10*g* R2 Management Agent Deployment Best Practices

An Oracle White Paper
June 2006

10*g* R2 Management Agent Deployment Best Practices

1.0 – INTRODUCTION

Note: this document describes Agent deployment practices in Enterprise Manager 10.2.0.2.0 and 10.2.0.1.0.

The architecture of Oracle Enterprise Manager 10*g* R2 (EM) is comprised of a central Oracle Management Service (OMS) storing data in a central repository, and communicating with Management Agents on all managed hosts. Those Management Agents discover, monitor and administer all targets on their hosts, including databases, application servers, other software, and aspects of the hosts themselves. Deploying the Management Agents onto hosts in a scalable fashion can be a challenge – without facilities for automating installation, the effort required to perform mass numbers of manual installs would likely preclude administrators from using EM to its full potential.

Enterprise Manager 10*g* R2 provides a variety of methods to install Management Agents on hosts to be managed by EM. Multiple options are provided to allow system administrators to choose methods that best suit an enterprise's configuration. Several new capabilities have been added since 10*g* R1, including the Agent Deploy application, NFS-mounted installations, and improvements to the downloadable Agent mechanism. This document will highlight the best practices for using these methods to deploy Management Agents across large-scale environments.

For information on installing Agents via the agentDownload script, please see section 3, beginning on page 5. For information on the Agent Deploy application, please see section 5, beginning on page 12. (Please note that interim patches may be required for successful use of the Agent Deploy application in version 10.2.0.1.0.) These are the best-practice recommendations for most environments; the other sections describe alternate options.

MORE INFORMATION

The "Grid Control Basic Installation and Configuration Guide" can compliment the information in this paper. The latest copy of this guide can be found at following location:

HTML: http://download.oracle.com/docs/cd/B16240_01/doc/install.102/b16228/toc.htm

PDF: http://download.oracle.com/docs/cd/B16240_01/doc/install.102/b16228.pdf

2.0 – CONCEPTS

What is an EM state directory?

The EM state directory is a directory used for storing the configuration files (for instance, emd.properties and targets.xml), log files, etc. that are unique to each host. State directories are used in clustered Agents as well as NFS mounted Agents (though technically, regular standalone Agents have them as well, integrated into their ORACLE_HOME.) Each host that shares an Agent will have its own state directory. To know the location of the EM state directory you can issue the following command:

```
$ emctl getemhome
```

How much space is required for EM state directories?

The EM state directory initially requires 1 Megabyte of space. However, all upload files, collection files and log files are kept in this directory, so adequate space should be allocated to allow them to grow.

Which deployment method is most suitable for the majority of environments?

For most situations, the Agent Deploy application is recommended; please see section 5, beginning on page 11, for details.

3.0 – DOWNLOADABLE AGENT INSTALLATION

Every successfully installed OMS instance includes a directory that contains (along with a README file and various library files) a response file for non-interactive installation, platform-specific download scripts and installation code. The directory is located on the filesystem at

<OMS_ORACLE_HOME>/sysman/agent_download/

and configured through the application server to be accessible at

http://<OMS_host>:<OMS_port>/agent_download/

This directory contains a subdirectory named after the version of the Agent install software, and further subdirectories for the platform with which the Agent install is compatible. The download scripts themselves, named **agentDownload.<platform>**, are what are executed to run the installations. Thus, to obtain the installation script for the 10.2.0.1.0 or 10.2.0.2 Agent for Linux, one would access the script at the URL

http://<OMS_host>:<OMS_port>/agent_download/<10.2.0.2.0 or 10.2.0.1.0>/linux/agentDownload.linux

For windows the URL would be

http://<OMS_host>:<OMS_port>/agent_download/10.2.0.2.0/<win32>/agentDownload.vbs

Note: The URL for windows only has 10.2.0.2 as this is the first full release of Enterprise Manager 10gR2 on windows platform.

When executed, the script uses the "wget" utility to access the Oracle Universal Installer and the installation response file, and download them from the OMS host to the Agent install host. Then, the installer is executed in silent (non-interactive) mode, using the values specified in the response file. To access the actual install binaries (which remain located on the OMS host), the Agent install host specifies their location via HTTP. Note that the wget utility is a requirement, so for environments lacking the utility, this deployment method may not be ideal. To initiate installation, follow these steps:

Open a browser window on the new host

Download the installation script

One 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

Change the file permissions on the script to allow file execution.

Run the script with the –b option (specifying the base installation directory) For example, the command to be executed might be:

For Linux:

./agentDownload.linux –b /scratch/oracle_products

For Windows:

CScript.exe agentDownload.vbs b <**C:\scratch\oracle_products** > m <OMS_HOST> r <HTTPport>

Note 1: Before executing the `agentDownload.vbs` script, ensure *Windows Script Host version 5.6* is installed on the target host. This is required for the script to be executed successfully.

Note 2: Make sure wget location is included in the $PATH variable.

This will install an agent with an ORACLE_HOME of **/scratch/oracle_products/agent10g (on linux) and C:\scratch\oracle_products\agent10g (on windows)**

Because the installation process is scripted, it can be executed via a wrapper script or cron job to aid mass deployment.

After installation, the root.sh script must be run manually (i.e., it is not run as part of the installation script) for UNIX like platforms. Additionally, Management Agents installed through this process are not secure by default – in order to have the newly installed Agent communicate with the OMS via HTTPS, one of two additional steps must be taken. Either the user must specify the value of the AGENT_INSTALL_PASSWORD environment variable before installation begins, or must run the command

<Agent_ORACLE_HOME>/bin/emctl secure agent <password>

after installation completes. Note that using one of these two methods to secure the Agent will be required for successful operation if the OMS is configured to require secure communications.

For Enterprise Manager release 10.2.0.2 all the communications between the agents and the OMS are secured. So if the variable AGENT_INSTALL_PASSWORD is not set then the user would be prompted for it.

3.0.1 – Additional Parameters supported by agentDownload script

Additional Parameters Supported by agentDownload Script, please see **Appendix G**

3.0.2 – Downloadable Agent Readme

The Readme document for the Downloadable Agent deployment method can be found on the Oracle Technology Network (OTN) website, labeled as an Important Note in the 10.2.0.1 section of the Mass Agent Deployment page:

http://www.oracle.com/technology/software/products/oem/htdocs/agentsoft.html

3.1 – Staging the Downloadable Agent for Various Platforms and Versions

By default, installation files for the downloadable Agent are only staged in the OMS ORACLE_HOME for Management Agents to be set up on hosts of the same platform as that of the OMS host. Thus if the OMS is installed on a Linux-based host, only the agentDownload.linux script and accompanying installation binaries will be present.

In order to use this functionality to deploy Management Agents onto platforms different from that of the OMS host, the downloadable Agent package for each alternate platform will need to be downloaded from the Oracle Technology Network (OTN) website. Those packages can be found at **http://www.oracle.com/technology/software/products/oem/htdocs/agentsoft.html**. Once downloaded, the packages should be unpacked into the sysman/agent_download subdirectory of the OMS ORACLE_HOME, whereupon it will be available for use.

Unpacking those into the /sysman/agent_download directory will also work, as the <version> subdirectory will keep different Agent version installers distinct.

Note 1: Agent can be installed interactively also using the agent download kit. On linux platforms for example, interactive install can be done using the download kit by invoking the <Unzip directory where the Download kit is unzipped>/linux/agent/runInstaller. This is start the interactive install using Oracle Universal Installer.

Note 2: While the wget utility is typically present on most Linux/UNIX systems, Windows hosts do not usually support wget by default. In order to successfully deploy an Agent onto Windows, the target Windows hosts will have to have the wget utility installed. A Windows version of the utility can be found at:

http://gnuwin32.sourceforge.net/packages/wget.htm

3.2 – Using the Downloadable Agent With a Server Load Balancer

The response file used by the downloaded installer will ordinarily not need to be changed; the correct values for allowing the new Agent to communicate with the OMS are pre-populated at the time of OMS installation. However, deploying Agents to communicate with a Server Load Balancer (SLB) in multi-OMS environments (instead of communicating with a single specific OMS) will require a change. The response file found in an OMS ORACLE_HOME will contain the Agent communication URL of that OMS, and so any Agent installed using the default response file will be configured to communicate just with the OMS. To configure Agents to communicate with the SLB, the values in the response file for the properties s_OMSHost and s_OMSPort must be changed to the hostname and port of the SLB.

The response file can be found in the filesystem of the OMS host at:

<OMS_ORACLE_HOME>/sysman/agent_download/<version>/agent_download.rsp

3.3 – Using the Downloadable Agent With Real Application Clusters

In order to use the downloadable Agent feature in a clustered environment, users may choose to deploy either as standalone Agents on each host in the cluster, or as a single clustered Agent installation. The installation script supports command-line options to enable either case.

3.3.1 – Standalone Agents

Installing a standalone Agent on a cluster node while retaining the ability to discover cluster targets can be easily accomplished using the downloadable Agent script by using the –n <clustername> argument. Alternatively, the same can be accomplished by setting the value of the CLUSTER_NAME environment variable. Note that for 9.2 clusters, without setting or passing this value, the Agent will be unable to discover any cluster targets. For 10*g* Clusterware clusters, setting or passing this value is optional and only required in order to override the default cluster name; if it is not set or passed, the Agent will use as a target name the cluster name specified in the Oracle Clusterware installation.For example, the command to be executed might be:

./agentDownload.linux –b /scratch/oracle_products –n myCRS

This will install an agent on the target host that, while standalone, will have the ability to discover cluster targets for a cluster named “myCRS”.

3.3.2 – Clustered Agents

Clustered Agents can also be easily installed using the downloadable Agent script. This functionality is supported by using the –c <node1,node2,…> argument. Using this option will install the cluster Agent on all nodes specified in the node list. Similar to the standalone Agent, specifying the cluster name can also be done with the –n <clustername> argument or the CLUSTER_NAME environment variable. Without specifying the cluster name, the default name will be used as a target name.For example, the command to be executed might be:

./agentDownload.linux –b /scratch/oracle_products –n myCRS –c “node1,node3,node6”

This will install a clustered agent onto all three nodes in the cluster with target name “myCRS”.

4.0 – NFS Mounted Agent Installation

Enterprise Manager 10*g* R2 introduces the ability to install a single Agent on a shared NFS filesystem, and then have multiple hosts share that same ORACLE_HOME. This method of deployment places the host-specific configuration files in non-shared locations on each host called "state directories".

Note: NFS Agent Installation Is Not Supported on Microsoft Windows.

In order to install an NFS mounted Agent, the best practices are to follow these steps:

Configure a shared NFS disk so that hosts on which the agents have to be installed have read access to it.

On one of the host that has read access to the shared drive, perform an Agent installation in the shared area (using any standalone Agent deployment method).

Stop the Agent from the installed ORACLE_HOME – it should never be started from that location. To make sure that the agent does not start when the host is restarted remove the following script:

<Agent_ORACLE_HOME>/install/<platform name>/scripts/agentstup

From every host on which an NFS mounted Agent is desired (including the host from which the original Agent was installed), execute this script:

<Agent_ORACLE_HOME>/sysman/install/nfsagentinstall

If the NFS mounted Agent is the first Oracle product installed on the host, then the install process will prompt the user to execute the following script as the root user:

<install user home directory>/oraInventory/oraInstRoot.sh

At the end of installation, the install process will prompt the user to execute the following script as the root user:

<EM state directory>/root.sh

The usage of the "nfsagentinstall" script is as follows:

./nfsagentinstall –s <EM state directory location> –p <port number>

where:

<EM state directory location> = The full path to the location in which the state directory will be created.

<port number> = The port on which the Agent listens. Note that this is a required parameter.

Note: From Enterprise Manager 10.2.0.2 onwards it is not mandatory to specify the port number when running nfsagentinstall script.

The NFS mounted Agent installation can also be performed through the Agent Deploy application; (please refer to **section 5.2.3** for details.)

4.1 – Important Installation Notes

It should be noted that the Oracle inventory directory cannot be in a shared location, as it will contain information individual to each host. Thus, if the home directory of the install user is shared across multiple hosts, the default location for the inventory (which is a subdirectory of the user home) will not work.

If the NFS mounted Agent is the first Oracle product to be installed on a host (and the NFS install user's home is shared), the user will need to manually create a "oraInst.loc" file in the /etc directory. That file should contain the following two lines:

inventory_loc=/scratch/oraInventory [or any non-shared location]

inst_group=<group to which the install user belongs>

If the NFS mounted Agent is not the first Oracle product to be installed on a host (and the NFS install user's home is shared), then the user will have to review the contents of the /etc/oraInst.loc file to see if it uses an inventory in a shared location. If it does, the file will have to be edited to provide an inventory location in a non-shared directory.

Also, if the NFS mounted Agent is the first Oracle product to be installed on a host, the user will need to execute the following command in order to properly collect information about the host's inventory:

<EM state directory>/bin/emctl control agent runCollection <hostname>:host Inventory

Please see **Appendix A** for more details.

Finally, it should also be noted that the NFS mounted Agent can only be installed as the same user with which the master Agent was installed.

4.2 – De-installing a NFS Mounted Agent

The steps required for full removal of Agents installed via the NFS installation method depend on whether the Agent is the only Oracle product installed on the host or if other Oracle products are present. For hosts on which the NFS mounted Agent is the only Oracle product or on which the NFS mounted Agent is in its own inventory (and is the only product in that inventory), follow these steps:

Stop the Agent, using the following command:

<EM state directory>/bin/emctl stop agent

On windows box, user must delete the agent service by executing the command:

OH\bin\nmesrvops delete <agent service>

Find the location of the Oracle inventory by viewing the contents of:

/etc/oraInst.loc

Or, if the NFS mounted Agent is in its own inventory, identify the location of that inventory.

Delete the inventory directory using the following command:

rm –rf <inventory location>

Delete the state directory using the following command:

rm –rf <EM state directory>

For hosts on which other Oracle products than the NFS mounted Agent have been installed, follow these steps:

Stop the Agent, using the following command:

<EM state directory>/bin/emctl stop agent

From the mounted master Agent directory, execute the following command:

<master agent home>/oui/bin/runInstaller -detachHome ORACLE_HOME=<master agent home>

Delete the state directory using the following command:

rm –rf <EM state directory>

4.3 – Related Concepts

Where should the EM state directories for NFS mounted Agents reside?

> For security reasons, the state directories of Agents on different hosts should be local to each host, not on the mounted drive. The directories contain information about targets on each host, so the best practice is to keep the directory on the same host as the targets themselves.

Does running a NFS mounted Agent require any packages or operating system patches for shared hosts?

> As of the release of EM 10*g* R2, no specific packages or patches are required to support running an Agent on a shared host.

Can a NFS mounted Agent be installed on a cluster?

> NFS mounted Agent deployment is not supported on clusters. In order to monitor clustered hosts or RAC databases, the best practice would be to use the Agent Deploy application with the cluster option rather than the NFS deployment model.

5.0 – AGENT DEPLOYMENT FROM GRID CONTROL

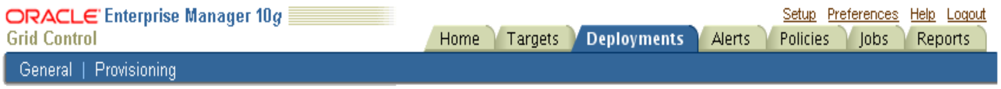
Another new feature in Enterprise Manager 10*g* R2 is the Agent Deploy application, which allows users to specify a list of hosts and "push" additional Management Agents onto those machines. This feature uses the SSH protocol to connect to the destination hosts and then to copy the required installation files and scripts; after that, the scripts are executed on those destination hosts and use the HTTP protocol to perform the installation (similar to the downloadable Agent).

It should be noted that interim patches may be required for successful use of the Agent Deploy application in Enterprise Manager version 10.2.0.1.0

In Enterprise Manager version 10.2.0.1 agent push is limited to pushing agents on the targets having the same platform as the one on which Enterprise Manager was installed. This limitation has been overcome in Enterprise Manager 10.2.0.2, which allows pushing of agents to different platform using the Grid Control.

To access Agent Deploy application:

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.

5.1 – Environment Setup for Agent Deploy Application

1) SSH equivalence:

As mentioned, the Agent Deploy application uses SSH to transfer files and execute remote commands (thus this installation method is not appropriate for environments that do not use, or block, SSH connections). SSH offers the following benefits:

The ability to transfer files

The ability to set/modify environments

The ability to remotely execute host commands

A high level of security compared to other remote execution methods (e.g. rsh)

While SSH is typically present on most Linux/UNIX systems, Windows hosts do not usually support SSH access by default. In order to allow the OMS to connect to Windows hosts, SSH services will need to be installed; agent deploy needs this along with other software tools that come along with the Cygwin suite (full collection of softwares packaged in Cygwin Suite). See, **Appendix C** for details. The full suite can be downloaded from:

http://www.cygwin.com

In order to prepare a host as a destination for Agent deployment, the user must run a script mentioned below to set up SSH connectivity between the OMS host and all hosts on which the Agent is to be installed. The purpose of this script is to allow seamless access by a user on the OMS host (which contains the installation files) onto the target hosts (onto which the installation files need to be copied). Without configuring this equivalency, the connection between the OMS host and the target hosts will continually be interrupted by requests for password authentication, thus removing the non-interactive capabilities of the application. Note that this equivalency is only one-way (from OMS host to target host), not in the opposite direction.

Depending upon the version of the Enterprise Manager the script can be found at the following location:

From Enterprise Manager version 10.2.0.2 onwards

<OMS_ORACLE_HOME>/sysman/prov/resources/scripts/sshConnectivity.sh

For Enterprise Manager version 10.2.0.1

For 10.20.1 if you want to push agents from an OMS installed on a linux box the following script needs to be run:

<OMS_ORACLE_HOME>/sysman/prov/resources/scripts/sshUserSetup.sh

For 10.2.0.2 if you want to push agents from an OMS installed on a Windows NT/XP host then the following script needs to be run:

<OMS_ORACLE_HOME>/sysman/prov/resources/scripts/sshUserSetupNT.sh

All the scripts above require the arguments "–hosts", followed by a double-quoted and space-separated list of hostnames, and "–user", followed by the username to be used for installation on the remote hosts. For example:

```
./sshConnectivity.sh –hosts "node6 node7 node8" –user oracle

                         OR

./sshUserSetup.sh –hosts "node6 node7 node8" –user oracle
```

These commands will set up SSH connectivity between the OMS host and each of the three specified remote hosts, using the "oracle" user.

The scripts will confirm connectivity between the OMS host and each of the remote hosts, and then ask for the user's password on the remote hosts (possibly multiple times). In order to test that the equivalency has been successfully created, the scripts will finish by attempting to run the "date" command remotely on the target hosts via SSH; if the final output is the date, then configuration succeeded. If the user is asked for a password once more while running the date command, then SSH connectivity was not successfully established.

For detailed help of the scripts and an example of the output generated by these scripts, see **Appendix B**.

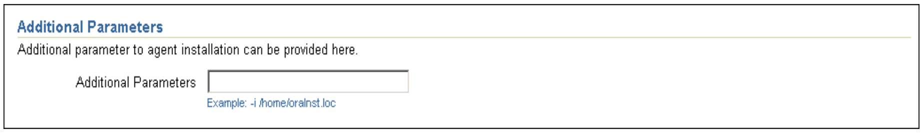
For more details on setting up SSH and using connectivity script on windows please see **Appendix C.**

2) Time Zone Configuration:

Successful Agent deployment requires that the host time zones be configured correctly. Even if destination hosts have the TZ environment variable set for logged in users, the SSH access needed by the Agent Deploy application usually does not have the variable set. The best practice for passing the correct time zone to the remote hosts is to use the "Additional Parameters" field on the Agent Deploy application's page, and specify the following:

-z <timezone>

e.g.: **-z PST8PDT**



Additional Parameters

Additional parameter to agent installation can be provided here.

Additional Parameters

Example: -i /home/oralnst.loc

Note that if the time zone is not set, the prerequisite checking of the application will fail, with the recommended fix to use the "–z" parameter from the application interface.

For more details on setting up timezone on remote hosts please see **Appendix D**.

3) 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 and remote host, you can specify the path to an alternative inventory location by using the -i <location> option in the Additional Parameters section mentioned above for default software location. For non-default software location use –invPtrLoc <location> option in the Additional Parameters section. Default and non-default software locations are explained in section 5.2 below.

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.

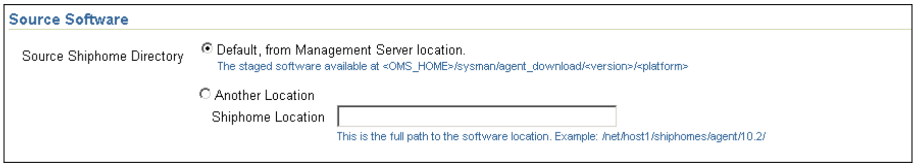
4) Verify User Credentials:

Ensure the user installing the agent belongs to the same group 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 using msu or sudo. This script must be run after the installation is complete in order to discover all the targets.

5.2 – Performing a Deployment

In order to access the Agent Deploy application, navigate to the "Deployments" page of Enterprise Manager, and select the "Install Agent" link. That will load the application, by presenting the option to perform a fresh install, add a host to a shared Agent, or upgrade Agents. In order to perform a deployment operation, choose "Fresh Install". The "New Agent Installation: Installation Details" screen will then be loaded, and will present a sequence of installation options.

The best practice for the source shiphome directory is to use the default option, which is location within the Management Server. It is worth noting that this location is the "Agent Download" directory of the OMS. Thus, only Agents for operating systems that have had their installation files placed in that directory can be deployed using this application. (For more information on adding additional platforms, please see the "Downloading to Alternate Platforms and Versions" subsection of the Downloadable Agent **section 3.0 and section 5.4)** If you are not using the default location then please make sure that the shiphome location you provide is shared and visible by all the hosts on which the agent has to be installed.



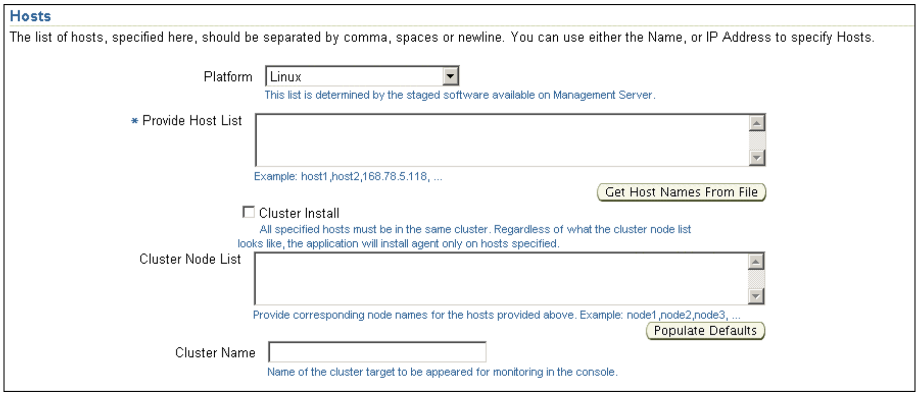
Source Software

Source Shiphome Directory ● Default, from Management Server location.
The staged software available at <OMS_HOME>/sysman/agent_download/<version>/<platform>

○ Another Location
Shiphome Location

This is the full path to the software location. Example: /net/host1/shiphomes/agent/10.2/

The hosts section is used to define the hosts that are to have Agents installed on them, as well as their platform. Only one platform type can be deployed to in a single operation – in order to deploy Agents onto hosts of platforms A, B and C, a user would be required to perform three operations (one for each set of machines on a single platform). Also, the list of platforms available in the drop-down menu corresponds to the platforms for which installation software exists in the "Agent Download" directory of the OMS.



Hosts

The list of hosts, specified here, should be separated by comma, spaces or newline. You can use either the Name, or IP Address to specify Hosts.

Platform: Linux

This list is determined by the staged software available on Management Server.

* Provide Host List

Example: host1,host2,168.78.5.118, ...

☐ Cluster Install

All specified hosts must be in the same cluster. Regardless of what the cluster node list looks like, the application will install agent only on hosts specified.

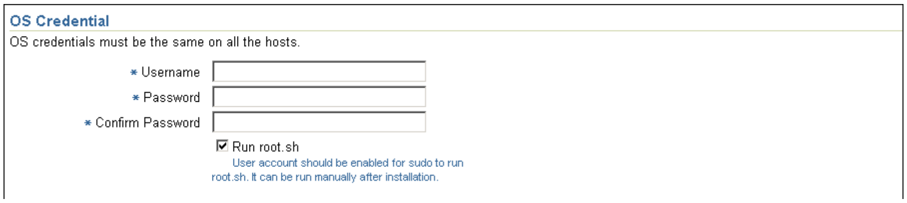
Cluster Node List

Provide corresponding node names for the hosts provided above. Example: node1,node2,node3, ...

Cluster Name

Name of the cluster target to be appeared for monitoring in the console.

The operating system credentials entered on the details screen must be the same for all hosts being deployed to in the current deployment operation. They must also be the same credentials used when running the sshUserSetup.sh/sshUserSetupNT.sh or the sshConnectivity script to set up SSH connectivity. If this user has "sudo" privileges enabled on the remote hosts, then having the deployment process run the root.sh script is recommended.



OS Credential

OS credentials must be the same on all the hosts.

* Username

* Password

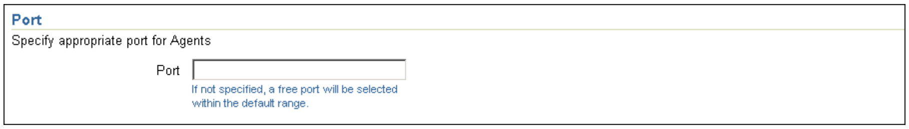
* Confirm Password

☑ Run root.sh

User account should be enabled for sudo to run root.sh. It can be run manually after installation.

The destination for the Agent installation will be the same for all hosts being deployed to in the current deployment operation. Make sure that the specified base installation directory is empty.

In most cases, there is no need to specify a port, as the application is able to detect a free port to use. Note that if a port is specified in this field, that port will be used for all hosts being deployed onto, regardless of whether that port is free or not.



Port

Specify appropriate port for Agents

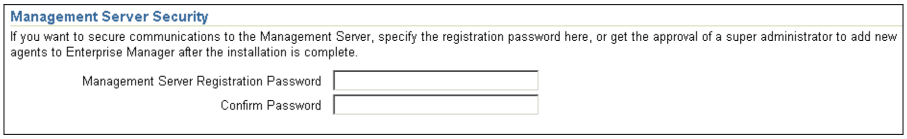
Port

If not specified, a free port will be selected within the default range.

For additional parameters that can be used, please see **Appendix G.**

Management Server Registration Password can be optionally provided in Manager Server Security section shown next. Providing the password will configure the agents to run in secure mode after installation. In Enterprise Manager version 10.2.0.x the communication between the he Oracle Management Service (OMS) and the agent can either be secure (over HTTPS between a secured agent and the Oracle Management Server) or insecure (over HTTP between a insecure agent and the Oracle Management Server). The Oracle Management Service runs in a secure mode and can further have a "locked" or "unlocked" state. If it is unlocked then both secure and insecure agents can talk to the Oracle Management service.If it is locked then only secure agents can talk to it. The password should be provided depending on the requirement of secure communication and the Oracle Management Server state. You can also secure the agent later sometime by issuing the following command:

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



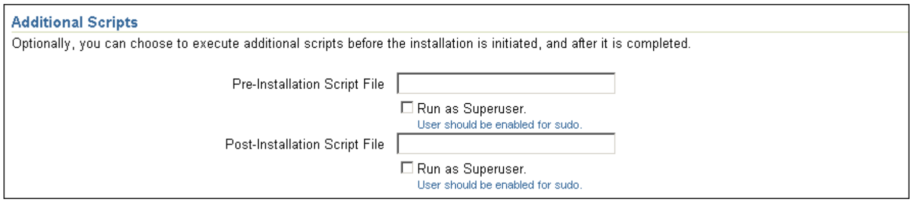
Management Server Security

If you want to secure communications to the Management Server, specify the registration password here, or get the approval of a super administrator to add new agents to Enterprise Manager after the installation is complete.

Management Server Registration Password

Confirm Password

Finally, the application offers the ability to run additional scripts both before and after installation. If the user being used for installation has "sudo" privileges, these scripts can optionally be run as root.



Additional Scripts

Optionally, you can choose to execute additional scripts before the installation is initiated, and after it is completed.

Pre-Installation Script File

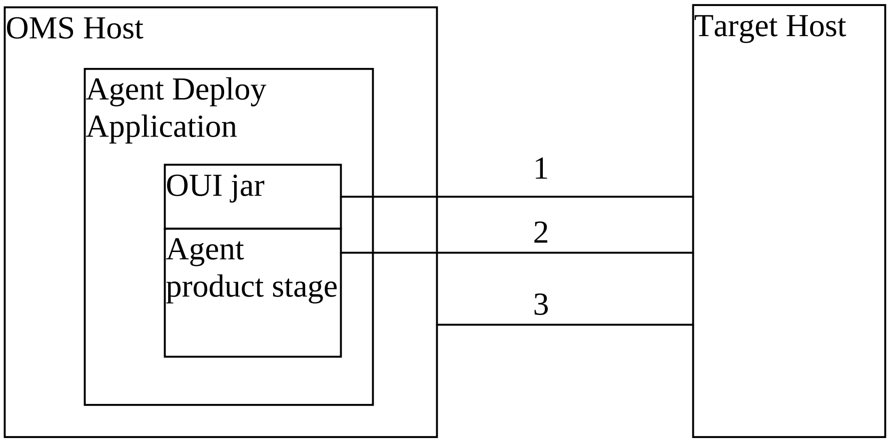
□ Run as Superuser.
User should be enabled for sudo.

Post-Installation Script File

□ Run as Superuser.
User should be enabled for sudo.

After details page is complete, the application will proceed to check connectivity between the OMS host and the hosts designated for Agent deployment. If 10.2.0.2 agents are being pushed then an additional page for Oracle Configuration Manager (see **section 5.5**) comes up before the application checks connectivity. Next, a series of prerequisite checks will be executed on the remote hosts. If any prerequisites fail or result in warnings, the application will display a page explaining the nature of the failures or warnings, and how they can be corrected. (For non-fatal warnings, the user will be offered the opportunity to ignore the messages and continue.) If no problems were found during the prerequisite checks, the actual installation itself will commence. Details of the pre-reqs checks and error resolution in case of pre-req failures can be found in **Appendix F**.

5.2.1 – Agent Deploy Architecture



Step 1: Both a dynamically generated script containing installation parameters and the Oracle Universal Installer (OUI) jar file are pushed to all target hosts via SSH.

Step 2: The OUI initiates HTTP-based installation of the Agent on all target hosts, using the product staging location on the OMS host as the product source.

Step 3: Agent installation completes, including execution of the root.sh file (if specified); the Agent then begins regular communication with the OMS.

Agent deploy application uses some commands that are required for successful execution of certain application programming interfaces (APIs), for example, the zip executable.on the remote target box and ping executable on the host having Oracle management server. The properties files located at <omshome>/sysman/prov/resources/ comprises the default locations of these commands required by the application. See **Appendix E** for details on these properties files and the their usage.

5.2.2 – Including Additional Files

It is possible to have the deployment process include additional files to be copied to the remote hosts. In order to include additional files, perform the following steps from the ORACLE_HOME of the OMS:

Change the active directory ("cd") to:

<OMS_ORACLE_HOME>/sysman/agent_download/10.2.0.1.0/linux/addons

Copy all files that you intend to deploy along with the Agent into this directory.

If necessary, modify the script file "userSetup.sh" to set desired permissions on files.

Execute the following command:

<OMS_ORACLE_HOME>/jdk/bin/jar/cvfM <OMS_ORACLE_HOME>/sysman/agent_download/<version>/<platform>/agent_scripts.jar *

All files in that directory will be extracted in the ORACLE_HOME of the newly installed Agent after the deployment process, and the set_perms.sh script will be executed to set any desired file permissions.

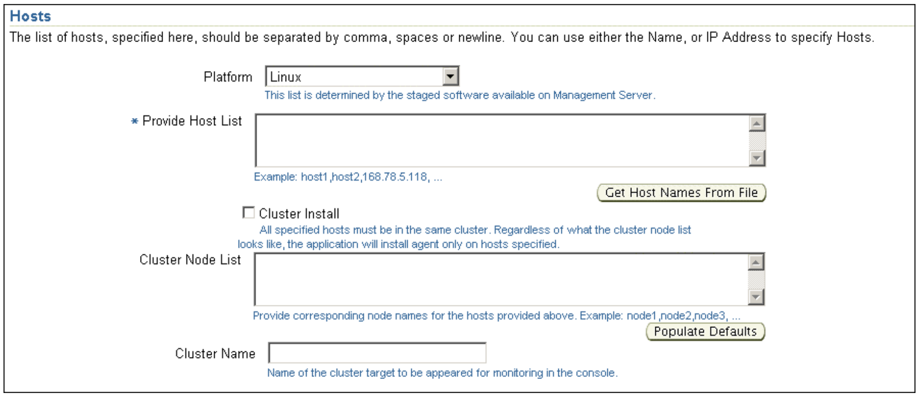
5.2.3 – Deploying on a Cluster

Standalone Agents

Installing a standalone Agent on a cluster node while retaining the ability to discover cluster targets can be accomplished by specifying the destination hostnames in exactly the same manner as with non-clustered installs. Entering the cluster name in the text field in the "Hosts" section does not work for standalone Agent installs for Enterprise Manager version 10.2.0.1; please see **Appendix A** for more details. For 10*g* Clusterware clusters, the default cluster name will be used as the cluster target name.

Clustered Agents

Checking the "Cluster Install" checkbox in the Hosts section and entering the nodes of the cluster in addition to their hostnames will install clustered Agents. For 10.2.0.1 and 10.2.0.2 Enterprise Manager versions please use the "Populate Details" button to populate the cluster node list. The cluster name is optional and can be specified in the appropriate text field; for 9.2 clusters using vendor cluster software, if the name is not specified, the cluster targets will take names of the form "<first node>_cluster". For 10*g* Clusterware clusters, entering the cluster name is only required if the user intends to override the default cluster name to be used as the cluster target name.



Hosts

The list of hosts, specified here, should be separated by comma, spaces or newline. You can use either the Name, or IP Address to specify Hosts.

Platform: Linux

This list is determined by the staged software available on Management Server.

* Provide Host List

Example: host1,host2,168.78.5.118, ...

□ Cluster Install

All specified hosts must be in the same cluster. Regardless of what the cluster node list looks like, the application will install agent only on hosts specified.

Cluster Node List

Provide corresponding node names for the hosts provided above. Example: node1,node2,node3, ...

Cluster Name

Name of the cluster target to be appeared for monitoring in the console.

Note 1: For Enterprise Manager version 10.2.0.1 and 10.2.0.2 please ensure that **no** the environment variables has a semicolon or space character it in. If present the cluster agent installation will fail. (For details, see "Cluster agent deployment fails with "Failed to copy file <agent O_H>/sysman/install/hosttgt.out to destination" in log file", known issue in **Appendix A**.)

Note 2: For Enterprise Manager version 10.2.0.1 and 10.2.0.2 please please use the "Populate Details" button to populate the cluster node list or provide only a comma ',' seperated list. For details, see "Cluster agent deployment fails with "Failed to copy file <agent O_H>/sysman/install/hosttgt.out to destination" in log file", known issue in **Appendix A**.)

5.2.4 – Deploying a NFS Mounted Agent

The Agent Deploy application can also be used to deploy shared NFS-mounted Agents (for more information on these types of Agents, please see the NFS Mounted Agent Installation section).

In order to deploy a shared NFS-mounted Agent, choose the "Add Host to Shared Agent" option from the initial Agent Deploy application screen. Most options are the same as those for a fresh Agent install, but this installation type includes fields to specify:

> The location of the master Agent ORACLE_HOME (which must be on a shared NFS drive, and visible and mounted on the destination host)
>
> The location of the state directory

Also different from the fresh Agent install is the "Port" field – for this install type, the port for Agent communication is a required field.

Note that the master Agent must be installed on the shared NFS drive before using the Agent Deploy application to add shared hosts to the Agent.

5.2.4.1 – Known Issues in 10.2.0.1.0

In the initial release of EM 10*g*R2, using the Agent Deploy application to deploy a mounted NFS Agent will not run the root.sh script, even if the "Run root.sh" checkbox is checked. Thus, after deployment, that script must be run manually on the hosts onto which the Agent was deployed. This will be fixed in the 10.2.0.2 release; please see **Appendix A** for more details.

Also as with NFS mounted Agents deployed via the "nfsagentinstall" script, if this NFS mounted Agent is the first Oracle product to be installed on a host, the user will need to execute the following command after the root scripts have been executed in order to properly collect information about the host's inventory:

<EM state directory>/bin/emctl control agent runCollection <hostname>:host Inventory

Again, this is fixed in the 10.2.0.2 release; please see **Appendix A** for more details.

5.3 – Additional Information

It is worth noting that the Agent Deploy application runs in a different OC4J (Oracle Containers For Java) container than Enterprise Manager. Consequently, problems or errors with the Agent Deploy application can be diagnosed and dealt with separately from EM. Should an application error occur, the best practice would be to stop and restart the OC4J instance in which Agent Deploy is running.

In order to stop and restart the application, perform the following steps:

Execute the following command:

<OMS_ORACLE_HOME>/opmn/bin/opmnctl stopproc process-type=OC4J_EMPROV

Execute the following command:

<OMS_ORACLE_HOME>/opmn/bin/opmnctl startproc process-type=OC4J_EMPROV

5.3.1 – Ignoring Banner Messages

Some hosts can be configured to present a banner message to users who connect via SSH; this banner message is typically stored in the files /etc/issue or /etc/issue.net. However, since the SSH connection used by the Agent Deploy application will receive and attempt to parse this banner message, successfully deploying an Agent in this scenario will require configuring the OMS to ignore the banner message.

In order to do this, the exact contents of the banner message should be added to the end of this file:

<OMS_ORACLE_HOME>/sysman/prov/resources/ignoreMessages.txt

Note that this may require copying the contents of the /etc/issue or /etc/issue.net file from a target host onto the host on which the OMS resides, in order to put those contents in the ignoreMessages.txt file.

5.3.2 – Runtime System Requirements

The average CPU consumption on the host on which the OMS resides has been measured at approximately 15%, on Linux hosts with two Pentium 4 3.00 GHz processors. (This was sampled during deployment operations of anywhere from six to nine target hosts.) Additionally, at least two Gigabytes of memory are required.

5.3.3 – Using non default SSH port

The Agent Deploy application by default needs SSH to be running on its default port 22. If for some reason the SSH ports for your environment are different then you need to edit the file /etc/ssh/ssh_config on OMS box .In this file just uncomment the following line:

“Port 22” and change it to the target box's sshd-port value (say **“Port 23”**).

Make sure the non-default port value (say 23) is the port of sshd on EACH targets-box.

5.3.4 – Command locations

Agent Deploy application needs locations of some commands that are required for successful execution of certain application programming interfaces (APIs), for example, the ping executable. The paths for these executables are present in properties files located at <omshome>/sysman/prov/resources/. Please see **Appendix E** for details.

5.3.5 - For known issues of agentdeploy application please see Appendix A.

5.3.6 – For Troubleshooting Information like location of log files and common problems please see Appendix H.

5.4 Patch Information for Cross Platform Agent Push

For Enterprise Manager version 10.2.0.2, doing a cross platform push using the Agent Deploy application you should apply patch number 5455350 to your 10.2.0.2 OMS. The details of this patch can be found in section "Patch for cross platform agent push in Enterprise Manager 10.2.0.2" in **Appendix J**.

For Enterprise Manager version 10.2.0.1, doing a cross platform push using the Agent Deploy application you should apply patch number 4645135 to your 10.2.0.1 OMS. This patch is only available for Linux x86 and Solaris (SPARC-64bit) platforms. The details of this patch can be found in section "Patch for cross platform agent push in Enterprise Manager 10.2.0.1" in **Appendix J**.

5.5 A Note on Oracle Configuration Manager (OCM)

Oracle Configuration Manager (OCM) allows you to associate your configuration data with your Oracle MetaLink account. On a periodic basis, information will be uploaded to Oracle over a secure communications link and made accessible to you via MetaLink.

The data collected does not include personally identifiable information (with the exception of a local contact name in case of transmission problems) or business data files residing in your production environment. You may still use all licensed Oracle functionality if you decline to enable the Oracle Configuration Manager.

6.0 – AGENT CLONING

A simple way to deploy management Agents across an enterprise would be to clone an existing Agent install. This has the benefit of using an Agent installation known to be working, patched to the appropriate level, and certified for use. This functionality is only available by executing command-line utilities, not from the Grid Control console.

Note: It should be noted that Agent cloning is **not supported** to deploy Agents onto clusters.

The steps for deploying an Agent via cloning are as follows:

Install a Management Agent using any method, and patch/certify the installation as desired.

Zip or tar the Agent's ORACLE_HOME, and transfer the archive to the destination location or locations.

Unzip or expand the archive in the destination location.

Inside the now-unpacked ORACLE_HOME, execute the following command:

<Agent_ORACLE_HOME>/oui/bin/runInstaller –clone –forceClone ORACLE_HOME=<full path of ORACLE_HOME> ORACLE_HOME_NAME=<ORACLE_HOME name> -noconfig -silent

Run the Agent configuration assistant to configure the Agent and discover the host's targets by executing the following command:

<Agent_ORACLE_HOME>/bin/agentca –f

Run the newly cloned Agent's root.sh script:

<Agent_ORACLE_HOME>/root.sh

In order to enable secure communication between the Agent and the OMS (a required step if the OMS requires secure communications), secure the Agent by executing the following command:

<Agent_ORACLE_HOME>/bin/emctl secure agent

APPENDIX A

Some of the 10.2.0.1.0 known issues are also applicable for 10.2.0.2 and vice-versa.

Known Issues and Workarounds related to the Agent Deploy Application in EM 10.2.0.1.0

1) Hostnames used to set up SSH connectivity via the sshUserSetup.sh script must be identical to the hostnames listed in the Agent Deploy application (Bug 4679997).

Using a fully qualified domain name (e.g. "host8.mycompany.com") in one and a non-qualified hostname (e.g. "host8") in the other will cause the Agent Deploy application to fail.

Workaround: make sure to use the exactly the same hostname in both the SSH connectivity setup script and the Agent Deploy UI.

2) Accessing the Agent Deploy application via a server load balancer (SLB) will not work (Bug 4690736).

If an EM environment is using a SLB, the link to the application will also use the hostname of the SLB in its URL.

Workaround: in order to perform a successful deployment, the user will have to manually change the browser URL to use the hostname of the particular OMS host on which the SSH connectivity setup script was run.

3) Choosing "Another Location" for "Source Shiphome Directory"(Bug 4576575).

When asked to choose the Source Software on the Installation Details page, do not choose the "Another Location" option for "Source Shiphome Directory."

Workaround: always use the "Default, from Management Server location" option for Agent source software.

4) Installing a standalone agent on a cluster node (Bug 4711588)

The "Cluster Name" text field in the "Hosts" section of the Installation Details page is not usable unless the "Cluster Install" checkbox is checked, which will prevent users from specifying the cluster's name while installing a standalone Agent on a cluster node. For 10g Clusterware clusters only, the default cluster name in the Agent's target.xml will be used for cluster target discovery.

Workaround: If the cluster is a 9.2 cluster or a 10*g* Clusterware cluster with a name different from that in the target.xml file, the user will need to reconfigure the Agent from the command line after it has been installed. In order to do that, execute the following command:

```
<Agent_ORACLE_HOME>/bin/agentca –f –n <cluster_name>
```

Other Agent Installation Known Issues and Workarounds in EM 10.2.0.1.0

1) Upon Agent installation on the SLES 9 platform, the automatic agent startup link points to an incorrect location. (Bug 4765942)

Workaround: Manually change the link location by executing the following command:

```
ln -s /etc/init.d/gcstartup /etc/init.d/rc3.d/S99gcstartup
```

2) Agent installation on the Solaris platform fails on Prereq check by saying SUNWsprox package missing. (Bug5103613)

This issue has been fixed in the 10.2.0.2 Solaris agent shiphome. Please use this shiphome for installing the agent on Solaris platform.

Known Issues and Workarounds related to the Agent Deploy Application in EM 10.2.0.2.0

1) At the end of Cluster agent deployment, the Deployment page does not come up (Bug 4673479)

For a shared cluster deployment, at the end of the deployment, the applicatiowill not bring up the deployment page. It will bring up the status page only. The status page shows details of deployment and you will be able to identify whether deployment succeeded or not.

2) Oracle Configuration Manager (OCM) collector only configured for local node for agent installation in Real Application Cluster environment (Bug 5083308)

For an agent installation in a Real Application Clusters (RAC) environment, the Oracle Configuration Manager (OCM) collector is only installed and configured on the local node. On the remote node, the OCM collector is installed but not configured. To configure the OCM collector on the remote agent nodes, construct an Oracle Enterprise Manager Grid Control OS job to complete the configuration.

From the Oracle Enterprise Manager Grid Control home page, perform thefollowing steps:

1. Go to Jobs Tab.

2. Select the host command from Create Job drop-down list and specify a

suitable job name.

3. Go to Parameters.

4. Select command type to be os script.

5. Specify /bin/sh $ORACLE_HOME/ccr/bin/setupCCR –s <csi>

<metalink-id> <country-code>.

Where <csi> is the Customer Support Identifier, <metalink-id> is the Oracle Metalink Id and <country-code> is the country code specified during the OUI install. If a proxy is required for the server to access the internet, the setupCCR

command should also contain the –p qualifier specifying the proxy.

$ORACHE_HOME/ccr/bin/setupCCR –h describes the command syntax for proxy specification.

3) sshUserSetup fails with "Bad owner or permissions on the file XYZ" (Bug 5157782)

If the sshUserSetup fails with "Bad owner or permissions onthe file XYZ" error, then check the umask option on the local and remote machines by using the unmask command.

Workaround: Then, set the umask to 022 on the local machine before running the script. On remote machines, the umask should be set to 022 in the rc of the shell. For example, bashrc.

4) AGENT_INSTALL_PASSWORD needs to be set for non-default agent download (Bug 5124872)

The default platform agent download stage that gets installed with the OMS, will have the agent registration password in the response file that was used for securing the OMS, hence the default platform agent download installs can use this password from response file or overwrite it by setting AGENT_INSTALL_PASSWORD environment variable.

Workaround: The agent download kits that will be manually staged into OMS home of adifferent platform of the agent download, the response file will not have the password, so if users want to secure the agent, they have to set the AGENT_INSTALL_PASSWORD environment variable and invoke the agentDownload script, else the agent download script will prompt for password.

5) 10.2.0.1 deployment requires OS locale to be set to en_US (Bug 5116075).

When you deploy 10.2.0.1 agent using "push" method, in the host where agent will be deployed, the OS locale should be English locale (en_US). If the locale is other than English, such as zh_CN or ja_JP, it will fail in the pre-requisite check stage. This issue has been fixed in 10.2.0.2 agent. To work around this issue, deploy 10.2.0.2 agent. If you need to deploy 10.2.0.1 agent, perform the deployment in English environment.

6) Cygwin has to be in the same location on all target hosts and the OMS machine (Bug 5037758).

Cygwin on a different location may be c:\ABCD\. But this has to be same on all of the remote hosts and OMS machine. Note that the path should not have a space in it. To do this, you need to modify the ssPaths_msplats.properties file or the userPaths.properties file.

7) Database status shows "Unavailable" after being discovered by the agent (Bug 4954787).

After an agent discovers a database (at the end stage of an agent installation) the status of database is "unavailable". The reason is that Enterprise Manager does not know the password of "dbsnmp" to monitor and manage the database.

Workaround:

You need to logon EM, go to database list page and configure the database again.

8) Sometimes reconfiguration of agent on Real Application Clusters requires agent to be secured manually (Bug 4912661).

In the Real Application Clusters (RAC) Agent install, after you reconfigure a secured Management Agent using the <AGENT_HOME>/bin/agentca –f script, check its status. Ideally, the Management Agent should have regained its secured status in spite of being reconfigured. However, if the Management Agent is not secured, you need to manually secure it by running the following script:

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

9) "Another location" used to provide the non-default location for agent shiphome should be shared and visible from target hosts (Bug 5178469).

If you try to install an Agent from a non-default shiphome, you cannot use the agentdownload shiphome as it is. If you do so, the installation will fail.

Workaround: To workaround this bug, perform the following steps:

1. Download the AgentDownload shiphome from OTN to some location, say /shared/mydir/, which is visible as /net/shared/mydir/ from target boxes.

2. Unzip it, you will get /shared/mydir/linux/ directory with the following contents:

addons/

agentDownload.linux

agent_scripts.jar

agent/

oui/

prereqs/

response/

3. Rename or Copy /shared/mydir/linux/agent to

/shared/mydir/linux/Disk1/

4. Use /net/shared/mydir/linux/ as the NFS shiphome location.

10) Agent deplooyment fails with “Values for the following variables could not be obtained from the command line or response file(s)” message (Bug 5183333).

When you install a 10.2.0.2 agent through Agent Deploy application using non-default shiphome option, it may fail with the following error:

SEVERE: Values for the following variables could not be obtained from the command line or response file(s):

ToplevelComp (TopLevelComp) Silent install cannot continue.

Workaround:

1. Go to <oms-home>/sysman/agent_download/10.2.0.1.0 directory and open the agent_download.rsp file.

2. Replace the line TOPLEVEL_COMPONENT={"oracle.sysman.top.agent","10.2.0.1.0"} with

TOPLEVEL_COMPONENT={"oracle.sysman.top.agent","10.2.0.2.0"}.

3. Save the agent_download.rsp file and try the installation again.

11) Cluster agent deployment fails with “Failed to copy file <agent O_H>/sysman/install/hosttgt.out to destination” in log file. (Bug 5208716)

Installation failure is also observed if **any** environment variable contains semicolon (';') or space (‘ ‘) character.

Workaround:

Look for the all the environment variables with a space or semicolon that have been set on all the cluster nodes. These could be any environment variables and not just Oracle specific environment variables. Unset all these variables. Then use the runconfig utility to reconfigure the cluster agents as mentioned below:

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

ACTION=configure
```

Windows Specific known Issues and Workarounds related to the Agent Deploy Application in EM 10.2.0.2.0

1) Unsuccessful SSH Setup (Bug 5103331, 5090704)

On Microsoft Windows, after installing the cygwin ssh server, one has to enable users to log in via ssh by using the mkpasswd command that adds passwd entry for that user in the /etc/passwd file.

For example:

```
mkpasswd -d -u userid >> /etc/passwd
```

```
mkpasswd -l -u userid >> /etc/passwd
```

This is how a passwd entry looks in the /etc/passwd file:

```
aime1:unused_by_nt/2000/xp:36357:10513:U-ST-ADC\aime,S-1-5-21-22612181

-1167196868-26564730-26357:/home/aime:/bin/bash/
```

where "aime1" is the login id that is mapped to "aime/ST-ADC" on the machine. After the /etc/passwd file is updated, the command "ssh -l userid m/c 'date'" to check the date may run successfully, but the sshUserSetupNT.sh may not succeed.

One of the reasons for the sshUserSetupNT.sh to fail is that your /etc/passwd file may have multiple entries for a particular login id. These multiple entries cause conflicts with the permissions on your home directory. For example:

"STINST03\aime" and "ST-ADC\aime"

where "aime" is the login id for both STINST03 and ST-ADC.

Workaround: To resolve this issue, do one of the following:

1. Update the /etc/passwd file to specify different login names for different user accounts. This will ensure that you have unique login names. For example:

"aime1" for STINST03\aime

"aime2" for ST-ADC\aime

2. Edit the /etc/passwd file to remove entries that are not required. This will ensure that you do not have multiple entries with the same login name.

For example:

If you have entries like STINST03\aime and ST-ADC\aime in your /etc/passwd file, where "aime" is the login id for both STINST03 and ST-ADC, and if you want to setup ssh for "STINST03\aime" only, then edit the /etc/passwd file to retain the entry for "STINST03\aime" and remove the entry for "ST-ADC\aime".

Note: Ensure that you do not remove any other entries (like the SYSTEM entries).

2) Errors While Setting Up SSH Connection (Bug 5144511)

When you set up an ssh connection from an Oracle Management Service running on Microsoft Windows to a remote machine, you may see a java exception if you do not have the /.ssh directory in the cygwin bash prompt ("/" here points to the cygwin directory).

Workaround: To resolve this issue, manually create the /.ssh directory in the cygwin bash prompt. To do so, follow these steps:

1. Access the CD and navigate to c:\cygwin bash prompt.

2. Create the directory by running mkdir .ssh.

3. Run this command on the local machine:

```
./sshConnectivity.sh -user <username> -localPlatformGrp win -asUser
```

Your command should look like:

```
./sshConnectivity.sh -user <username> -localPlatformGrp win -asUser <should be –SYSTEM for agentpush>

[-asUserGrp <group, which the user specified in asUser belongs to>] -sshLocalDir <cygwin installation directory (C:\cygwin by default)> -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 jwarne -localPlatformGrp win -asUser SYSTEM -asUserGrp root –sshLocalDir "C:\cygwin"

 -hosts hostname1.host.com
```

Note: Always specify the path in double quotes.

3) Prerequisite for Agentpush on SSH Client (Bug 5068074)

Sometimes, when you install an Agent Push on a machine where SSH client is set up, you may see the following error message:

Application Error Message: Internal Application Error. Click Home to go to Application Home Page.

This may happen if the ssPaths_msplats.properties file located in the $OMS_HOME/sysman/prov/resources/ directory has incorrect path for cygwin binaries and ping binaries.

Workaround: To resolve this issue, ensure that the ssPaths_msplats.properties file points to the correct location where cygwin and ping are actually located.

For cygwin binaries:

By default, cygwin gets installed in C:\cygwin drive, and the ssPaths_msplats.properties file has the following entry:

```
MKDIR_PATH=C:/cygwin/bin/mkdir.exe
```

However, if you choose to install cygwin in any other directory that is after installing Enterprise Manager Grid Control then update the ssPaths_msplats.properties file with proper values for the cygwin binaries. For example, if you choose to install cygwin in D:/cygwin1, then update the path from MKDIR_PATH=C:/cygwin/bin/mkdir.exe to MKDIR_ PATH=D:/cygwin1/bin/mkdir.exe.

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\/
```

Also, 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 that these files are part of the platforminfo.properties file. If they are not, then 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. Similar changes need to be done to all the cygwin entries in this properties file.

For ping binaries:

By default, the ping executable is located in C:\WINNT\system32\. However, the ssPaths_msplats.properties file may show the following entry:

PING_PATH=C:\\WINDOWS\\system32\\ping.exe

So update the ssPaths_msplats.properties file by modifying the existing entry to:

PING_PATH=C:\\WINNT\\system32\\ping.exe

4) sshUserSetupNT.sh Script Displays an Error Despite Successful Execution (Bug 5135679)

When you run the sshUserSetupNT.sh script to set up the SSH on a remote machine, you may see the following error even if the execution ends successfully:

chmod: getting attributes of `c:\\Documents and Settings\\aime\\.ssh\\authorized_keys': No such file or directory

Technically, the script checks for authorized keys in the specified location, and if they are not found, the script creates the keys in that location and completes the execution. However, it displays an error despite completing the set-up successfully.

If you see the date displayed at the end of the execution, consider this error to be harmless and ignore the message. Your set-up has been successful. However, if you do not see the date displayed at the end of the execution or you are prompted for password, then your set-up has not been successful.

5) SSHCONNECTIVITY Script Asks for a Passwood at the End of the Execution Due To Home Directory Inconsistency (Bug 5370763)

If the cygwin bash prompt home directory is set to /home/aime, and the actual home directory is something like C:\Documents and Settings\aime.ST -ADC, then due to this home directory inconsistency, the .sshconnectivity script asks for a password at the end of the execution. Ideally, this script should not ask for a password at the end of the execution. However, the password is asked only because of the home directory inconsistency.

Workaround: Provide the password and proceed with the push install. Or alternatively run the sshConnectivity.sh script with –homeDir option, which should have the proper path of the cygwin bash home directory. In this example the value to be passed with –homeDir option should be “C:\Documents and Settings\aime. ST –ADC”.

6) Exceptions While Starting CMSDK Domain Controller (Bug 4883113)

When 10.2.0.2 Management Agent and CMSDK's "ifsctl start" are installed on the same machine, you may encounter an exception when you run "ifsctl start" on that machine to start the CMSDK domain controller. This is because the 10.2.0.2 Management Agent install prefixes its directories to the path of the system environment variable.

Workaround: To avoid this exception, manually remove $AGENT_ORACLE_HOME related entries from the system environment variable "PATH", and then run "ifsctl start".

Note: This issue occurs only if CMSDK is installed first and then Management Agent is installed.

7) Interview Page Displays an Error While Deploying Management Agent from Oracle Management Service (Bug 5246184)

The interview page displays an error while deploying a Management Agent from Oracle Management Service on Microsoft Windows NT. In the <OMS_HOME>/opmn/logs/OC4J~OC4J_EMPROV~default_island~1 log file, you will find this message:

The action 'runlocalprereqs' failed.

In the OMS_ HOME>/sysman/prov/agentpush/<time-stamp>/cfgtoollogs/cfgfw/CfmLogger_<time-stamp>.log file, you will find this message:

INFO: CfwProgressMonitor:plugInEnd: PlugIn=RunLocalPrereq_msplatOMS in MicroStep=0, type=External Command PlugIn, status=Has been aborted

Workaround: To resolve this issue, ensure that on the machine running Oracle Management Service, the localtion pointed by environment variable TEMP is writable, and all the directories under TEMP have read/write permissions.

8) Installation from a Non-Default Release Location Is Not Supported for Microsoft Windows NT (Bug 5097303)

Installation from a non-default release location is not supported in case of Microsoft Windows NT. If the user selects Windows from the agentpush dropdown menu, the non-default release choice gets disabled.

9) Unclear Error Message for Passwords (Bug 4917719)

While installing 10.2.0.2 Enterprise Manager, you will be asked to specify the registration password for Management Service Security and the SYSMAN password for SYSMAN account. If you provide invalid passwords, you may see the following message:

Note: Enterprise Manager implements a password policy requiring passwords to be at least 5 characters long, with at least one number. Passwords must start with an alphabet character. Re-enter the secure Management password.

Note that although this message does not have a mention of the special characters, ensure that you DO NOT use any special characters in your password other than "-" (hyphen), "_" (underscore), and "$" (dollar).

10) Parent Directory Path Validation Rule (Bug 4908224)

While installing 10.2.0.2 Enterprise Manager, you are asked to specify the location for the parent directory. Note that the sub-directories you specify in the location should be an alpha-numberic value, and can have characters like "_" and "-". Besides these characters, you are not permitted to use any other special characters as the directory name. However, you can use ":" for specifying the drive. Also, ensure that directories and subdirectories you specify in your installation path begin with letters other than "u".

11) During Upgrade of Oracle Management Service with Seed Installation, the Old Services Do Not Get Disabled or Removed (Bug 5186434)

On Microsoft Windows, for Oracle Management Service with seed installation, after the upgrade of Oracle Management Service is complete, the startup type of the old Listener in the previous version of database home would need to be switched to "Disabled". Once that is done, the startup type of the new Listener in the updated seed database for the upgraded Oracle Management Service would need to be switched to "Automatic".

12) Oracle Management Service Config Fails with Exception "The Pipe Is Being Closed" (Bug 5203206)

Workaround: Close the installer and run the config using this command:

```
<OH>/oui/bin/runConfig.bat ORACLE_HOME=<OH> MODE=perform ACTION=configure
COMPONENT_XML={XML name}
```

For EM Using New DB installs:

-- <OH> is <DB Home>

-- <XML name> is encap_emseed.1_0_0_0_0.xml

For EM Using Existing DB & Additional OMS installs:

-- <OH> is <OMS Home>

-- <XML name> is encap_oms.1_0_0_0_0.xml

13) ORACLE_HOME Has To Be Unset Before Invoking setup.exe (Bug 5022962)

When Oracle Management Service installation is about to begin, an error message "ORACLE_HOME should not be set" appears if ORACLE_HOME is set.

Workaround: To resolve this issue, delete ORACLE_HOME from system environment before invoking setup.exe.

14) Net Config Fails While Installing or Ugrading Enerprise Manager using 'EM Using New Database' Option (Bug 5236773)

While installing or upgrading using the "EM using new database" option, the Net Config Assistant fails with the following error:

"UnsatisfiedLinkError exception loading native library: oranjni10"

Workaround: To resolve this issue, reboot the machine and retry the config using this command:

```
<DB Home>\oui\bin\runConfig.bat ORACLE_HOME=<DB Home> MODE=perform ACTION=configure COMPONENT_XML={encap_emseed.1_0_0_0_0.xml}
```

15) Oracle Management Service Config Hangs While Dropping the Repository (Bug 5085466, 5260792)

While installing Enterprise Manager, the Oracle Management Service Config hangs while dropping the repository if there are active SYSMAN sessions connected to the database.

Workaround: To resolve this issue, you have to end those active SYSMAN sessions connected to the database. To do so, follow these instructions:

1. Stop the config.

2. Shutdown the database.

3. If database is on Microsoft Windows, then stop the OracleService<SID> service.

4. If database is on Microsoft Windows, then start the OracleService<SID> service; else startup the database using "startup" command through sqlplus.

5. Retry the config.

16) Management Agent (version 10.1) for Microsoft Windows Cannot Be Installed Against 10.2 Oracle Management Service (Bug 5237309)

When you install a 10.1 Management Agent for Microsoft Windows against a 10.2 Oracle Management Service, the installation may hang at the Agent config phase while discovering the targets.

Workaround: The workaround is to stop the installation and discover the targets from the console.

17) IAS Console Password Defaults to "WELCOME1" After the Upgrade Is Complete (Bug 4650351)

The ias_admin password for the IAS Console will be defaulted to "welcome1" after the Enterprise Manager Grid Control 10.2 upgrade process is complete. The user should modify the ias_admin password by executing the following command:

<new_OMS_Home>/bin/emctl set password welcome1 <new_password>

18) Installation and Upgrade Fails if the Environment Variable Path Is Too Long (Bug 5093853)

On Microsoft Windows 2000 and Windows NT, the install or upgrade operation may fail if the value of the environment variable path is more than 1023 characters.

Similarly, for Microsoft Windows XP, the install or upgrade operation may fail if the value of the environment variable path is more than 8191 characters.

Workaround: For silent installation, there is no resolution for this issue. However for interactive installation on Microsoft Windows 2000 and Windows NT, you can resolve this issue by first reducing the value of the environment variable path to less than 1023 characters, and then retrying the install or upgrade operation. For interactive installation on Microsoft Windows XP, reduce the length of the environment variable path to less than 8191, and then retry the install or upgrade operation.

19) Oracle Universal Installer Displays Incorrect Secure Grid Control URL When Upgrading from 10.1 (Bug 5120305)

At the end of the Oracle Management Service upgrade install, Oracle Universal Installer displays incorrect secure Grid Control URL.

To access the secure Oracle Management Service Grid Control URL, open the emoms.properties file from the <UPGRADED OMS HOME>/sysman/config/ directory, copy the secure port provided for "oracle.sysman.emSDK.svlt.ConsoleServerHTTPSPort", and then paste that port number in the secure Grid Control URL, that is

https://<hostname>: <portnumber>/em.

Note: This will happen only if the base, that is 10.1, Oracle Management Service is not secure.

20) NFS Agent Installation Is Not Supported on Microsoft Windows (Bug 5307539, 5178469)

The NFS Agent installation is not supported on Microsoft Windows.

21) Issues While Installing Management Agent on Shared Location (Bug 5117689)

In order to install 10.2.0.2 Management Agent on a machine that has Microsoft Windows operating system with RAC/OCFS on a shared location, the device SYMTDI (if there is any) needs to be disabled on all the nodes.

To do so, follow these steps:

-- Bring up Computer Management on each node.

-- Click Device Manager.

-- On Menu View, select Show hidden devices to display the legacy devices and the devices that are no longer installed.

-- Click NON-PLUG and PLAY DRIVER.

-- In the right pane, right click SYMTDI and select Disable.

-- Click OK to reboot the machine.

22) NT Shared OH Cluster Upgrade Fails (Bug 5312081)

The installation status page shows the following message for the local node:

"Upgrade : Success, Collection of Logs : Success"

And on the remaining nodes (or failed nodes), you get the following message:

"Upgrade : Not Executed, Collection of Logs : Not Executed"

Workaround: To resolve this issue, do the following on each of the failed nodes, that is all the nodes other than the local node:

1. Run <new_agent_home>/oui/bin/<node>.upgrade.bat

2. Run <new_agent_home>/bin/emctl.bat start agent

3. Run <new_agent_home>/bin/emctl.bat stop blackout Agent_Upgrade

Note: Local node is the first node of the host list that you specify on the interview page, or the first node in Remote Host Names of the Session Details page.

23) Menu Lists Only Those Platforms That Are Supported by Agentpush (Bug 5303864)

The 10.2.0.2 Agentpush supports Linux (32 bit); Microsoft Windows NT, Microsoft Windows 2000 (32 bit); IBM-AIX; HP - UX; SOLARIS (32 bit).

Other platforms are not supported. So even if you add the other shiphomes in the Oracle Management Service, these platforms will not appear in the dropdown menu.

24) Only Host and Cluster Get Discovered During RAC Agent Install (Bug 5362120)

When a RAC Agent is installed on Microsoft Windows, only the host cluster targets get discovered during install. After the install, the user can execute the following commnd on each node to discover all the targets:

```
<Agent Home>/bin/agentca -d -n <Cluster Name> -c <node name>
```

25) Application Error Displayed When the Microsoft Windows NT Machine CYGWIN Is in a Location Other Than C Drive (Bug 5037758)

Cygwin on a different location, may be c:\ABCD\. But this has to be same on all of the remote hosts and Oracle Management Service machines. To do this, you need to modify the ssPaths_msplats.properties file or the userPaths.properties file.

26) Metric Collection Errors for Database Target (Bug 4954787)

After a Management Agent discovers a database (at the final installation stage of a Management Agent) the status of that database is "unavailable". The reason is that Enterprise Manager does not know the password of "dbsnmp" to monitor and manage the database.

Workaround: To resolve this issue, you need to login to Enterprise Manager, go to the Database List page, and configure the database again.

27) RAC Agent Not Secured (Bug 4912661)

In the Real Application Clusters (RAC) Agent install, after you reconfigure a secured Management Agent using the <AGENT_HOME>/bin/agentca –f script, check its status. Ideally, the Management Agent should have regained its secured status in spite of being reconfigured. However, if the Management Agent is not secured, you need to manually secure it by running the following script:

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

28) Patch Cache Needs To Be Increased For Patching/Upgrading From 10.2.0.1 To 10.2.0.2 Management Agent (Bug 5211366)

We cannot patch 10.2.0.1 Management Agent to 10.2.0.2 using 10.1.0.x Oracle Management Service because the patch cache size is insufficient to accommodate the 10.2.0.2 patch set.

29) WGET Cannot Get PATHSET.RSP (Bug 5353343)

This is happening only in the RAC environment. For RAC environment, place the wget.exe in the AGENT_HOME/bin directory.

Note: This bug is only for Method 2 that is while using the 3731596.zip file.

HP -UX specific known Issues and Workarounds related to Agent Installation in EM 10.2.0.2.0

1) "agentDownload.hpi: not found" error is seen in log files (Bug 5383553)

When agentDownload.hpi is edited (to edit oms host, version,port),this file is saved in dos format. So this script won't execute in HPUX machine(which fails saying filenot found error).
Workaround: Run dos2unix from OMS cygwin prompt for agentDownload.hpi file.

Known Issues and Workarounds related to NFS Mounted Agent Installation in EM 10.2.0.1.0

If a user attempts to perform an NFS mounted Agent installation on a host that has a different time zone than the host on which the master Agent is installed, the mounted Agent may fail to start. (Bug 4661323)

Workaround: execute the following commands on the new host:

```
<EM state directory>/bin/emctl config agent updateTZ
```

```
<EM state directory>/bin/emctl start agent
```

Only one NFS mounted Agent can be installed on any given host. (Bug 4687105)

Workaround: use the Agent Deploy application for installation of an additional agent on the same host, if required.

As mentioned above in the NFS mounted Agent important installation notes, if a NFS mounted Agent is installed as the first Oracle product on a host, host inventory collection does not occur automatically. (Bug 4683334)

Workaround: in order to perform collection, the user must perform either of these two steps after the root scripts have been executed:

Either execute the following command:

```
<EM state directory>/bin/emctl control agent runCollection <hostname>:host Inventory
```

Or alternatively, after executing the oraInstRoot.sh script, stop the NFS mounted Agent and restart it before continuing.

As mentioned above in NFS mounted Agent installation notes, using the Agent Deploy application to deploy an NFS mounted Agent will not run the root.sh script on the target host, regardless of whether the "Run root.sh" checkbox is checked or not. (Bug 4687187)

Workaround: the user will need to run this script manually on the target hosts after the deployment has been completed.

APPENDIX B

Help for sshConnectivity.sh Script

Note: ORACLE_HOME variable should be set to the OMS oracle home before using sshConnectivity.sh script.

Executing "sshConnectivity -help" will display the following help:

```
Usage: ./sshConnectivity.sh -user <user name> -hosts "<space separated hostlist>" | -hostfile <absolute
path of cluster configuration file>  [-asUser <user for which setup need to be done on the local
machine, eg, SYSTEM> [-asUserGrp <group, which the user specified in 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:

Local Platform = Unix :

./sshConnectivity.sh -user jgangwar -hosts stact24

./sshConnectivity.sh -user jgangwar -hosts hsunnab19 -remotePlatform 453

Local Platform = Windows :

 ./sshConnectivity.sh -user jgangwar -asUser SYSTEM -asUserGrp root -sshLocalDir "C:\cygwin\.ssh" -
localPlatformGrp win -hosts iwinrbb12

NOTE: Please specify the paths in double quotes.

This script is used to setup SSH user equivalence from the host on which it is run to the specified
remote hosts. After this script is run, the user can use  SSH to run 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 the user name on the remote host is specified as a command
line parameter to the script.

-user : User on remote hosts.

-hosts : Space separated remote hosts list.

-hostfile : The user can specify the host names either through the -hosts option or by specifying the
absolute path of a cluster configuration file. A sample host file contents are below:

   stacg30 stacg30int 10.1.0.0 stacg30v  -

   stacg34 stacg34int 10.1.0.1 stacg34v  -

The first column in each row of the host file will be used as the host name.

-usePassphrase : The user wants to set up passphrase to encrypt the private key on the local host.

-asUser : User, on local machine, for which ssh equivalence need to be set, eg, SYSTEM.

-asUserGrp : Group, which the user specified in asUser belongs to, eg: SYSTEM belongs to the group root.
```

-sshLocalDir : Directory where keys should be generated on the local machine for asUser. The path should be a windows style absolute path. Specify the path in double quotes. Example: -sshLocalDir "C:\cygwin\.ssh". The value "C:\cygwin" can be found from the registry "HKEY_LOCAL_MACHINE\Software\Cygnus Solutions\Cygwin\mounts v2\/".

-homeDir : Windows style full path of home directory of the current user. The value of /home can be found from the registry "HKEY_LOCAL_MACHINE\Software\Cygnus Solutions\Cygwin\mounts v2\/home". Specify the path in double quotes. Example: -homeDir "C:\Documents And Settings\spramani".

-shared : In case the user on the remote host has its home directory NFS mounted or shared across the remote hosts, this script should be used with -shared option.

It is possible for the user to determine whether a user's home directory is shared or non-shared. Let us say we want to determine that user user1's home directory is shared across hosts A, B and C.

Follow the following steps:

1. On host A, touch ~user1/checkSharedHome.tmp
2. On hosts B and C, ls -al ~user1/checkSharedHome.tmp
3. If the file is present on hosts B and C in ~user1 directory and

   is identical on all hosts A, B, C, it means that the user's home

   directory is shared.
4. On host A, rm -f ~user1/checkSharedHome.tmp

In case the user accidentally passes -shared option for non-shared homes or viceversa,SSH equivalence would only be set up for a subset of the hosts. The user would have to re-run the setup script with the correct option to rectify this problem.

-remotePlatform : It is necessary to specify this option if the remote platform is not same as the local platform. You need to specify the platform id of the remote platform. The platform ids of the supported platforms is present in the platforminfo.properties file.

-localPlatformGrp : It is necessary to specify this option if the local platform is windows: win

The default value of this option is: unix.

-advanced : Specifying the -advanced option on the command line would result in SSH user equivalence being setup among the remote hosts which means that SSH can be used to run commands on one remote host from the other remote host or copy files between the remote hosts without being prompted for passwords or confirmations.

-confirm: The script would remove write permissions on the remote hosts for the user home directory and ~/.ssh directory for "group" and "others". This is an SSH requirement. The user would be explicitly informed about this by the script and prompted to continue. In case the user presses no, the script would exit. In case the user does not want to be prompted, he can use -confirm option.

As a part of the setup, the script would use SSH to create files within ~/.ssh directory of the remote node and to setup the requisite permissions. The script also uses SCP tocopy the local host public key to the remote hosts so that the remote hosts trust the local host for SSH. At the time, the script performs these steps, SSH user equivalence has not been completely setup hence the script would prompt the user for the remote host password.

-verify : -verify option means that the user just wants to verify whether SSH has been set up. In this case, the script would not setup SSH but would only check whether SSH user equivalence has been setup from the local host to the remote hosts. The script would run the date command on each remote host using SSH. In case the user is prompted for a password or sees a warning message for a particular host, it means SSH user equivalence has not been setup correctly for that host. In case the -verify option is not specified, the script would setup SSH and then do the verification as well.

-exverify : In case the user speciies the -exverify option, an exhaustive verification for all hosts would be done. In that case, the following would be checked:

1. SSH equivalence from local host to all remote hosts.

2. SSH equivalanece from each remote host to itself and other remote hosts.

The -exverify option can be used in conjunction with the -verify option as well to do an exhaustive verification once the setup has been done.

Taking some examples: Let us say local host is Z, remote hosts are A,B and C. Local user is njerath. Remote users are racqa(non-shared), aime(shared).

```
$0 -user racqa -hosts "A B C" -advanced -exverify -confirm
```

Script would set up user equivalence from Z -> A, Z -> B, Z -> C, A -> A, A -> B, A -> C, B -> A, B -> B, B -> C, C -> A, C -> B, C -> C.

Since user has given -exverify option, all these scenario would be verified too.

Now the user runs : $0 -user racqa -hosts "A B C" -verify

Since -verify option is given, no SSH setup would be done, only verification of existing setup. Also, since -exverify or -advanced options are not given, script would only verify user equivalence from Z -> A, Z -> B, Z -> C

Now the user runs : $0 -user racqa -hosts "A B C" -verify -advanced

Since -verify option is given, no SSH setup would be done, only verification of existing setup. Also, since -advanced options is given, script would verify user equivalence from Z -> A, Z -> B, Z -> C, A-> A, A->B, A->C, A->D

Now the user runs:

```
$0 -user aime -hosts "A B C" -confirm -shared
```

Script would set up user equivalence between Z->A, Z->B, Z->C only since advanced option is not given.

All these scenarios would be verified too.

Sample Output of the sshConnectivity.sh script

```
Hosts are stabd22

user is supchoud

Remote host reachability check succeeded.

All hosts are reachable. Proceeding further...

firsthost stabd22

numhosts 1

The script will setup SSH connectivity from the host stabd22 to all

the remote hosts. After the script is executed, the user can use SSH to run

commands on the remote hosts or copy files between this host stabd22

and the remote hosts without being prompted for passwords or confirmations.

NOTE :

As part of the setup procedure, this script will use ssh and scp to copy

files between the local host and the remote hosts. You may be prompted for

the password during the execution of the script.

AS PER SSH REQUIREMENTS, THIS SCRIPT WILL SECURE THE USER HOME DIRECTORY

AND THE .ssh DIRECTORY BY REVOKING GROUP AND WORLD WRITE PRIVILEDGES TO THESE

directories.

Do you want to continue and let the script make the above mentioned changes (yes/no)?

The user chose yes

LIBRARY_LOC = /scratch/EM/P10.2/oms10g/oui/lib/linux

Loading file from jar: oracle/sysman/prov/remoteinterfaces/logger/logging_conf.xml

Enter the password:

LIBRARY_LOC = /scratch/EM/P10.2/oms10g/oui/lib/linux

The files containing the client public and private keys already exist on the local host. The current
private key may or may not have a passphrase associated with it. In case you remember the passphrase and
do not want to re-run ssh-keygen, type 'no'. If you type 'yes', the script will remove the old
private/public key files and, any previous SSH user setups would be reset.

Enter 'yes', 'no'

yes

User selected : yes
```

```
Generating new keys

[stabd22]

echo $HOME

Exit-status: 0

/home/supchoud

[stabd22]

/bin/mkdir -p /home/supchoud/.ssh

Exit-status: 0

[stabd22]

/bin/rm -f /home/supchoud/.ssh/identity.pubstabd22

Exit-status: 0

Copy localfile: /home/supchoud/.ssh/identity.pub to remotefile: /home/supchoud/.ssh/identity.pubstabd22

[stabd22]

/bin/cp -p /home/supchoud/.ssh/authorized_keys /home/supchoud/.ssh/authorized_keys.bak

Exit-status: 0

[stabd22]

/bin/cat /home/supchoud/.ssh/identity.pubstabd22 >> /home/supchoud/.ssh/authorized_keys

Exit-status: 0

[stabd22]

/bin/rm -f /home/supchoud/.ssh/identity.pubstabd22

Exit-status: 0

[stabd22]

/bin/chmod 644 /home/supchoud/.ssh/authorized_keys

Exit-status: 0

[stabd22]

/bin/chmod og-w /home/supchoud

Exit-status: 0

[stabd22]

/bin/chmod og-w /home/supchoud/.ssh

Exit-status: 0
```

```
[stabd22]

/bin/mv -f /home/supchoud/.ssh/config /home/supchoud/.ssh/config.bak

Exit-status: 0

Copy localfile: /home/supchoud/.ssh/config to remotefile: /home/supchoud/.ssh/config

[stabd22]

/bin/cat /etc/ssh/ssh_host_rsa_key.pub

Exit-status: 0

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxiTZAFJDxRckRx5kuwOkQ0nRYjQRTz4hpwUVkmuV/2+E+98XTPPXmLl6D44uFi3od7l3KSG5+q+5
+yAoo6gkCSEfqJr9jKKgwYk4uVGjfIcvGuoYq6VjvZDBzxB+YNCPzu9wmM69Q7SWVQfe3qrJrkM6Pher3dz9AKpmqcPZ2fE=

Hostname : stabd22

FullHostname : stabd22.us.oracle.com

IP address : 140.87.84.72

Local Platform:- Linux

------------------------------------------------------------------------

Verifying SSH setup

===================

The script will now run the date command on the remote nodes using ssh

to verify if ssh is setup correctly. IF THE SETUP IS CORRECTLY SETUP,

THERE SHOULD BE NO OUTPUT OTHER THAN THE DATE AND SSH SHOULD NOT ASK FOR

PASSWORDS. If you see any output other than date or are prompted for the

password, ssh is not setup correctly and you will need to resolve the

issue and set up ssh again.

The possible causes for failure could be:

1. The server settings in /etc/ssh/sshd_config file do not allow ssh

for user supchoud.

2. The server may have disabled public key based authentication.

3. The client public key on the server may be outdated.

4. ~supchoud or ~supchoud/.ssh on the remote host may not be owned by supchoud.

5. User may not have passed -shared option for shared remote users or

may be passing the -shared option for non-shared remote users.

6. If there is output in addition to the date, but no password is asked,
it may be a security alert shown as part of company policy. Append the

additional text to the <OMS HOME>/sysman/prov/resources/ignoreMessages.txt file.

------------------------------------------------------------------------

--stabd22:--

Running /usr/bin/ssh -x -l supchoud stabd22 date to verify SSH connectivity has been setup from local
host to stabd22.

IF YOU SEE ANY OTHER OUTPUT BESIDES THE OUTPUT OF THE DATE COMMAND OR IF YOU ARE PROMPTED FOR A PASSWORD
HERE, IT MEANS SSH SETUP HAS NOT BEEN SUCCESSFUL. Please note that being prompted for a passphrase may
be OK but being prompted for a password is ERROR.

Wed May 24 18:55:51 UTC 2006

------------------------------------------------------------------------

SSH verification complete.
```

APPENDIX C

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. Also remove the Cygnus Solutions Key (HKEY_LOCAL_MACHINE\SOFTWARE\Cygnus Solutions) from the Registry. To do it, go to a windows command prompt, type regedit. It will open the Registry Editor. Search for the Cygnus Solutions key under SOFTWARE, which is under HKEY_LOCAL_MACHINE). Right click on “Cygnus Solutions” entry in the Registry tree, select Delete and comfirm yes.

3. To install the full suite of Cygwin software, go to http://www.cygwin.com, and install Cygwin in your C:\cygwin directory.

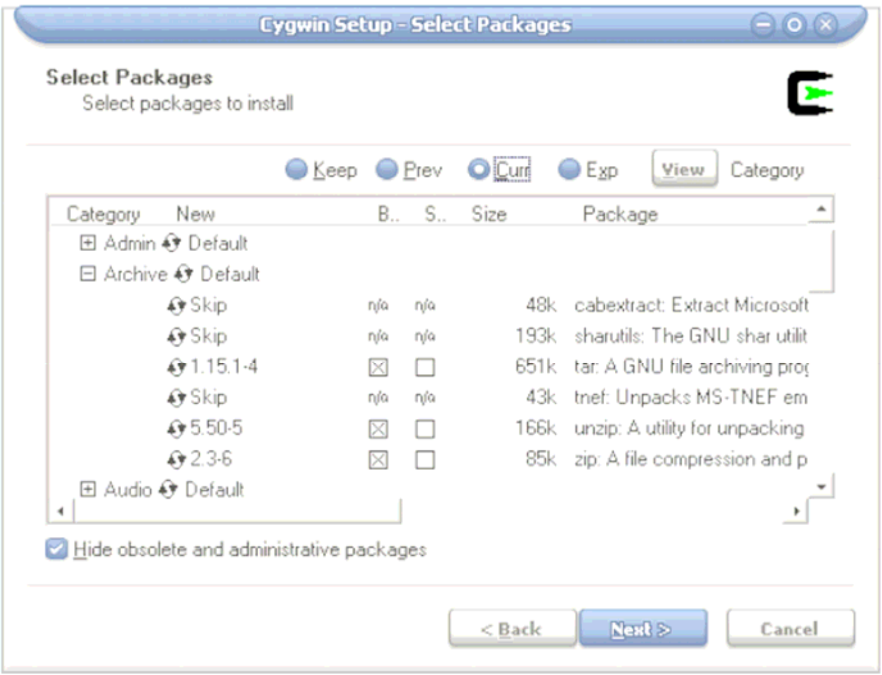
Note: If you are installing Cygwin into another directory than what has been previously mentioned, ensure you update the $OMS_HOME/sysman/prov/resources/ssPaths_msplats.properties file with the proper Cygwin binary values after installing Oracle Enterprise Manager Grid Control.

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 packages



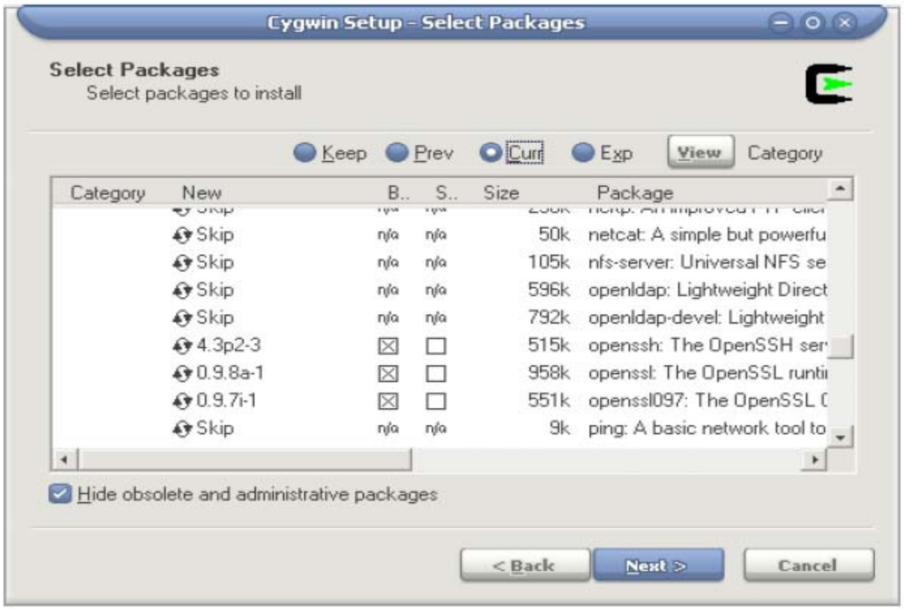
Select Packages
Select packages to install

Category	New	B..	S..	Size	Package
⊞ Admin	Default				
⊟ Archive	Default				
	Skip	n/a	n/a	48k	cabextract: Extract Microsoft
	Skip	n/a	n/a	193k	sharutils: The GNU shar utilit
	1.15.1-4	☒	□	651k	tar: A GNU file archiving proc
	Skip	n/a	n/a	43k	tnef: Unpacks MS-TNEF em
	5.50-5	☒	□	166k	unzip: A utility for unpacking
	2.3-6	☒	□	85k	zip: A file compression and p
⊞ Audio	Default				

☑ Hide obsolete and administrative packages

b. OpenSSH and dependencies (automatically selected if you choose OpenSSH) from the Net package.

Figure C-2: Net packages



Select Packages
Select packages to install

Category	New	B..	S..	Size	Package
	Skip	n/a	n/a	50k	netcat: A simple but powerfu
	Skip	n/a	n/a	105k	nfs-server: Universal NFS se
	Skip	n/a	n/a	596k	openldap: Lightweight Direct
	Skip	n/a	n/a	792k	openldap-devel: Lightweight
	4.3p2-3	☒	□	515k	openssh: The OpenSSH ser
	0.9.8a-1	☒	□	958k	openssl: The OpenSSL runti
	0.9.7i-1	☒	□	551k	openssl097: The OpenSSL (
	Skip	n/a	n/a	9k	ping: A basic network tool to

☑ Hide obsolete and administrative 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 **Appendix H,** "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 755 <username>/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 or OMS machine(that has the ssh client), 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.

Also, refer to Common problems in **Appendix H** in case of problems using SSHD or Cygwin

Setting Up SSH connectivity on Microsoft Windows Using sshUserSetupNT.sh

This example demonstrates the setting up of SSH using the sshUserSetupNT.sh. This script is only used for Enterprise Manager with version upto 10.2.0.1. From Enterprise Manager version 10.2.0.2 onwards sshConnectivity.sh script is used for same purpose.

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, go to the Registry Editor (use the command regedit in windows command prompt), find the HKEY_LOCAL_MACHINE\SOFTWARE\Cygnus Solutions\. If this has a /home subkey, modify the keyvalue to give it the value you want. Exit the registry. If there is no /home subkey then exit registry.

Open the /etc/password file, find (For more details on updating $HOME in /etcpasswd see "**Identifying the Correct Entry in the /etc/passwd File"** section below) the entry for the user logged in on the OMS box, modify the last but one column in this entry to give the value you have given for HKEY_LOCAL_MACHINE\SOFTWARE\Cygnus Solutions\/home. If you have not given any, give the value /home/<username>. Save and exit the /etc/passwd file. (See section "**Updating the $HOME (used for -homeDir option in sshUserSetupNT.sh) value in /etc/passwd"** below for more details).

Go to cygwin bash-prompt, execute the command ' mkdir –p /home/<username>'. Echo $HOME to check the home dir value.

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 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. . To Change the value of $HOME, follow instructions in step 2 mentioned above to update registry(if needed) and to update /etc/passwd.

If $HOME does not have any value (is empty), then you must update the /etc/passwd file as mentioned above in step 2.

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 $HOME (used for -homeDir option in sshConnectivity.sh or sshUserSetupNT.sh) value in /etc/passwd

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 (this is last but one field). You can 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, you can modify this to:

/cygdrive/c/cygwin/pjohn

Now, save the password file and reenter the BASH shell. Whatever value you specify for this home directory field will be picked up by cygwin for $HOME.

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"). This value will be used as a value for –homeDir option while running sshConnectivity.sh or sshUserSetupNT.sh script.

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.

APPENDIX D

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:

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'
```

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 G**, for more information.

APPENDIX E

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 theValidatepaths script which can be found at $OMS_HOME/sysman/prov/resources/scripts directory, 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.

sPaths/paths/userPaths/ssPaths properties contain path to various binaries, commands and parameters that are used both on the OMS side and on the remote nodes by the Agent Deploy application.

Following are the list of commands and arguments that are run on both the OMS and the remote hosts on which the agent needs to be installed. The starred(*) ones are run only on OMS host.

RSH_PATH *

SSH_PATH *

RCP_PATH *

SCP_PATH *

SSH_ARGS *

SCP_ARGS *

RCP_ARGS *

PING_PATH

SH_PATH

SHELL_PATH

SHELL_ARGS

TAR_PATH

TAR_EXTRACT_ARGS

TAR_MTIME_ARGS

UNZIP_PATH*

UNZIP_ARGS *

MKDIR

Rest of the commands in sPaths/paths/userPaths/ssPaths properties are run only on the remote hosts.

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.

APPENDIX F

Agent deploy Application pre-reqs and resolution in case of pre-req errors

Prerequisite Check done on the Local host (OMS host), Errors encountered and their Resolutions

Prerequisite Check	**Reason for Failure**	**User Action**[Foot 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. 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.

[Footnote 1] where there are multiple user actions listed, you can choose to perform the action that is most appropriate.

Prerequisite Check done on the Remote Hosts, Errors encountered and their Resolutions

Prerequisite Check	**Reason for Failure**	**User Action**[Foot 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. See **Appendix I** for package requirements.
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).
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 are registered with the central inventory.	Uninstall the existing agent and retry the prerequisite checks. Continue with the installation bacause the failure message is only a warning (though not recommended).
Write	The installation base directory is	Include write permissions on the failed nodes by executing the

Prerequisite Check	**Reason for Failure**	**User Action**[Foot 1]
Permissions for Base Directory	not writable.	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: Log in to the local host (machine running the Oracle Management Service). Change the directory to: <HOME>/sysman/prov/agentpush/resources/fixup 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.
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).

Prerequisite Check	**Reason for Failure**	**User Action**[Foot 1]
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).

[Footnote 1] where there are multiple user actions listed, you can choose to perform the action that is most appropriate.

APPENDIX G

Additional Parameters for the Agent Deploy Application

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.

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.

Additional Parameters Supported by agentDownload Script

Table 1 lists the possible parameters that you can specify if you select the default (Management Service) location.

Table 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/
-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.

Parameters	Description
	# 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

Additional Parameters Supported by Oracle Universal Installer

Table 2 lists the possible parameters that you can specify if you select an alternative software source (nondefault) location:

Table 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,

Parameter	Description
	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.

APPENDIX H

TROUBLESHOOTING INFORMATION

Location of Installation Logs

The following prerequisite check and installation logs are available at these locations:

1) <OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/prereqs

Connectivity logs: The following logs are available at

$OMS_HOME/sysman/prov/agentpush/<time-stamp>/prereqs/local:

prereq<time_stamp>.log

prereq<time_stamp>.out

prereq<time_stamp>.err

Prereq Logs: The following prerequisite logs for <node 1> will be available at $OMS_HOME/sysman/prov/agentpush/<time-stamp>/prereqs/<node1>:

prereq<time_stamp>.log

prereq<time_stamp>.out

prereq<time_stamp>.err

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.

2) <OMS_HOME>/sysman/prov/agentpush/logs/

EMAgentPush<TIMESTAMP>.log: Agent Deploy application logs.

remoteInterfaces<TIMESTAMP>.log: Logs of the remote interfaces layer.

3) <OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/

install.log/.err: Log or error of the new agent installation or new cluster agent installation.

upgrade.log/.err : Log or error of the upgrade operation using Agent Deploy.

nfsinstall.log/err: Log or error of the agent installation using the Shared Agent Home option in Agent Deploy.

clusterUpgrade.log/err: Log or error of the cluster upgrade operation using Agent Deploy.

sharedClusterUpgradeConfig.log/err: Log or error of the config operation in case of upgrade on a shared cluster.

config.log/err: Log or error of the configuration of shared cluster in case of an agent installation on a shared cluster.

preinstallscript.log/.err: Log/error of the running of preinstallation script, if specified.

rootsh.log/.err: Log/error of running of root.sh.

postinstallscript.log/.err: Log or error of running of postinstallation script, if specified.

installActions<timestamp>.log, oraInstall<timestamp>.err/.out : Logs of Oracle Universal Installer.

agentStatus.log : Status of agent after running emctl status agent from the agent home.

Common problems that are encountered

1) 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.

2) 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.

3) 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\
```

4) 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.

5) 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:

a) The 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

b) The Cygwin installation was not successful.

If restarting the SSHD service does not resolve the error, then you must reinstall Cygwin. To do this:

Remove the Keys and Subkeys under Cygnus Solutions using regedit.

Remove the Cygwin directory (C:\cygwin), and all Cygwin icons.

Remove the .ssh directory from the Documents and Settings folder of the domain user.

Reinstall Cygwin.

For detailed instructions on Cygwin installation, see **Appendix C**, "Setting Up SSH Server (SSHD) on Microsoft Windows"

Execute the following command to start SSH daemon:

cygrunsrv -start sshd

6) 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:

Stop the SSHD service (cygrunsrv -stop sshd).

Go to the etc directory (cd /etc).

Change the SSH file owner to the appropriate system (chown <SYSTEM> ssh*).

Go to the Cygwin command prompt and execute the following:

chmod 644 /etc/ssh*

chmod 755 /var/empty

chmod 644 /var/log/sshd.log

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.

Finally, start the SSHD service (from /usr/bin/sshd), or by executing cygrunsrv -start sshd.

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.

7) 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:

Right-click on My Computer and select Manage.

In the Computer Management dialog box that appears, click Services under Services and Applications.

In the rightpane, select the Cygwin SSHD service, right-click and go to Properties.

In the Cygwin SSHD Properties window that appears, select This Account.

Now, specify the appropriate domain name and user (in the form of domain\user, for example, FOO-US\pjohn).

Specify the password for this user, and click Apply.

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
```

Start SSHD by executing the following command:

```
/usr/sbin/sshd
```

8) Configuration Issues - Agent Configuration Assistants Fail During Enterprise Manager Installation

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..."
```

APPENDIX I

Platform-Specific Package Requirements for Agent Installation

===

***Note: The Target Monitor Check, Host name Check and Oracle Home Compatibility check are the same for all platforms.**

Target Monitor Check: The agent won't be able to monitor the targets, which are installed by different users.

Host Name Check: The host name in /etc/rhosts file where agent is going to installed should not have ip-address or localhost.localdomainname.

Oracle Home Compatibility Check: Products oracle.rsf.oracore_rsf, oracle.java.j2ee.container should not be present in OracleHome before agent installation.

Packages required only for interactive install are marked in blue color

Windows Specific check

Upgrade Check: If it's an agent upgrade install on cluster, then user has to upgrade each node separately.

===

Platform	Architeccture Value	Packages/Patches	Disk Space for Install	* Target Monitor check	* Host Name Check	*Oracle Home Compatibility Check	*Upgrade Check
SOLARIS							
Solaris 5.8	Sparc	SUNWarc, SUNWbtool, SUNWhea, SUNWlibm, SUNWlibms, SUNWsprot, SUNWsprox, SUNWtoo, SUNWi1of, SUNWxwfnt.	0.85 GB	Done	Done	Done	**N/A**
Solaris 5.9	Sparc	SUNWlibm, SUNWlibms, SUNWsprot, SUNWsprox, SUNWtoo, SUNWi1of, SUNWxwfnt	0.85 GB	Done	Done	Done	**N/A**
Solaris 5.10	Sparc	SUNWbtool	0.85 GB	Done	Done	Done	**N/A**
HP-UX							
HP-UX 11.11	PA_RISC2.0	**X11MotifDevKit version 0.0, X11MotifDevKit.MOTIF21-PRG version 0.0**	1.5 GB	Done	Done	Done	**N/A**
HP-UX 11.23	PA_RISC2.0	BUNDLE11i version B.11.23.0409.3	1.5 GB	Done	Done	Done	**N/A**
HP Itanium							
HP Itanium 11.23	IA64N	No packages are checked. Packages are picked from DB shiphomes, which do not have any package check for this.	2GB	Done	Done	Done	**N/A**
AIX							
AIX 5200	N/A	bos.perf.proctools version 0.0	1.5 GB	Done	Done	Done	**N/A**
AIX 5300	N/A	bos.perf.proctools version 0.0	1.5 GB	Done	Done	Done	**N/A**

Platform	Architeccture Value	Packages/Patches	Disk Space for Install	* Target Monitor check	* Host Name Check	*Oracle Home Compatibility Check	*Upgrade Check
LINUX ITANIUM							
Redhat 3	ia64	GLIBC>=2.3.2-95.27,Make version 3.79, binutils version 2.14, Libaio version 0.3.96	0.75 GB	Done	Done	Done	**N/A**
Redhat 4	ia64	GLIBC>=2.3.2-95.27Make version 3.79, binutils version 2.14, Libaio version 0.3.96, gcc version 3.2	0.75 GB	Done	Done	Done	**N/A**
Suse 9	ia64	GLIBC>=2.3.3-98.28Make version 3.80, binutils version 2.14, Libaio version 0.3.102, gcc version 3.3	0.75 GB	Done	Done	Done	**N/A**
LINUX (32-bit)							
Redhat 3	N/A	GLIBC value - 2.3.2-95.3, make version 3.79, binutils version 2.11.90.0.8-12, gcc version 3.2.3, setarch version 1.3, pdksh version 5.2, **openmotif21 version 2.1.30**, sysstat version 4.0.7, gnome-libs version 1.4.1.2.90-34.1, libstdc++ version 3.2.3, compat-libstdc++-devel version 7.3-2.96.122, compat-glibc-7.x version 2.2.4.32.5, compat-gcc version 7.3-2.96, compat-gcc-c++ version 7.3-2.96, compat-libstdc++ version 7.3-2.96	0.45 GB	Done	Done	Done	**N/A**
Redhat 4	N/A	GLIBC value - 2.2.5, make version 3.79, binutils version 2.11.90.0.8-12, gcc version 2.96, **openmotif version 2.1.30-11**, gcc_old version - 2.95, pdksh version 5.2, sysstat version 4.0.3, **openmotif-2.1.30MLI4 version 0.0,** libstdc++ version 3.2.2-38	0.45 GB	Done	Done	Done	**N/A**
Suse 8	N/A	GLIBC Value - 2.2.5, make version 3.79, binutils version 2.11.90.0.8-12, gcc version 2.96, **openmotif version 2.1.30-11**, gcc_old version 2.95, pdksh version 5.2, sysstat version 4.0.3, **openmotif-2.1.30MLI4 version 0.0,** libstdc++ version 3.2.2-38	0.45 GB	Done	Done	Done	**N/A**
Suse 9	N/A	**No checks performed**	0.45 GB	Done	Done	Done	**N/A**
Windows (32-bit)							
NT	N/A	Service Pack 6a for Windows_NT only	0.45 GB	Done	Done	Done	Done
2000	N/A	**No checks performed**	0.45 GB	Done	Done	Done	Done
XP	N/A	**No checks performed**	0.45 GB	Done	Done	Done	Done

APPENDIX J

Patch for cross platform agent push in Enterprise Manager 10.2.0.2

If you are using Enterprise Manager version 10.2.0.2 then patch number 5455350 needs to be applied to your 10.2.0.2 OMS. The content of the readme for patch 5455350 is mentioned below.

README for patch 5455350

This patch provides enhanced agentpush functionality, when applied over 10.2.0.2 OMS.

Important: You must use opatch version 10.2.0.1.2 or later. It can be downloaded from Metalink (http://metalink.oracle.com) with Patch#4898608. Backup <OMS_HOME>/OPatch directory and unzip the downloaded zip file in <OMS_HOME>. It wil create new OPatch directory. Run "<OMS_HOME>/OPatch/opatch version" and verify that it shows 10.2.0.1.2 version.

Make sure ORACLE_HOME environment variable is set to <OMS_HOME>.

Run "<OMS_HOME>/OPatch/opatch apply <TMP_LOCATION>/5455350" to apply this patch, where <TMP_LOCATION> is the directory where this patch is unzipped.

BUG fixes in this patch: 5303864,5353934

Bug Fix: 5303864

This fix is for supporting agentpush functionality across platforms.

Requirements in the agent download kit for supporting agentpush across platforms:

1. The platforminfo.properties file should be present in

<OMS_HOME>/sysman/agent_download/<version>/<platform>/agentdeploy/. This file should contain the platform id and the list of path property files for the <platform> as key value pair. The platform id should be the same as the

one specified in the file <OMS_HOME>/sysman/agent_download/<version>/<platform>/agent/stage/shiphomeproperties.xml (the value of tag ARU_ID). Also add a entry for platform id 0(zero). In case the platform id specified here is not recognized, the files specified for 0(zero) will be used.

Example: For Solaris,

453=Paths.properties, sPaths.properties, ssPaths_sol.properties, userPaths.properties

0=Paths.properties, sPaths.properties, ssPaths_sol.properties, userPaths.properties

2. The path property files (sPaths.properties etc) specified in platforminfo.properties above should be present in

<OMS_HOME>/sysman/agent_download/<version>/<platform>/agentdeploy/.

(For sample property files refer to <OMS_HOME>/sysman/prov/resources). If these files are not specified here, the ones from <OMS_HOME>/sysman/prov/resources will be refered to by the agentpush application.

3. The display name for the platforms in agentpush pages is loaded from

<OMS_HOME>/sysman/agent_download/<version>/<platform>/agent/stage/shiphomeproperties.xml

(the value of tag ARU_ID_DESCRIPTION). In case the platform staged by you in <OMS_HOME>/sysman/agent_download/<version>/ is not displayed in agentpush pages, please check this file.

Note: By agent download kit, we mean the agent source software for a platform. This is staged in

<OMS_HOME>/sysman/agent_download/10.2.0.2.0/ directory, by default for the current platform.

Bug Fix: 5353934

This fix is required for allowing the install through agentpush even when timezone environment variable is not set on the remote host(s).

1. When the timezone environment variable ($TZ) is set on the remote hosts, and it is not passed by the user in additional parameters of agentpush, the TZ value set in the SSH environment of the remote hosts will be used for the agent.

2. When the timezone environment variable ($TZ) is not set on the remote hosts, and it is not passed by the user in additional parameters of agentpush, agent will calculate a timezone and set it. In this case, prerequisite checks for the same will not be performed, and hence the user will not be prompted for any error/warning.

3. When the timezone environment variable ($TZ) is not set on the remote hosts, and a timezone is passed by the user in additional parameters of agentpush (example -z PST8PDT), this value will be used.

4. When the timezone environment variable ($TZ) is set on the remote hosts, and also a timezone is passed by the user in additional parameters of agentpush, the TZ value set in the SSH environment of the remote hosts will be used for the agent. Note that if the TZ value passed, and that in the environment are different, this message will be logged in the logs, but the TZ value in the environment will be used.

Patch for cross platform agent push in Enterprise Manager 10.2.0.1

If you are using Enterprise Manager version 10.2.0.2 then patch number 4645135 needs to be applied to your 10.2.0.1 OMS. The content of the readme for patch 4645135 is mentioned below.

README for patch 4645135

This patch provides enhanced agentpush functionality, when applied over 10.2.0.1 OMS.

Important: You must use opatch version 10.2.0.1.2 or later. It can be downloaded from Metalink (http://metalink.oracle.com) with Patch#4898608. Backup <OMS_HOME>/OPatch directory and unzip the downloaded zip file in <OMS_HOME>. It wil create new OPatch directory. Run "<OMS_HOME>/OPatch/opatch version" and verify that it shows 10.2.0.1.2 version.

Make sure ORACLE_HOME environment variable is set to <OMS_HOME>.

Run "<OMS_HOME>/OPatch/opatch apply <TMP_LOCATION>/4645135" to apply this patch, where <TMP_LOCATION> is the directory where this patch is unzipped.

Management Agent Deployment Best Practices
November 2005
Author: Rajat Nigam and Joshua Solomin

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Copyright © 2005, Oracle. All rights reserved.
This document is provided for information purposes only and the
contents hereof are subject to change without notice.
This document is not warranted to be error-free, nor subject to any
other warranties or conditions, whether expressed orally or implied
in law, including implied warranties and conditions of merchantability
or fitness for a particular purpose. We specifically disclaim any
liability with respect to this document and no contractual obligations
are formed either directly or indirectly by this document. This document
may not be reproduced or transmitted in any form or by any means,
electronic or mechanical, for any purpose, without our prior written permission.
Oracle, JD Edwards, and PeopleSoft are registered trademarks of
Oracle Corporation and/or its affiliates. Other names may be trademarks
of their respective owners.