Oracle® Enterprise Manager

System Monitoring Plug-in Installation Guide for VMware ESX Server

Release 5 (1.0.3.0.0) to Release 8 (1.1.3.2.0)

E13339-05

November 2009

This document is the installation guide for the System Monitoring Plug-in for VMware ESX Server. You can find the following information in this document:

- A brief description of the VMware ESX Server
- VMware ESX Server versions and Enterprise Manager versions that the Plug-in supports
- Prerequisites for installing the Plug-in
- Step-by-step instructions to download, install, verify, and validate the Plug-in

> **Note:** This Installation Guide can be used for the following VMware ESX Server Plug-in releases:
>
> - Release 5 (1.0.3.0.0)
> - Release 6 (1.1.3.0.0)
> - Release 7 (1.1.3.1.0)
> - Release 8 (1.1.3.2.0)

Description

The System Monitoring Plug-in for VMware ESX Server extends Oracle Enterprise Manager Grid Control to add support for managing the VMware ESX Server. By deploying the plug-in in your Grid Control environment, you gain the following management features:

- Monitor the VMware ESX Server.
- Gather configuration data and track configuration changes for the VMware ESX Server.
- Raise alerts and violations based on thresholds set on monitored metrics and configuration data.
- Provide rich out-of-box reports based on the gathered data.
- Support monitoring by a remote Agent. For remote monitoring, the agent need not be on the same host as the VMware ESX Server.

Versions Supported

Release 8 of this plug-in supports the following versions of products:

- Enterprise Manager Grid Control 10*g* Release 3 or higher Management Service and Agent
- The following versions of VMWare:
  - VMware ESX Server 3.0.0, 3.0.1, 3.0.2, 3.5.0
  - VMware ESXi 3.5.0

Prerequisites

You must ensure that the following prerequisites are fulfilled before you use the plug-in:

- Oracle Enterprise Manager Grid Control 10g Release 3 or higher Management Service and Agent
- VMware ESX Server can be configured to accept either HTTPS or HTTP web service calls (which the Agent makes). The default set up of the VMware ESX Server is HTTPS.

  In VMware's "Developer's Setup Guide - VMware Infrasturcture SDK 2.5", it is stated that "VMware recommends that secure HTTP (HTTPS; the default configuration) be used for production deployments. Modifying the server configuration to support HTTP access to the VI API is recommended for test or development only, not for production deployments". If HTTPS is used, a keystore must be created to hold the certificate that ships with each VMware ESX Server.

  In VMware ESXi, access to the console is no longer available. In order to get or update files on that server, it is now necessary to use either `https://<ESXi_machine>/host` or the VMware VI Remote CLI (that is, `vifs.pl`). In either case, some files are no longer accessed through their real file names, but instead are accessed through symbolic names. For example, on VMware ESXi, the `rui.crt` file is now accessed with the symbolic name `ssl_cert`. The instructions below still refer to `rui.crt`, but for VMware ESXi `ssl_cert` would be used in its place.

  This certificate is specific for each installation of an ESX Server. So, if an Agent is monitoring three ESX Servers, the Agent must have read access to the keystore file(s) that hold the certificates for those three installations of the ESX Server. There are two ways to make the certificates available to the agent through keystore files:

  1. Create a separate keystore file for each ESX Server's certificate.
  2. Create a single keystore file that contains all the certificates for all the ESX Servers that will be monitored by the Agent.

  The keystore file is created by using the Java SDK tool keytool. It can be run in an iterative fashion to add more than one certificate to the same keystore file. For example, if you take the first approach, you can use the following command. Assume that you are in a directory where the rui.crt certificate file exists for the ESX Server:

  ```
  > keytool -import -file rui.crt -alias my_esx_svr -keystore single_
cert.keystore
  ```

  Then:

  ```
  > keytool -list -keystore single_cert.keystore
  ```

would show (partial output shown below):

```
Your keystore contains 1 entry
     my_esx_svr, Aug 17, 2007, trustedCertEntry,
   Certificate fingerprint (MD5): FF:53:87:A0.................
```

For the second approach, each rui.crt file was renamed to have the ESX Server name for clarity:

```
   > keytool -import -file svr1_rui.crt -alias my_esx_svr1 -keystore
multi_cert.keystore
   > keytool -import -file svr2_rui.crt -alias my_esx_svr2 -keystore
multi_cert.keystore
```

Then:

```
> keytool -list -keystore multi_cert.keystore
```

would show (partial output shown below):

```
   Your keystore contains 2 entries
     my_esx_svr1, Aug 17, 2007, trustedCertEntry,
   Certificate fingerprint (MD5): B3:29:56:0C.................
   my_esx_svr2, Aug 17, 2007, trustedCertEntry,
   Certificate fingerprint (MD5): 3F:22:89:B1.................
```

If HTTP is used, then the VMware ESX Server must be reconfigured with the file:

```
/etc/vmware/hostd/config.xml (for versions before 3.5.0)
/etc/vmware/hostd/proxy.xml (for version 3.5.0 and above)
```

For more details, refer to the sections "Modifying ESX Server 3.5 or VirtualCenter 2.5 Configurations" and "Modifying ESX Server 3.0.x and VirtualCenter 2.0.x Configuration" of VMware's "Developer's Setup Guide - VMware Infrastructure SDK 2.5".

- Preferred credentials are set on all Agents where you want to deploy the plug-in. Unless you assign the correct privileges, the deployment will fail.
- In order for the Response metric to correctly report the status of the ESX Server, IP-level connectivity must exist between the host where the Agent is running (where this plug-in is installed) and the host where ESX Server is running.

  The Response metric uses the `ping` command to check the status of the ESX Server. Make sure that you are able to ping the ESX Server host from the Agent host. If you are unable to ping the ESX Server host, then check with your system administrator to get the IP connectivity set up between the two hosts.

  The `ifconfig` command allows the operating system to set up network interfaces and enables you to view information about the configured network interfaces. The IP connectivity can also be configured on the ESX Server host using the `net.ipv4.icmp_echo_ignore_all` setting in the `/etc/sysctl.conf` file. Setting the value to 1 causes all incoming ping packets to be dropped. Hence, the value should be set to 0 for the Repsonse metric to work correctly.

Deploying the Plug-in

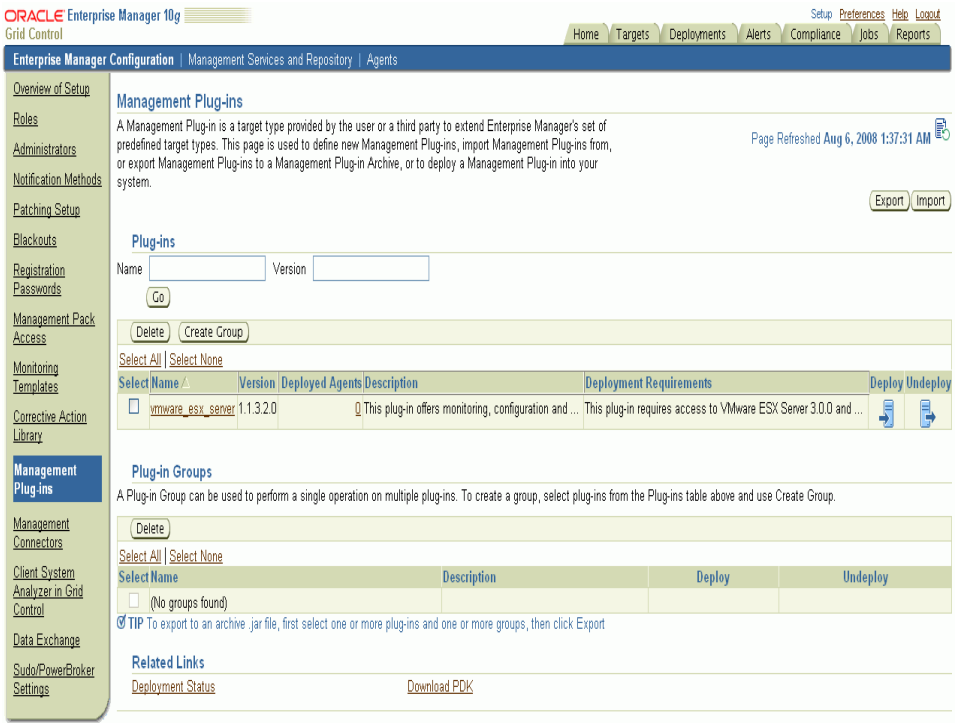
After you ensure that the prerequisites are met, follow these steps to deploy the plug-in:

1. Download the VMWare ESX Server Plug-in archive to your desktop or computer on which the browser is launched. You can download the archive from the Oracle Technology Network (OTN).
2. Log on to Enterprise Manager Grid Control as a Super Administrator.
3. Click the **Setup** link in the upper right corner of the Grid Control Home page, then click the **Management Plug-ins** link on the left side of the Setup page.
4. Click **Import**.
5. Click **Browse** and select the plug-in archive.
6. Click **List Archive**.
7. Select the plug-in and click **OK**.
8. Verify that you have set preferred credentials on all Agents where you want to deploy the plug-in.
9. In the Management Plug-ins page, click the icon in the **Deploy** column for the VMWare ESX Server plug-in. The Deploy Management Plug-in wizard appears.
10. Click **Add Agents**, then select one or more Agents for which you want to deploy the plug-in. The wizard reappears and displays the Agent or Agents selected.
11. Click **Next**, then click **Finish**.

    If you see an error message stating that the preferred credential is not set up, go to the Preferences page and add the preferred credentials for the Agent target type.
12. If you are using HTTPS web service calls, you must copy the keystore file(s) to the location that you specify when adding target instances (this step must be completed before adding targets to these Agents).

    If there are no errors, you can see the following screen:

Figure 1 Successful Deployment



Adding Instances for Monitoring

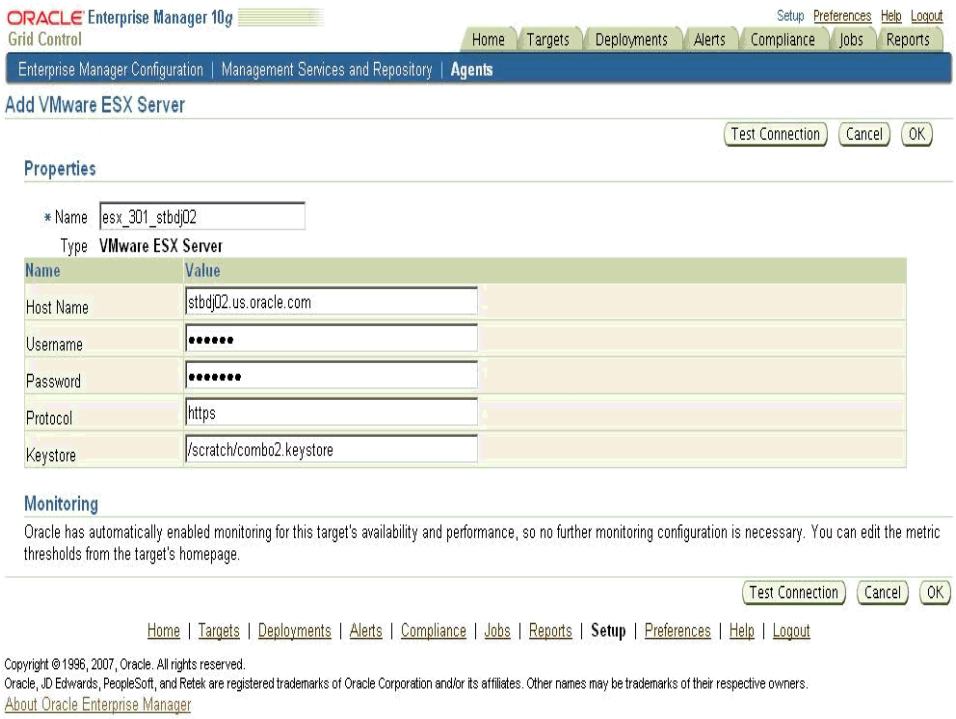
After successfully deploying the plug-in, follow these steps to add the plug-in target to Grid Control for central monitoring and management:

1. From the Agent home page where the plug-in was deployed, select the VMware ESX Server target type from the **Add** drop-down list, then click Go. The Add VMware ESX Server page appears.
2. Provide the following information for the properties:
   - **Name** — Name of the VMware ESX Server being monitored
   - **Host Name** — Fully qualified host name, including domain, of the ESX Server
   - **Username** — Name of the user with proper privileges for enabling the plug-in to access data through the embedded Web Service in the VMWare ESX Server
   - **Password** — Password for the specified Username
   - **Protocol** — Either HTTP or HTTPS can be specified. If HTTPS is specified, you must specify the Keystore parameter (with HTTP set, the Keystore parameter is left blank). However, due to an issue with the ESX Server, Oracle recommends using the HTTP protocol at this time. Refer to the "Limitations" section for more details.
   - **Keystore** — Full path name and file name to the keystore file that contains the certificate for the VMware ESX Server. The agent must have access to this keystore file.

3. Click **Test Connection** to make sure the parameters you entered are correct.
4. Reenter the encrypted parameters from step 2 if the connection test was successful, then click **OK**. This step is not required if the Enterprise Manager version is 10.2.0.4 or above.
5. To run EM jobs that stop, start and suspend VMs or set or exit ESX Server into/from maintenance mode, credentials must be supplied to the job. This can be accomplished either ahead of time by specifying the preferred credentials (both Agent Host Username/Password and Web Service Username/Password) in the Preferences section of EM or by specifying the same credentials when the job is actually submitted.

Note: After you deploy and configure the plug-in to monitor one or more targets in the environment, you can customize the monitoring settings of the plug-in. This alters the collection intervals and threshold settings of the metrics to meet the particular needs of your environment. If you decide to disable one or more metric collections, this could impact the reports that the metric is part of.

Figure 2 Add VMWare ESX Server Page

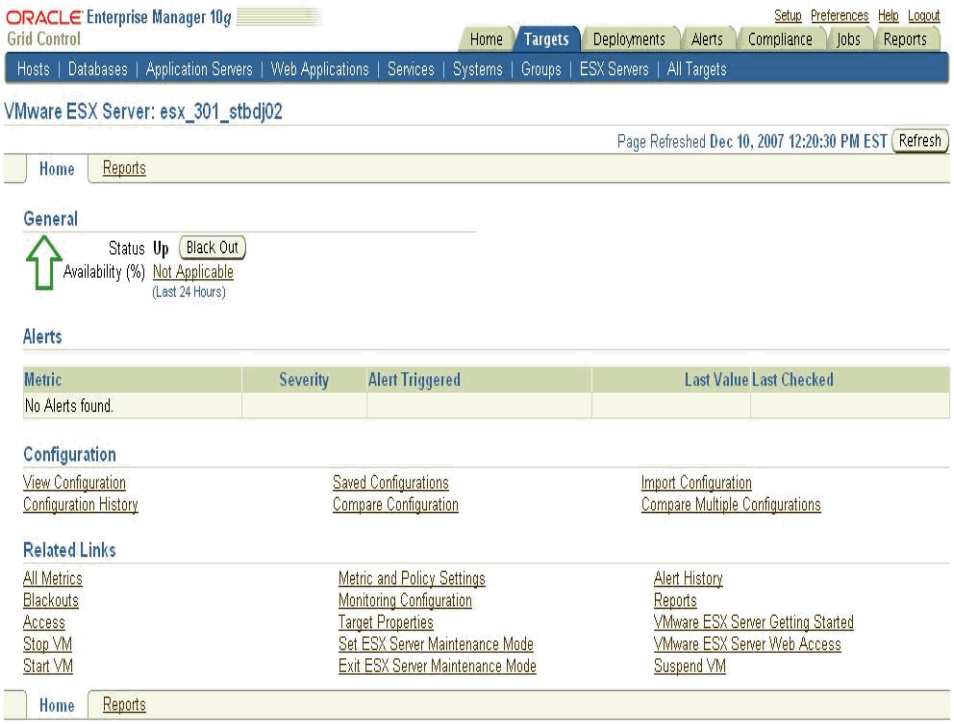


Verifying and Validating the Plug-in

After waiting a few minutes for the plug-in to start collecting data, deploy the following steps to verify and validate that Enterprise Manager is properly monitoring the plug-in target:

1. Click the VMware ESX Server target link from the Agent home page Monitored Targets table. The VMware ESX Server home page appears.

Figure 3 VMware ESX Server Home Page



2. Verify that no metric collection errors are reported in the Metrics table.
3. Ensure that reports can be seen by selecting the Reports property page.
4. Ensure that configuration data can be seen by clicking the **View Configuration** link in the Configuration section. If configuration data does not appear immediately, click **Refresh** in the View Configuration page.

Undeploying the Plug-in

Follow these steps to undeploy the plug-in from an Agent:

1. Log in to Enterprise Manager Grid Control as a Super Administrator.
2. Select the **Targets** tab, then the **All Targets** subtab.
3. Select the VMware ESX Server Plug-in target and click **Remove**. You must do this step for all target instances of the plug-in.
4. Make sure that the preferred credentials are set on the Agents where the plug-in is deployed.
5. Click the **Setup** link in the upper right corner of the All Targets page, then click the Management Plug-ins link on the left side of the Setup page. The Management Plug-ins page appears.
6. Click the icon in the **Undeploy** column for the VMware ESX Server plug-in. The Undeploy Management Plug-in page appears.
7. Check all the Agents that are currently deployed with the VMware ESX Server plug-in and click **OK**.

You must undeploy the plug-in from every Agent in the system to completely remove it from the enterprise.

8. Select the VMware ESX Server Plug-in on the Management Plug-ins page and click **Delete**.

Limitations

1. The ESX Server VM Summary report contains a table of the VMs that have been created on a particular ESX Server. The VM column of that table contains the names of the VMs represented as links. If you click the link for a particular VM and that VM has an EM agent installed on it, the Host homepage for that VM as a host is displayed. If an agent in not installed on that VM, the homepage is still displayed, but the error message 'An error has occurred! Error finding target <VM name> from the repository. The target does not exist or you may not have the access to the target.' is displayed. This is the expected behavior since the VM is not being monitored as a host target instance if it does not have an agent installed on it.

   This functionality is available in 10.2.0.4. In 10.2.0.3, the links do not appear unless an EM Grid Control patch is provided for this generic report-related functionality. In addition, in 10.2.0.3, columns named Domain and Host Homepage URL appear at the end of the VM Summary table. They do not appear in 10.2.0.4 or the patch.

2. It is possible to rename a VM while it is on a particular ESX Server. When a VM is renamed, its metric history and other EM repository data will not be accessible as the key to the data is the VM name.

3. This plug-in supports both HTTP and HTTPS-based connections to the embedded Web Service in the VMware ESX Server. However, due to an issue found in ESX Server version 3.0.2 (and earlier), configuring an EM ESX Server target instance with a protocol setting of HTTPS will cause SSL Handshake errors to eventually appear in `/etc/vmware/log/hostd.log` on the ESX Server while the EM Agent is collecting metrics or running jobs. When this occurs, the EM Agent is no longer able to communicate with the Web Service. The same holds true for the VMware-supplied Virtual Infrastructure Client tool.

   For details on the ESX Server issue, refer to note 455661.1 available at: `http://metalink.oracle.com/`. To locate document 455661.1:

   1. Click **Advanced** at the top of the OracleMetaLink page.
   2. Enter 455661.1 in the **Document ID** field and click **Submit**.

   Note: This is no longer an issue with ESX Server version 3.0.3 (and later).

   ---

4. The VMware ESX Server target type should not be monitored by an agent that is remote from the ESX Server. Though it is possible to install an EM agent on a virtual machine running on an ESX Server and have that agent monitor that ESX Server as a target, this should not be done. The reason is that some of the administrative functionalities of the VMware ESX Server plug-in may conflict with the running of that agent. For example, you can run a job to stop the VM that the agent is running on. This can cause

problems because the VM must communicate with the agent to stop the EM job. However, the agent is shut down on stopping the VM and the agent and OMS relationship is put into an indeterminate state.

Job Error Codes

Table 1 provides details of the job error codes that may be encountered if there are errors while running the jobs.

Table 1 Job Error Codes and Description

Error Codes	Description
1	ESX Web Service username and/or password not supplied. Recheck the ESX Server target instance configuration.
2	ESX remote exception occurred in setting up the ESX Server task. Ensure that the ESX Server is up and retry.
3	ESX unknown host exception occurred in setting up the ESX Server task. Recheck the ESX Server target instance configuration.
4	ESX Server is in a state that is not valid for this operation. Check state of the ESX Server and retry when appropriate.
5	The request was cancelled. Retry when appropriate.
6	ESX runtime exception occurred in running the ESX Server task. Ensure that the ESX Server is up or that the ESX Server user has the proper privileges and/or roles, then retry.
7	Time out occurred in running the ESX Server task. Ensure that the ESX Server is up and retry.
8	Remote exception occurred in running the ESX Server task. Retry.
9	Invalid number of arguments passed to EM job. Recheck the ESX Server target instance configuration.
100	Invalid ESX Web Service username and/or password. Recheck the ESX Server target instance configuration.
101	ESX runtime exception occurred when connecting to the ESX Web Service. Ensure that the ESX Server is up and retry.
102	ESX remote exception occurred when connecting to the ESX Web Service. Ensure that the ESX Server is up and retry.
103	Exception occurred when connecting to the ESX Web Service. Recheck the ESX Server target instance configuration and ensure that the ESX Server is up and retry.
104	ESX Server task did not complete successfully. Check ESX Server log files and/or task status through VMware-supplied tools.
105	General exception occurred during ESX Server task execution. Check ESX Server log files and/or task status through VMware-supplied tools.
106	Permission exception occurred when connecting to the ESX Web Service. Check that the username specified in the ESX Server target instance configuration has the proper privileges (typically the Administrator role) on the ESX Server.
107	Setting ESX Server in maintenance mode timed out. Check that there are no VMs currently running on that server. You cannot set maintenance mode until all VMs on the ESX Server are shutdown. Retry, if this is not the case.

Table 1 (Cont.) Job Error Codes and Description

Error Codes	Description
200	Invalid number of arguments passed to EM job. Recheck the ESX Server target instance configuration.
201	ESX Web Service username and/or password not supplied. Recheck the ESX Server target instance configuration.
202	VM name specified does not exist on this ESX Server. Retry with correct VM name.
203	ESX remote exception occurred in setting up the ESX Server task. Ensure that the ESX Server is up and then retry.
204	VM is in an invalid state for this operation. Check status of VM or if the ESX Server is in maintenance mode, and then retry when appropriate.
205	There is an issue with the internal files of the VM.
206	VM configuration fault received.
207	ESX task against the VM is already running. Retry when appropriate.
208	There are insufficient resources for this ESX task. Retry when appropriate.
209	ESX runtime exception occurred in running the ESX Server task. Ensure that the ESX Server is up or that the ESX Server user has the proper privileges and/or roles, then retry.
210	Remote exception occurred in running the ESX Server task. Retry.

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will

handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at http://www.fcc.gov/cgb/consumerfacts/trs.html, and a list of phone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html.

System Monitoring Plug-in Installation Guide for VMware ESX Server, Release 5 (1.0.3.0.0) to Release 8 (1.1.3.2.0)
E13339-05