This document provides a brief description about the Oracle System Monitoring Plug-in for Microsoft Active Directory, details on the Active Directory versions and operating system platforms the plug-in supports, prerequisites for installing the plug-in, and step-by-step instructions on how to download, install, verify, and validate the plug-in.

Description

Microsoft Active Directory, which is included with the Microsoft Windows Server 2003 operating system, is a directory service enabling centralized, secure management of an entire network. It is used to manage identities and broker relationships between distributed resources.

The Active Directory Management Plug-in extends Oracle Enterprise Manager Grid Control to add support for managing the Microsoft Active Directory instances. By deploying the plug-in within your Grid Control environment, you gain the following management features for Microsoft Active Directory:

- Monitor availability and performance.
- Perform trend analysis on collected performance information.
- View and compare configuration data, as well as track configuration changes.
- Receive email and/or page notification concerning potential problems surrounding availability, performance, and/or configuration data.
- Gain access to rich out-of-box reports.
- Support monitoring by a remote Agent. For remote monitoring, the Agent does not need to be on the same computer as Active Directory.

Versions Supported

This plug-in supports the following versions of products:

- Enterprise Manager Grid Control 10g Release 2 or higher Management Service
- Enterprise Manager Grid Control 10g Release 2 or higher Agent for Windows
- Microsoft Windows 2003 Active Directory
- Microsoft Active Directory running on Microsoft Windows Server 2003 (see note below)
Prerequisites

The following prerequisites must be met before you can deploy the plug-in:

- Microsoft Windows 2003 Active Directory is installed.
- The following components of Oracle Enterprise Manager 10g Grid Control release 2 or higher are installed:
  - Oracle Management Service with Oracle Management Repository
  - Oracle Management Agent for Windows
    You can install the Agent on the same computer as Active Directory (referred to as local Agent monitoring), or you can install the Agent on a different computer from Active Directory (referred to as remote Agent monitoring).
- Ensure that the Windows Management Instrumentation Service is up and running.
- For remote Agent monitoring, a remote Agent must be properly configured. See "Configuring a Remote Agent" for the procedure.
- User privileges for the Job system of Enterprise Manager. For the procedure, refer to "Setting Credentials for the Job System to Work with Enterprise Manager" in one of the following installation guides:
  - Oracle Database Installation Guide 10g Release 2 (10.2) for Microsoft Windows (32-Bit) — B14316-01
  - Oracle Database Installation Guide 10g Release 2 (10.2) for Microsoft Windows (64-Bit) on Intel Itanium — B14317-02
  - Oracle Database Installation Guide 10g Release 2 (10.2) for Microsoft Windows (x64) — B15681-02
  These guides are listed in the Installation Guides section of the Oracle Database Documentation Library at the following location:
  http://www.oracle.com/pls/db102/homepage

Note: For details on which editions (such as Enterprise, Standard, and so forth) and versions of Windows operating systems that this Microsoft product is supported to run on, refer to the Microsoft website and/or documentation.

Deploying the Plug-in

After you ensure that the prerequisites are met, follow these steps to deploy the plug-in:
1. Download the Active Directory 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 in 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.


10. Click Add Agents, then select one or more Agents to which you want to deploy the plug-in. The wizard reappears and displays the Agent you 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.

---

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 Microsoft Active Directory Plug-in was deployed, select the Microsoft Active Directory target type from the Add drop-down list, then click Go. The Add Microsoft Active Directory page appears.

2. Provide the following information for the properties:

   - **Name** — Unique target name across all the Grid Control targets, such as `ActiveDirectory_Hostname`. This name represents this Active Directory target across all user interfaces within Grid Control.

   - **Host** — Host name or IP address of the computer hosting the Active Directory

   - **Username** — Host user name that must be an Administrator user or a user that is part of the Domain Admin Group. Required only for remote Agent monitoring.

   - **Password** — Password for the Username. Required only for remote Agent monitoring

   - **Agent Location** — Remote specifies that the Agent monitoring Active Directory targets is not on the same computer as the target being
monitored. (See "Configuring a Remote Agent" for more information.) Local specifies that the Agent monitoring the target is on the same computer as the target being monitored. Note that remote and local are case-sensitive and should be lowercase.

3. Click Test Connection to make sure the parameters you entered (such as the password) are correct.

4. Reenter the encrypted parameters from step 2 if the connection test was successful, then click OK.

Verifying and Validating the Plug-in

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

1. Click the Active Directory target link from the Agent home page Monitored Targets table. The Microsoft Active Directory home page appears.

2. Verify that no metric collection errors are reported in the Metrics table.

3. Ensure that reports can be seen and no errors are reported by selecting the Reports property page.

Configuring a Remote Agent

The steps for deploying the plug-in are the same for remote Agent monitoring and local Agent monitoring. However, if the Agent is on a remote computer from the plug-in target, certain configuration changes are required to access the Windows Management Instrumentation (WMI) data on the computer where the plug-in target resides.

In a scenario where Computer A runs the Agent, and the target is installed on computer B, do the following to set up Computer A:

1. Go to the Windows Control Panel and select Administrative Tools, then Services.

2. Select the Oracle Enterprise Manager Agent service from the listed computer where the Agent is running.

3. Right-click the service, then select Properties.

4. Click the Log On tab. By default, this service is started with the Local System account.

5. Change the default account by selecting the This account radio button, and provide an account and password that exist on both computer A and computer B.
Note that the account should be a member of the Administrators group, and the account should have administrative privileges on computer B. The password should not be left blank.

6. Click OK, then restart the Agent service.
7. Ensure that the Remote Registry Service for computer B is up and running.
8. Ensure that the Windows Management Instrumentation Service is up and running on both computers.

The Agent should now be able to collect data from the remote plug-in target computer. If the configuration above is not initiated, metric collection errors can appear for the plug-in target’s metrics.

To ensure that metric collection errors do not occur within Enterprise Manager, Oracle recommends reviewing the Microsoft documentation on the WMI setup. Refer to the Microsoft documentation from the Microsoft website for additional configuration details.

Note: For remote Agent monitoring with default settings, Grid Control can monitor only the Active Directory associated with the primary domain controller.

For a remote Agent, the platform to which the Agent is installed can be any Windows type that may not be supported for Active Directory. For example, if Active Directory is running on Windows 2003, you can install the remote Agent on Windows XP to monitor it.

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. The All Targets page appears.
3. Select the Active Directory Plug-in target and click Remove. You must do this step for all targets of the plug-in.
4. 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.
5. Make sure that the preferred credentials are set on the Agents where the plug-in is deployed.
6. Click the icon in the Undeploy column for the Active Directory Plug-in. The Undeploy Management Plug-in page appears.
7. Check all the Agents that are currently deployed with the Active Directory Plug-in and click OK. You must undeploy the plug-in from every Agent in the system to completely remove it from the enterprise.
Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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