosts.	No	Yes	No
Write Permissions for NFS Agent	Checks if the installation base directory, `EMSTATE` directory, and the NFS location are writable from all the remote hosts.	No	Yes	No
Time Zone ENV Check (UNIX Only)	Checks if the Timezone (TZ) environmental variable is set on the remote hosts.	Yes	Yes	Yes
Software Existence Check	Ensures the alternative software that you have specified is valid. Note: This check is executed only if you have selected a nondefault (Another Location) software location for the agent installation.	Yes		

C.3 Troubleshooting Failed Prerequisite Checks

This section details the possible errors that you may encounter when the prerequisite checks are executed, and the appropriate user actions to be taken to resolve the errors.

C.3.1 Prerequisite Check Errors and Resolutions on Local Host

Table C–4 lists the most common reasons for prerequisite check failures, and the corresponding user actions to be performed to resolve them.

Table C–4 Prerequisite Check Errors and Resolutions on Local Host

Prerequisite Check	Reason for Failure	User Action[1]
Nodes are active	Nodes are not accessible.	▪ Ensure all the nodes are active. ▪ Remove the nodes that are not accessible from the nodes list.
SSH Server is up	SSH daemon on one or more nodes is not up.	▪ Try to start the SSH daemon on the failed nodes. ▪ Remove the failed nodes from the node list.
SSH user Equivalence is set	SSH user equivalence is not set up from the local host to the failed nodes for the specified user credentials.	▪ Set up the user equivalence for the specified user credentials between the Management Service and remote hosts using the `sshUserSetup.sh` script. See Section C.1.2, "Set Up SSH (Secure Shell) User Equivalence" for more information. ▪ Remove the failed nodes from the nodes list.
Installation directory is writable on the remote hosts	Installation base directory that you have specified is not writable, or cannot be created on the failed nodes.	▪ Include write permissions on the failed nodes by executing the following command on the failed hosts from the local (OMS) host: `[ssh -l <user> <host> "chmod +w -R <dir>"]` ▪ Remove failed nodes from the nodes list.

[1] Where there are multiple user actions listed, you can choose to perform the action that is most appropriate.

C.3.2 Prerequisite Check Errors and Resolutions on Remote Hosts

Table C–5 lists the most common reasons for prerequisite check failures on remote hosts, and the corresponding user actions to be performed to resolve them.

Table C–5 Reasons for Prerequisite Check Failure and Corresponding User Actions

Prerequisite Check	Reason for Failure	User Action[1]
Certified Versions	The failed host may have an operating system or version that is not certified to deploy the agent on that machine.	▪ Exit the current installation and retry the agent installation without the failed hosts. ▪ Upgrade the failed node to an operating system or version that is certified before proceeding with the installation.
Packages	The failed hosts may not comprise the recommended minimum packages required to deploy the agent.	Click **Fix and Retry** in the Prorate Details page. Agent Deploy performs an automatic packages fix using YUM or RPMs. During the process, it returns to the Installation Details page and prompts you to specify valid or alternative values where required, and then reruns the prerequisite checks.
Disk Space	This check may fail if the required minimum disk space for the installation is not found on the remote hosts.	▪ Increase the disk space on the failed hosts. ▪ Remove the failed nodes from the nodes list.
Agent Targets	The failed nodes may have some targets that were installed by a different user, and hence cannot be monitored by the agent.	▪ Remove the targets that cannot be monitored from the failed hosts. ▪ Continue with the installation because the failure message is only a warning (though not recommended).

Table C–5 (Cont.) Reasons for Prerequisite Check Failure and Corresponding User

Prerequisite Check	Reason for Failure	User Action[1]
Port	■ The specified port is not valid, or is not available. ■ You have not specified any port and there is no available port in the default range.	■ Ensure the specified port is not blocked on the failed hosts. ■ In the Installation Details page, leave the Port value blank. ■ If the default ports are either blocked or not available, remove the failed nodes from the nodes list.
Oracle Home Location	The `<install_base_dir>/agent10g` already exists and is not empty.	■ Clean up the `<install_base_dir>/agent10g` directory. ■ Specify an alternative installation base directory. ■ Remove the failed nodes from the nodes list.
Existing Agent Installations	An agent already exists on the failed remote hosts that is registered with the central inventory.	■ Uninstall the existing agent and retry the prerequisite checks. ■ Continue with the installation because the failure message is only a warning (though not recommended).
Write Permissions for Base Directory	The installation base directory is not writable.	■ Include write permissions on the failed nodes by executing the following command on the failed hosts from the local (OMS) host: `[ssh -l <user> <host> "chmod +w -R <dir>"]` ■ Remove failed nodes from the nodes list.

Inventory Check	The specified user credential does not have write permissions on the central inventory.	Change the central inventory permission settings to render the central inventory and its subdirectories writable. Complete the following steps to resolve this issue:
		1. Log in to the local host (machine running the Oracle Management Service).
		2. Change the directory to:
		`<HOME>/sysman/prov/agentpush/resources/fixup`
		3. For each failed host, run the following script:
		`./fixOraInvPermissions.sh <install user> <install group> <failed host name> <inventory location>.`
		As this script must be run as `root` (using `sudo`) on the failed remote host, you are prompted to specify the `sudo` password.

Upgrade Agent Existence Check	A Management Agent release 10.1 is not present in the remote hosts on which you want to perform the agent upgrade.	Exit the upgrade process.
Write Permissions for Upgrade Agent	The installation base directory is not writable.	■ Include write permissions on the failed nodes by executing the following command on the failed hosts from the local (OMS) host: `[ssh -l <user> <host> "chmod +w -R <dir>"]` ■ Remove failed nodes from the nodes list.

Table C–5 (Cont.) Reasons for Prerequisite Check Failure and Corresponding User

Prerequisite Check	Reason for Failure	User Action[1]
NFS Agent Existence Check	An agent already exists on the remote hosts that is registered with the central inventory.	▪ Uninstall the existing agent and retry the prerequisite checks. ▪ Continue with the installation since the failure message is only a warning (though not recommended).
Write Permissions 'for NFS Agent	▪ The installation base directory is not writable. ▪ The NFS location is not accessible. ▪ The `EMSTATE` directory is not writable.	▪ Include write permissions on the failed nodes by executing the following command on the failed hosts from the local (OMS) host: `[ssh -l <user> <host> "chmod +w -R <dir>"]` ▪ Remove failed nodes from the nodes list.
Time Zone ENV Check	The TZ environment variable is not set on the remote hosts.	Recommended ▪ Specify the time zone in the Additional Parameters section (using the -z option) of the Installation Details page. Optional ▪ Set the TZ environment variable. Shut down and restart SSH on all remote hosts. ▪ Update with the TZ environment variable on all remote hosts.
Software Existence Check	The alternative software location that you have specified is not valid.	▪ Revert to the default software source location. ▪ Change the alternative software location to a valid location (having `./stage/product.xml`).

[1] Where there are multiple user actions listed, you can choose to perform the action that is most appropriate.

C.4 Commands and Arguments Executed to Run Agent Deploy Plugins

The Agent Deploy application makes use of plugins to perform certain functions (for example, collect installation logs from targets). These plugins execute certain commands from the local (OMS) node (for example, `mkdir`, `scp`, and `unzip`), while others are executed from the remote nodes (for example, `zip`).

Table C–6 provides a list of commands that are executed on local and remote nodes.

Table C–6 Commands Executed on Local (OMS) and Remote Nodes

Commands Executed on Local Node (OMS)	Commands Executed on Remote Nodes
PING_PATH	RSH_PATH
SH_PATH	SSH_PATH
SHELL_PATH	RCP_PATH
SHELL_ARGS	SCP_PATH
TAR_PATH	SSH_ARGS
TAR_EXTRACT_ARGS	SCP_ARGS
TAR_MTIME_ARGS	RCP_ARGS
MKDIR	UNZIP_PATH
	UNZIP_ARGS

C.5 Sample Properties Files

A sample of each property file in the `platforminfo.properties` file is provided as follows:

platforminfo.properties

Contains the mapping between platform ID and the files to be loaded for that platform.

```
# Copyright (c) 2005, Oracle. All rights reserved.

#unix
-1=Paths.properties,sPaths.properties,userPaths.properties
#linux x86
46=Paths.properties,sPaths.properties,userPaths.properties
#solaris sparc
453=Paths.properties,sPaths.properties,ssPaths_sol.properties,userPaths.properties
#ms_plats
-3=Paths.properties,ssPaths_msplats.properties
#windows nt
912=Paths.properties,ssPaths_msplats.properties
#HP-UIX
2=Paths.properties,sPaths.properties,ssPaths_hpuix.properties,userPaths.properties
#AIX
610=Paths.properties,sPaths.properties,ssPaths_aix.properties,userPaths.properties
```

Paths.properties

This is a generic file.

```
# Copyright (c) 2005, 2006, Oracle. All rights reserved.

SSH_ARGS=-o FallBackToRsh=no  -o PasswordAuthentication=no  -o
StrictHostKeyChecking=yes
SCP_ARGS=-p -o FallBackToRsh=no  -o PasswordAuthentication=no  -o
StrictHostKeyChecking=yes
UNZIP_ARGS=-o
ZIP_ARGS=-r
ZIP_EXCLUDE_ARGS=-x
ZIP_INCLUDE_ARGS=-i
```

sPaths.properties

This is a UNIX-specific file.

```
# Copyright (c) 2006, Oracle. All rights reserved.

TRUE=/bin/true
SSH_PATH=/usr/bin/ssh
SCP_PATH=/usr/bin/scp
RSH_PATH=/usr/bin/rsh
RCP_PATH=/usr/bin/rcp
RCP_ARGS=-p
SH_PATH=/bin/sh
SH_ARGS=-c
KSH_PATH=/usr/bin/ksh
PING_ARGS=-c 1 -w
PING_PATH=/bin/ping
ZIP_PATH=/usr/bin/zip
UNZIP_PATH=/usr/bin/unzip
TAR_PATH=/bin/tar
TAR_CREATE_ARGS=cvf
```

```
TAR_EXTRACT_ARGS=xvfm
TAR_EXCLUDE_ARGS=-X
TAR_INCLUDE_ARGS=-T
TAR_MTIME_ARGS=-m
CAT_PATH=/bin/cat
CP_PATH=/bin/cp
CP_ARGS=-p
MV_PATH=/bin/mv
MV_ARGS=-f
MKDIR_PATH=/bin/mkdir
MKDIR_ARGS=-p
RMDIR_PATH=/bin/rmdir
RMDIR_PARENTS_ARGS=-p
RMDIR_ARGS=--ignore-fail-on-non-empty
RM_PATH=/bin/rm
RM_F_ARGS=-f
RM_RF_ARGS=-rf
LN_PATH=/bin/ln
LN_ARGS=-fs
XARGS_PATH=/usr/bin/xargs
LS_PATH=/bin/ls
LS_ARGS=-A
CHMOD_PATH=/bin/chmod
CHOWN_PATH=/bin/chown
DF_PATH=/bin/df
DF_ARGS=-k
DF_COL_NAME=Available
SUDO_PATH=/usr/local/bin/sudo
SUDO_K_ARGS=-K
SUDO_S_ARGS=-S
TOUCH_PATH=/bin/touch
HOSTNAME_PATH=/bin/hostname
HOSTNAME_ARGS=-f
DATE_PATH=/bin/date
DATE_ARGS=+%s
SSH_KEYGEN_PATH=/usr/bin/ssh-keygen
SSH_KEYGEN_ARGS=-t rsa
SSH_KEYGEN_ARGS_KEYFILE=-f
SSH_KEYGEN_ARGS_PASSPHRASE=-N
SSH_HOST_KEY_LOC=/etc/ssh
PATH_EXISTS_FLAG=-e
FILE_EXISTS_FLAG=-f
DIR_EXISTS_FLAG=-d
DIR_WRITABLE_FLAG=-w
SLINK_EXISTS_FLAG=-h
SCRATCHPATH=/tmp

#{0} REMOTESHELL
#{1} NODE
#{2} LOGINSHELL
#{3} CMD

#KEY0=$REMOTESHELL $NODE $LOGINSHELL '$CMD;echo :EXITCODE:$? '
KEY0={0} {1} {2} ''{3};echo :EXITCODE:$? ''
#KEY1=$REMOTESHELL $NODE $LOGINSHELL '$CMD'
KEY1={0} {1} {2} ''{3}''
#KEY2=$LOGINSHELL '$CMD'
KEY2={2} ''{3}''
#KEY3=$REMOTESHELL $NODE $CMD
KEY3={0} {1} {3}
```

```
#KEY4=$LOGINSHELL '$CMD NODE'
KEY4={2} ''{3} {1}''


#{0} REMOTESHELLPATH
#{1} REMOTESHELLARGS
#{2} NODE
#{3} LOGINSHELLPATH
#{4} LOGINSHELLARGS
#{5} CMD

#KEY10=$REMOTESHELLPATH#$REMOTESHELLARGS#NODE#$LOGINSHELLPATH#$LOGINSHELLARGS#''$C
MD;echo :EXITCODE:$?''
KEY10={0}#{1}#{2}#{3}#{4}#''{5};echo :EXITCODE:$?''

#KEY11=$REMOTESHELLPATH#$REMOTESHELLARGS#NODE#$LOGINSHELLPATH#$LOGINSHELLARGS#''$C
MD''
KEY11={0}#{1}#{2}#{3}#{4}#''{5}''

#KEY12=$LOGINSHELLPATH#$LOGINSHELLARGS#''$CMD''
KEY12={3}#{4}#''{5}''

#KEY13=$REMOTESHELLPATH#$REMOTESHELLARGS#$NODE#$CMD
KEY13={0}#{1}#{2}#{5}

#KEY15=$REMOTESHELLPATH#$REMOTESHELLARGS#NODE#$LOGINSHELLPATH#$LOGINSHELLARGS#$CMD
KEY15={0}#{1}#{2}#{3}#{4}#{5}

#{0} ENV
#{1} PATH
#{2} ARGS
#{3} LOGINSHELL
#{4} FLAGS

#CMD0=$PATH $ARGS
CMD0={1} {2}

#CMD1=$ENV $PATH $ARGS
CMD1={0} {1} {2}

#CMD2=if [[ $FLAGS $PATH ]] ; then exit 0; else exit 1; fi
CMD2=if [[ {4} {1} ]] ; then exit 0; else exit 1; fi

#CMD3=if [[ $FLAGS $PATH ]] ; then echo :EXITCODE:0; else echo :EXITCODE:1; fi
CMD3=if [[ {4} {1} ]] ; then echo :EXITCODE:0; else echo :EXITCODE:1; fi

#CMD4=$PATH $ARGS $LOGINSHELL '$ENV $PATH $ARGS'
CMD4={0} {1} {2} ''{3} {4} {5}''

#CMD5=$PATH $ARGS $LOGINSHELL '$ENV $PATH $ARGS'
CMD5={0} {1} {2} ''{3} {4} {5};echo :EXITCODE:$?''

#CMD2=$CMD1 && $CMD1
#CMD2={0} {1} {2}
#CMD3=$CMD1 $LOGINSHELL $CMD1
#CMD6=( $CMD1 && $CMD1 )
#CMD7= $CMD1 | $CMD1
```

ssPaths_sol.properties (Solaris-specific file)

```
# Copyright (c) 2005, Oracle. All rights reserved.
```

```
SH_PATH=/bin/bash
SH_ARGS=-c
KSH_PATH=/usr/bin/ksh
RMDIR_ARGS=
#the date should be in the format of year:month:date:hour:minute:second
DATE_ARGS=-u +%y:%m:%d:%H:%M:%S
PING_PATH=/usr/sbin/ping
PING_ARGS=
SSH_PATH=/usr/local/bin/ssh
SSH_KEYGEN_PATH=/usr/local/bin/ssh-keygen
SCP_PATH=/usr/local/bin/scp
TAR_EXCLUDE_ARGS=X
TAR_INCLUDE_ARGS=-I
DF_COL_NAME=avail
SSH_HOST_KEY_LOC=/usr/local/etc
```

ssPaths_msplats.properties (Microsoft Windows-specific file)

```
# Copyright (c) 2005, 2006, Oracle. All rights reserved.

FALSE=C:/cygwin/bin/false.exe
#SSH_PATH=C:\\Program Files\\OpenSSH\\bin\\ssh.exe
#SCP_PATH=C:\\Program Files\\OpenSSH\\bin\\scp.exe
SSH_PATH=C:/cygwin/bin/ssh.exe
SCP_PATH=C:/cygwin/bin/scp.exe
PING_ARGS=-n 5 -w
PING_PATH=C:\\WINDOWS\\system32\\ping.exe
LS_PATH=C:/cygwin/bin/ls.exe
LS_ARGS=-A
MKDIR_PATH=C:/cygwin/bin/mkdir.exe
MKDIR_ARGS=-p
ZIP_PATH=C:/cygwin/bin/zip.exe
UNZIP_PATH=C:/cygwin/bin/unzip.exe
DATE_PATH=cmd.exe /c date
DATE_ARGS=/T
TIME_PATH=cmd.exe /c time
TIME_ARGS=/T
TOUCH_PATH=C:/cygwin/bin/touch.exe
HOSTNAME_PATH=C:/WINDOWS/system32/hostname.exe
MV_PATH=cmd.exe /c move
MV_ARGS=/Y
#MV_PATH=C:/cygwin/bin/mv.exe
#MV_ARGS=
SH_PATH=
SH_ARGS=
RMDIR_PATH=cmd.exe /c rmdir
#RM_PATH=C:/cygwin/bin/rm.exe
#RM_F_ARGS=-f
#RM_RF_ARGS=-rf
RM_PATH=cmd.exe /c del
RM_F_ARGS=/F /Q
RM_RF_ARGS=/S /Q
RM_ERR1=Could not find
CHMOD_PATH=C:/cygwin/bin/chmod.exe
CHOWN_PATH=C:/cygwin/bin/chown.exe
CP_PATH=cmd.exe /c copy
CP_ARGS=/Y
PATH_EXISTS_FLAG=-e
FILE_EXISTS_FLAG=-f
DIR_EXISTS_FLAG=-d
```

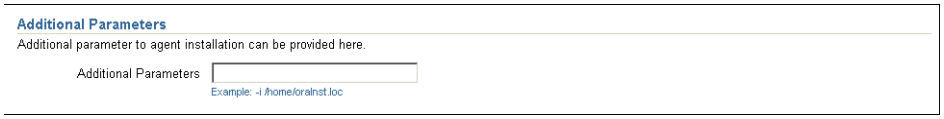
```
DIR_WRITABLE_FLAG=-w
SCRATCHPATH=C:/tmp
MORE_PATH=cmd.exe /c more
SHELL_PATH=C:/cygwin/bin/sh.exe
SHELL_ARGS=-c
CMD_PATH=C:/WINDOWS/system32/cmd.exe
CMD_ARGS=/c
SSH_HOST_KEY_LOC=C:/Program Files/OpenSSH/etc

#{0} REMOTESHELLPATH
#{1} REMOTESHELLARGS
#{2} NODE
#{3} LOGINSHELLPATH
#{4} LOGINSHELLARGS
#{5} CMD

#KEY1=$REMOTESHELLPATH#$REMOTESHELLARGS#NODE#$CMD
#KEY1={0}#{1}#{2}#\"{5}\"
KEY11={0}#{1}#{2}#{5}

#{0} ENV
#{1} PATH
#{2} ARGS
#{3} LOGINSHELL
#{4} FLAGS

#CMD2=if [ $FLAGS $PATH ] ; then exit 0; else exit 1; fi
CMD2=if [ {4} {1} ] ; then exit 0; else exit 1; fi
```

D

Additional Parameters for Agent Deploy

The additional parameters that you specify during the agent installation using the Agent Deploy application depend on the software source location that you have selected.

Figure D–1 Additional Parameters Section of the Installation Details Page



If you select the default source software location, you must specify additional parameters that are supported by the `agent Down Load` script. See Table D–1 for a list of parameters supported by this script.

If you select an alternative location, you must specify additional parameters that are supported by Oracle Universal Installer (OUI). See Table D–2 for a list of parameters supported by OUI.

Note: If the same parameters that you specify here are also specified independently (from the command-line option), the value of the parameters that you specify here take precedence over the other.

For example, if the installation base directory is specified independently, and `-b` option is specified here, the latter value (`-b`) is used in the installation.

D.1 Additional Parameters Supported by agentDownload Script

Table D–1 lists the possible parameters that you can specify if you select the default (Management Service) location.

Table D–1 Parameters Supported by agentDownload Script

Parameters	Description
-t	No value required. Do not start the agent after installation or upgrade.
-c	Cluster node list. Used during installation only. Nodes should be specified in double-quotation marks, separated by commas. For example, `-c "node1,node2,node3"`
-b	Installation base directory location. For example, -b `/home/OracleHomes/agent/`

Table D–1 (Cont.) Parameters Supported by agentDownload Script

Parameters	Description
-d	No value required. Do not initiate automatic target discovery.
-i	Inventory pointer location file. For example, `-i/etc/oraInst.loc`
-n	Cluster name. For example, `-n CLUSTER1`

-p	File location for static port for agent. For example, `-p /home/config/staticports.ini`
	The template file for the `-p` option follows:
	`# staticports.ini Template File`
	
	`# This file is a template for specifying port numbers at installation time.`
	`# To specify a port number, uncomment the appropriate line (remove #) and`
	`# replace "port_num" with the desired port number.`
	`# You can then launch Oracle Universal Installer with special options to use this file.`
	`# Please refer to Enterprise Manager Grid Control 10gR2 Installation Guide for instructions.`
	
	`# Enterprise Manager`
	
	`#Enterprise Manager Central Agent Port=port_num`

-z	Timezone environment variable value (`-z <timezone>`). For example, `-z PST8PDT`.

Note: Use the `-z` option to specify the time zone, but the Agent Deploy application discovers a `TZ` environment variable already set on the remote host, this `TZ` value will take precedence over the `-z` value that you specify.

You can verify if the `TZ` environment variable has been set on the remote host by executing the following command:

```
ssh -l <user_name> -n <remote_node> 'echo $TZ'
```

The `<user name>` argument is the ID that you are using for the agent installation, and `<remote host>` is the host on which you want to install the agent.

If you are installing the agent from a nondefault software location, you must specify the timezone environment variable using the following command:

```
s_timeZone=<timezone>
For example, s_timezone=PST8PDT
```

D.2 Additional Parameters Supported by Oracle Universal Installer

Table D–2 lists the possible parameters that you can specify if you select an alternative software source (nondefault) location:

Table D–2 Parameters Supported by Oracle Universal Installer

Parameter	Description
-clusterware oracle.crs, <crs version>	Version of the installed Oracle Clusterware.
-crslocation <path>	For cluster installs, specifies the path to the CRS home location. Specifying this overrides CRS information obtained from the central inventory.

-invPtrLoc <full path of oraInst.loc>	Linux only. To point to a different inventory location. The `orainst.loc` file contains:
	`inventory_loc=<location of central inventory>`
	`inst_group=<group of the user that is installing the agent>`

-jreLoc <location>	Path where the Java Runtime Environment is installed. OUI cannot be run without this.
-logLevel <level>	Filter log messages that have a lesser priority level than <level>. Valid options are: severe, warning, info, config, fine, finer, finest, basic, general, detailed, trace. The use of basic, general, detailed, and trace is deprecated.
-paramFile <location of file>	Location of `oraparam.ini` file to be used by Oracle Universal Installer.
-responseFile <Path>	Response file and path to use.
-sourceLoc <location of products.xml>	Software source location.
-cfs	Oracle home specified is on the cluster file system (shared). This is mandatory when '`-local`' is specified so that Oracle Universal Installer can register the home appropriately into the inventory.
-debug	Get debug information from OUI.
-executeSysPrereqs	Execute system prerequisite checks and exits.
-force	Allow silent mode installation into a non-empty directory.
-help	Display the usage of all preceding options.
-ignoreSysPrereqs	Ignore the results of the system prerequisite checks.
-local	Perform the operation on the local node irrespective of the cluster nodes specified.
-printmemory	Log debug information for memory usage.
-printtime	Log debug information for time usage.
-updateNodeList	Update the node list for this home in the OUI inventory.

D.2.1 Command-Line Variable Usage During Silent Installation

The command-line variables are specified using the `<name=value>` format.

```
For example,
[ session: | compName: | compName:version: ]variableName=" valueOfVariable"]
```

Session or installer variables are specified using the `[session:]varName=value` format.

```
For example:
session:ORACLE_HOME_NAME="OraHome"
ORACLE_HOME_NAME="OraHome"
```

> **Note:** The lookup order is `session:varName`, and then just the `varName`. The session prefix is used to avoid ambiguity.

Component variables are specified using `[compInternalName:[Version:]]varName`

```
For example:
oracle.comp1:1.0.1:varName="VarValue"
oracle.comp1:varName="VarValue"
```

> **Note:** The lookup order is `compInternalName:Version:varName`, the `compInternalName:varName`, and then just the `varName`.

See Section 4.1.4, "Silent Installation of an Additional Management Agent" for more information.

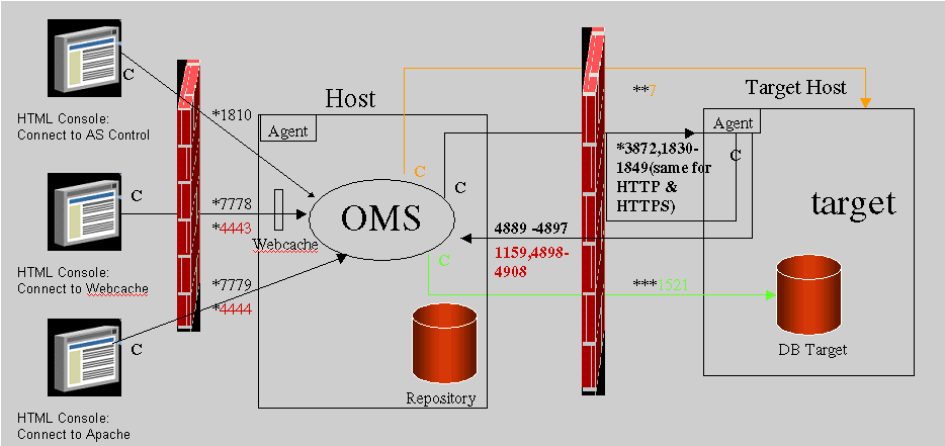
E

Enterprise Manager Firewall Port Requirements

If your Enterprise Manager grid environment is making use of firewalls, ensure you specify the appropriate ports.

Figure E–1 provides a topology of an Enterprise Manager grid environment that is using a firewall, and also illustrates the appropriate ports that you must specify.

Figure E–1 Enterprise Manager Firewall Port Requirements



The conventions used in the preceding illustration are as follows:

Table E–1 Conventions Used

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.
***	Are the Database listener ports.

Note:

- The direction of the arrows specify the direction of ports.
- Port 1159, 4898-4989 specify that 1159 is the default. If this port is not available, the management Service will search in the range that is specified.
- 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 agent will make the call.

F

Installation and Configuration Log File Locations

This appendix lists the locations of the various log files that are created during the prerequisites check, installation, and configuration phases of Enterprise Manager Grid Control components.

F.1 Enterprise Manager Grid Control Installation Log Files

During Enterprise Manager installation, the following log files are created:

1. Configuration Logs
2. Installation Logs
3. Repository Logs
4. Secure Logs

F.1.1 Configuration Logs

lists the installation logs that are created.

Table F–1 Installation Log Files

Installation Type	Log File	Location
Enterprise Manager Using New Database	cfm log	<DB_HOME>/cfgtools/cfgfw/cfmlogs
	oracle.sysman.top.em_seed.<timestamp>.log	<DB_HOME>/cfgtools/cfgfw/oracle.sysman.top.em_seed.<timestamp>.log
Enterprise Manager Using Existing Database	cfm log	<OMS_HOME>/cfgtools/cfgfw/cfmlogs
	oracle.sysman.top.oms<timestamp>.log	<OMS_HOME>/cfgtools/cfgfw/oracle.sysman.top.oms.<timestamp>.log
Additional Management Service	cfm log	<OMS_HOME>/cfgtools/cfgfw/cfmlogs
	oracle.sysman.top.oms<timestamp>.log	<OMS_HOME>/cfgtools/cfgfw/oracle.sysman.top.oms.<timestamp>.log

Table F–1 (Cont.) Installation Log Files

Installation Type	Log File	Location
Additional Management Agent	cfm log	<AGENT_HOME>/cfgtools/cfgfw/cfmlogs
	oracle.sysman.top.agent <timestamp>.log	<AGENT_HOME>/cfgtools/cfgfw/oracle.sysman.top.oms.<timestamp>.log

F.1.2 Installation Logs

The installation action logs that are created will provide complete information on the installation status. This log is located at the following locations:

- `oraInventory/logs/installActions<timestamp>.log`
- `<ORACLE_HOME>/cfgtoollogs/oui/installActions<timestamp>.log`

> **Note:** The `installActions` log file is located in the `oraInventory` directory by default. This log file will be copied on to the above-mentioned Oracle home location after the installation is complete.

F.1.3 Repository and Secure Logs

The repository and secure logs are located in the Management Service Oracle home for the following installation types:

- Enterprise Manager Using a New Database
- Enterprise Manager Using an Existing Database
- Additional Management Service

F.1.3.1 Repository Log Location

The repository log is located at:

```
<OMS_HOME>/sysman/log/emrepmgr<rep log>.<pid>
```

> **Note:** In the above-mentioned path, the `emrepmgr` will be the **SID**.

F.1.3.2 Secure Log Location

The secure log is located at:

```
<OMS_HOME>/sysman/log/<secure log>
```

If you are installing an additional Management Agent, the secure log is located at:

```
<AGENT_HOME>/sysman/log/<secure log>
```

F.2 Agent Deploy Log Files

The following agent prerequisite check and installation logs are available at these locations:

Connectivity Logs: the following connectivity logs for the local node will be available at the following locations:

Table F–2 Connectivity Log Locations

Log File	Location
prereq<time_stamp>.log	$OMS_HOME/sysman/prov/agentpush/<time-stamp>/prereqs/local
prereq<time_stamp>.out	$OMS_HOME/sysman/prov/agentpush/<time-stamp>/prereqs/local
prereq<time_stamp>.err	$OMS_HOME/sysman/prov/agentpush/<time-stamp>/prereqs/local

Prerequisite Logs: The following prerequisite logs for <node 1> will be available at the following locations:

Table F–3 Prerequisite Log Locations

Log File	Location
prereq<time_stamp>.log	$OMS_HOME/sysman/prov/agentpush/<time-stamp>/prereqs/<node1>
prereq<time_stamp>.out	$OMS_HOME/sysman/prov/agentpush/<time-stamp>/prereqs/<node1>
prereq<time_stamp>.err	$OMS_HOME/sysman/prov/agentpush/<time-stamp>/prereqs/<node1>

Note: The time stamp in the log files of prereq/install/upgrade function may not be the same as the time-stamp in the $OMS_HOME/sysman/prov/agentpush/<time-stamp>/. These time stamps can differ considerably from the OMS host because these logs are generated in remote nodes and are collected back to OMS after the agent installation or upgrade.

Table F–4 lists all the other installation logs that are created during an agent installation using Agent Deploy.

Table F–4 Installation Logs Created During Agent Installation Using Agent Deploy

Logs	Location	Description
EMAgentPush<TIMESTAMP>.log	<OMS_HOME>/sysman/prov/agentpush/logs/	Agent Deploy application logs.

Table F–4 (Cont.) Installation Logs Created During Agent Installation Using Agent

Logs	Location	Description
remoteInterfaces<TIMESTAMP>.log	<OMS_HOME>/sysman/prov/agentpush/logs/	Logs of the remote interfaces layer.
install.log/.err	<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/	Log or error of the new agent installation or new cluster agent installation.
upgrade.log/.err	<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/	Log or error of the upgrade operation using Agent Deploy
nfsinstall.log/err	<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/	Log or error of the agent installation using the Shared Agent Home option in Agent Deploy.
clusterUpgrade.log/err	<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/	Log or error of the cluster upgrade operation using Agent Deploy.
sharedClusterUpgradeConfig.log/err	<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/	Log or error of the config operation in case of upgrade on a shared cluster.
config.log/err	<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/	Log or error of the configuration of shared cluster in case of an agent installation on a shared cluster.
preinstallscript.log/.err	<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/	Log/error of the running of preinstallation script, if specified.
rootsh.log/.err	<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/	Log/error of running of `root.sh`.
postinstallscript.log/.err	<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/	Log or error of running of postinstallation script, if specified.
installActions<timestamp>.log, oraInstall<timestamp>.err/.out	<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/	Logs of Oracle Universal Installer.
agentStatus.log	<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/	Status of agent after running `emctl status agent` from the agent home.

G

Oracle Reserved Words

This appendix provides a complete list of Oracle reserved words.

G.1 List of Oracle Reserved Words

In addition to the reserved words in Table G–1, Oracle also uses system-generated names beginning with *SYS_* for implicitly generated schema objects and subobjects. Oracle discourages you from using this prefix in the names you explicitly provide to your schema objects and subobjects to avoid possible conflicts in name resolution.

Table G–1 List of Oracle Reserved Words

Oracle Reserved Words and Keywords		
ACCESS	ACCOUNT	ACTIVATE
ADD	ADMIN	ADVISE
AFTER	ALL	ALL_ROWS
ALLOCATE	ALTER	ANALYZE
AND	ANY	ARCHIVE
ARCHIVELOG	ARRAY	AS
ASC	AT	AUDIT
AUTHENTICATED	AUTHORIZATION	AUTOEXTEND
AUTOMATIC	BACKUP	BECOME
BEFORE	BEGIN	BETWEEN
BFILE	BITMAP	BLOB
BLOCK	BODY	BY
CACHE	CACHE_INSTANCES	CANCEL
CASCADE	CAST	CFILE
CHAINED	CHANGE	CHAR
CHAR_CS	CHARACTER	CHECK
CHECKPOINT	CHOOSE	CHUNK
CLEAR	CLOB	CLONE
CLOSE	CLOSE_CACHED_OPEN_CURSORS	CLUSTER
COALESCE	COLUMN	COLUMNS

Table G–1 (Cont.) List of Oracle Reserved Words

Oracle Reserved Words and Keywords		
COMMENT	COMMIT	COMMITTED
COMPATIBILITY	COMPILE	COMPLETE
COMPOSITE_LIMIT	COMPRESS	COMPUTE
CONNECT	CONNECT_TIME	CONSTRAINT
CONSTRAINTS	CONTENTS	CONTINUE
CONTROLFILE	CONVERT	COST
CPU_PER_CALL	CPU_PER_SESSION	CREATE
CURRENT	CURRENT_SCHEMA	CURREN_USER
CURSOR	CYCLE	
DANGLING	DATABASE	DATAFILE
DATAFILES	DATAOBJNO	DATE
DBA	DBHIGH	DBLOW
DBMAC	DEALLOCATE	DEBUG
DEC	DECIMAL	DECLARE
DEFAULT	DEFERRABLE	DEFERRED
DEGREE	DELETE	DEREF
DESC	DIRECTORY	DISABLE
DISCONNECT	DISMOUNT	DISTINCT
DISTRIBUTED	DML	DOUBLE
DROP	DUMP	EACH
ELSE	ENABLE	END
ENFORCE	ENTRY	ESCAPE
EXCEPT	EXCEPTIONS	EXCHANGE
EXCLUDING	EXCLUSIVE	EXECUTE
EXISTS	EXPIRE	EXPLAIN
EXTENT	EXTENTS	EXTERNALLY
FAILED_LOGIN_ ATTEMPTS	FALSE	FAST
FILE	FIRST_ROWS	FLAGGER
FLOAT	FLOB	FLUSH
FOR	FORCE	FOREIGN
FREELIST	FREELISTS	FROM
FULL	FUNCTION	GLOBAL
GLOBALLY	GLOBAL_NAME	GRANT
GROUP	GROUPS	HASH
HASHKEYS	HAVING	HEADER
HEAP	IDENTIFIED	IDGENERATORS

Table G–1 (Cont.) List of Oracle Reserved Words

Oracle Reserved Words and Keywords		
IDLE_TIME	IF	IMMEDIATE
IN	INCLUDING	INCREMENT
INDEX	INDEXED	INDEXES
INDICATOR	IND_PARTITION	INITIAL
INITIALLY	INITRANS	INSERT
INSTANCE	INSTANCES	INSTEAD
INT	INTEGER	INTERMEDIATE
INTERSECT	INTO	IS
ISOLATION	ISOLATION_LEVEL	KEEP
KEY	KILL	LABEL
LAYER	LESS	LEVEL
LIBRARY	LIKE	LIMIT
LINK	LIST	LOB
LOCAL	LOCK	LOCKED
LOG	LOGFILE	LOGGING
LOGICAL_READS_PER_CALL	LOGICAL_READS_PER_SESSION	LONG
MANAGE	MASTER	MAX
MAXARCHLOGS	MAXDATAFILES	MAXEXTENTS
MAXINSTANCES	MAXLOGFILES	MAXLOGHISTORY
MAXLOGMEMBERS	MAXSIZE	MAXTRANS
MAXVALUE	MIN	MEMBER
MINIMUM	MINEXTENTS	MINUS
MINVALUE	MLSLABEL	MLS_LABEL_FORMAT
MODE	MODIFY	MOUNT
MOVE	MTS_DISPATCHERS	MULTISET
NATIONAL	NCHAR	NCHAR_CS
NCLOB	NEEDED	NESTED
NETWORK	NEW	NEXT
NOARCHIVELOG	NOAUDIT	NOCACHE
NOCOMPRESS	NOCYCLE	NOFORCE
NOLOGGING	NOMAXVALUE	NOMINVALUE
NONE	NOORDER	NOOVERRIDE
NOPARALLEL	NOPARALLEL	NOREVERSE
NORMAL	NOSORT	NOT
NOTHING	NOWAIT	NULL
NUMBER	NUMERIC	NVARCHAR2

Table G–1 (Cont.) List of Oracle Reserved Words

Oracle Reserved Words and Keywords		
OBJECT	OBJNO	OBJNO_REUSE
OF	OFF	OFFLINE
OID	OIDINDEX	OLD
ON	ONLINE	ONLY
OPCODE	OPEN	OPTIMAL
OPTIMIZER_GOAL	OPTION	OR
ORDER	ORGANIZATION	OSLABEL
OVERFLOW	OWN	PACKAGE
PARALLEL	PARTITION	PASSWORD
PASSWORD_GRACE_TIME	PASSWORD_LIFE_TIME	PASSWORD_LOCK_TIME
PASSWORD_REUSE_MAX	PASSWORD_REUSE_TIME	PASSWORD_VERIFY_ FUNCTION
PCTFREE	PCTINCREASE	PCTTHRESHOLD
PCTUSED	PCTVERSION	PERCENT
PERMANENT	PLAN	PLSQL_DEBUG
POST_TRANSACTION	PRECISION	PRESERVE
PRIMARY	PRIOR	PRIVATE
PRIVATE_SGA	PRIVILEGE	PRIVILEGES
PROCEDURE	PROFILE	PUBLIC
PURGE	QUEUE	QUOTA
RANGE	RAW	RBA
READ	READUP	REAL
REBUILD	RECOVER	RECOVERABLE
RECOVERY	REF	REFERENCES
REFERENCING	REFRESH	RENAME
REPLACE	RESET	RESETLOGS
RESIZE	RESOURCE	RESTRICTED
RETURN	RETURNING	REUSE
REVERSE	REVOKE	ROLE
ROLES	ROLLBACK	ROW
ROWID	ROWNUM	ROWS
RULE	SAMPLE	SAVEPOINT
SB4	SCAN_INSTANCES	SCHEMA
SCN	SCOPE	SD_ALL
SD_INHIBIT	SD_SHOW	SEGMENT
SEG_BLOCK	SEG_FILE	SELECT
SEQUENCE	SERIALIZABLE	SESSION

Table G–1 (Cont.) List of Oracle Reserved Words

Oracle Reserved Words and Keywords		
SESSION_CACHED_ CURSORS	SESSIONS_PER_USER	SET
SHARE	SHARED	SHARED_POOL
SHRINK	SIZE	SKIP
SKIP_UNUSABLE_ INDEXES	SMALLINT	SNAPSHOT
SOME	SORT	SPECIFICATION
SPLIT	SQL_TRACE	STANDBY
START	STATEMENT_ID	STATISTICS
STOP	STORAGE	STORE
STRUCTURE	SUCCESSFUL	SWITCH
SYS_OP_ENFORCE_NOT_ NULL$	SYS_OP_NTCIMG$	SYNONYM
SYSDATE	SYSDBA	SYSOPER
SYSTEM	TABLE	TABLES
TABLESPACE	TABLESPACE_NO	TABNO
TEMPORARY	THAN	THE
THEN	THREAD	TIMESTAMP
TIME	TO	TOPLEVEL
TRACE	TRACING	TRANSACTION
TRANSITIONAL	TRIGGER	TRIGGERS
TRUE	TRUNCATE	TX
TYPE	UB2	UBA
UID	UNARCHIVED	UNDO
UNION	UNIQUE	UNLIMITED
UNLOCK	UNRECOVERABLE	UNTIL
UNUSABLE	UNUSED	UPDATABLE
UPDATE	USAGE	USE
USER	USING	VALIDATE
VALIDATION	VALUE	VALUES
VARCHAR	VARCHAR2	VARYING
VIEW	WHEN	WHENEVER
WHERE	WITH	WITHOUT
WORK	WRITE	WRITEDOWN
WRITEUP	XID	YEAR
ZONE		

Index

A

accessing
  Grid Control, 10-6
  installer, 3-1
  management packs, 7-3
  Oracle Metalink, 7-2
account, default for Super Administrator, 10-1
Agent Deploy Application, 6-1
Agent Registration password, 3-41
agentDownload script, 6-19
  actions performed, 6-23
  benefits of, 6-19
  customizing, 6-25
  options for, 6-24
  using, 6-20
agentDownload script, pull technology, 6-19
application server
  automatic discovery, 10-2
  password access to, 2-3
assigning custom ports, 4-5
automatic discovery, 10-2
Automatic Storage Management (ASM), monitoring, 7-5

B

base directory, 1-3, 2-2
  new database installation, 3-8
  upgrading Enterprise Manager, 11-10
benefits of agentDownload script, 6-19
Binary Large Objects (BLOBs), recommendations for, 3-27
browser certifications, 1-6, 1-7
browsers for Grid Control, 1-7

C

certifications
  operating system, 1-6
  operating system versions, 1-6
certified
  Enterprise Manager targets, 1-8
  targets for management or monitoring, 1-8
  targets, requirements of, 1-6
completing installation process, running root.sh, 7-1
component definitions, 1-2
Configuration Data Tablespace, 3-27
configuration tasks, post-installation, 1-1
configurations
  Enterprise Manager Configuration Plugin (EMCP), 2-4
  optional, 7-3
  proxy, 7-3
Configure Email Notification section, for new database installation, 3-13
connecting with Management Repository, 3-34
CPU and memory
  allocation requirements, 1-4
  recommended allocation, 1-4
cron job, in agentDownload script, 6-19
custom port numbers, 4-5
customizing agentDownload script, 6-25

D

Database Connection Details section, repository database configuration, 3-26
databases, and automatic discovery, 10-2
DBSNMP account
  password, 7-4
  Repository Database passwords passwords, 3-16
  unlocking, 10-7
deinstallation of Oracle homes, 3-45
deploying
  Management Agent, 6-1
  Management Agent, planning for, 1-1
deployment options for Management Agent, 6-1
directory, creating base directory, 1-3

E

e-mail notifications, for SYSMAN account, 10-2
EMCP, 2-4
Enterprise Manager
  certified targets, 1-8
  components overview, 1-2
  Configuration Plugin (EMCP), 2-4
  hardware requirements, 1-4
  installation options, 3-5
  platform and target certification requirements, 1-6

ready-to-use configuration, 10-1
recommended setup tasks for new users, 10-3
Repository Configuration Assistant, 3-31
software requirements, 1-9
topology, 1-3
Execute Configuration Scripts dialog, 3-18, 3-30, 3-37, 3-42

F

failed prerequisite checks, action required for, 3-11
firewall, accessing sites outside, 7-4
footprint, definition of, 3-5

G

Grid Control
accessing, 10-6
console, definition of, 1-2
using console for first time, 10-3
Group Specification section of Universal Installer, 3-13

H

hard disk space, 3-5
hard disk space recommended for tablespace, 1-5
hardware
pre-installation requirements, 1-4
requirements for Real Application Clusters, 11-22
host name, Database Connection Details section, 3-26

I

-ignoresysPrereqs flag, 6-24
Info-ZIP zip utility, 2-1
installation
options, 3-5
planning for, 1-1
prerequisite checks for installation types, 1-10
scripted using agentDownload, 6-19
silent, 6-2
typical scenario, 3-24
using Oracle Universal Installer, 6-2
installing
additional languages, 2-3
additional Management Agent using OUI, 3-38
Enterprise Manager, 1-1, 3-1
Enterprise Manager using existing database, 3-21
Enterprise Manager, using new database, 3-7
Management Agent, 3-37
interactive installation using Universal Installer, 6-2
inventory directory, 2-2

L

Language Selection page
additional Management Agent installation, 3-39
additional Management Service installation, 3-33
existing database installation, 3-25
new database installation, 3-9
languages, installing additional, 2-3
licensing information, and pre-installation considerations, 1-3
logging in as root, 2-3

M

Management Agent
definition of, 1-2
deploying, 6-1
deployment options, 6-1
proxy configuration, 4-5
starting and stopping, 10-5
upgrading, 11-8
management packs, accessing, 7-3
Management Repository
definition of, 1-2
software requirements, 1-9
Management Repository Database, starting, 10-4
Management Service
Agent Registration password, 3-41
definition of, 1-2
proxy configuration, 7-4
software requirements, 1-9
SSL-enabled, 3-41
starting and stopping, 10-4
upgrading, 11-7
upgrading existing database, 11-6
upgrading new database, 11-6
Management tablespace location, 3-27
memory and CPU
allocation requirements, 1-4
recommended allocation, 1-4
memory requirements, 3-5
MetaLink
accessing, 7-2
accessing Web site, 7-2
specifying credentials, 7-3
metric collection error, and Database Home page, 7-4
monitoring credentials, setting, 10-7
multiple Oracle home support, 1-4
pre-installation considerations, 1-3
multiple-Oracle home installations and configurations, 0-xvii

N

nfsagentinstall script, 6-1
Notification Methods option for e-mail, 3-28
notification rules for e-mail, 10-2

O

OMS
software requirements, 1-9
starting and stopping, 10-4
upgrading, 11-7
upgrading existing database, 11-6
upgrading new database, 11-6

operating system certifications, 1-6
optional configurations, 7-3
Oracle
  base directory, 1-3
  directory, 1-3
  directory and Oracle homes, 2-2
  directory, pre-installation requirements, 1-3
  homes, deinstallation of, 3-45
  MetaLink credentials, specifying, 7-3
  multiple home support, 1-4
  software requirements, 1-9
  System Identifier (SID), 3-26
  Universal Installer, starting, 2-4
  Universal Installer, using, 3-3
Oracle Management Agent
  see Management Agent
Oracle Management Repository
  see Management Repository
Oracle Management Service
  see Management Service
OracleMetaLink
  see MetaLink
oraInventory directory, 2-2
OSDBA group, 3-13
OSOPER group, 3-13

P

parent directory
  new database installation, 3-8
  upgrading Enterprise Manager, 11-10
passwords
  application server, 2-3
  restrictions and recommendations, 3-16
  securing Grid Control, 3-15
permissions and prerequisites, new database installation, 3-7
planning an installation, 1-1
port field, for proxy information, 3-14
port number, Database Connection Details section, 3-26
ports, assigning custom, 4-5
post-installation configuration tasks, 1-1
pre-installation
  considerations, 1-1
  considerations for Enterprise Manager, 1-3
  licensing information, 1-3
  Oracle directory, 1-3
  requirements for Enterprise Manager, 1-4
prerequisite
  check status, 3-11
  checks, 1-10
Prerequisite Checker, running in standalone mode, 1-11
prerequisites
  installing using existing database, 3-21
  product, 3-10
  software, 11-1
product prerequisites, 3-10
proxy configuration, 7-3
  for Management Agent, 4-5
  for Management Service, 7-4
proxy information, using for external access, 3-14
proxy settings for Web site access, 7-4
pulling Agent bits, 6-19

R

rdist, agentDownload script
  pull technology, agentDownload script, 6-19
ready-to-use configuration, 10-1
Real Application Clusters, installation requirements, 11-22
realm field, for proxy information, 3-14
recommended CPU and memory allocation, 1-4
Repository Configuration Assistant, 3-31
Repository Database passwords, 3-16
requirements
  CPU and memory allocation, 1-4
  for general system installation, 11-22
  hardware, 1-4
resource allocation considerations, 1-6
root, logging in as, 2-3
root.sh script as part of agentDownload script, 6-23
rules for e-mail notifications, 10-2
runInstaller script, 3-4, 3-6
running Prerequisite Checker, 1-11
running root.sh, 7-1

S

script actions, agentDownload, 6-23
script options, descriptions for agentDownload, 6-24
scripted installation, 6-19
securing
  Grid Control, passwords for, 3-15
  OMS, 3-15
SID, 3-26
silent installation
  definition, 6-2
  performing, 4-1
skipped prerequisite checks, action required for, 3-11
software
  extracting from zip files, 2-1
  getting from Oracle Technology Network, 2-1
  prerequisites, 11-1
  requirements for Enterprise Manager, 1-9
  requirements for Real Application Clusters, 11-23
Specify Repository Database Configuration page, 3-34
SSL-enabled Management Service, 3-41
starting
  Management Repository Database, 10-4
  Oracle Universal Installer, 2-4
starting and stopping Management Service, 10-4
Static Ports feature, 4-5
Super Administrator default account, 10-1
SYS account, Repository Database passwords, 3-16
SYSMAN account, 3-16, 10-2

default for Super Administrator, 10-1
SYSTEM account, Repository Database
passwords, 3-16

T

target discovery, troubleshooting issues for, 10-3
targets certified, 1-8
topology of Enterprise Manager, 1-3
troubleshooting issues for target discovery, 10-3

U

unlocking DBSNMP user account, 10-7
upgrading
Management Agent, 11-8
Oracle Management Service, 11-7
using
agentDownload script, 3-37, 6-20
existing database, 3-24
Oracle Universal Installer, 3-1, 3-3
OUI, 3-1, 3-37
response files, 4-1

V

versions of browser for console, 1-7

W

warning prerequisite checks, action required
for, 3-11

Z

zip files, extracting software from, 2-1