Oracle® Enterprise Manager

System Monitoring Plug-in Installation Guide for Microsoft Active Directory

Release 12.1.0.1.0

E28548-03

September 2012

Microsoft Active Directory, which is included with Microsoft Windows Server 2003 and Microsoft Windows Server 2008 operating systems, is a directory service enabling centralized, secure management of an entire network. It is used to manage identities and broker relationships between distributed resources.

Description

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

- Monitor availability and performance.
- Perform trend analysis on collected performance information.
- View and compare configuration data, as well as track configuration changes.
- Receive e-mail 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 local or remote Oracle Management Agent (Agent). Local Agent is an agent running on the same host as the Microsoft Active Directory. Remote Agent is an agent running on a host that is different from the host where Microsoft Active Directory is running.

Versions Supported

This plug-in supports the following versions of products:

- Enterprise Manager Cloud Control 12*c* Release 1 (12.1.0.1.0) or higher
- Oracle Management Agent 12*c* Release 1 or higher for Microsoft Windows
- Microsoft Windows 2003 Active Directory and Microsoft Windows 2008 Active Directory
- Microsoft Active Directory running on Microsoft Windows Server 2003 or Microsoft Windows Server 2008 operating systems (see note below).

ORACLE

Note: For information on the 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 Web site and/or documentation.

Prerequisites

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

- Microsoft Windows 2003 Active Directory or Microsoft Windows 2008 Active Directory is installed.
- The following components of Oracle Enterprise Manager Cloud Control 12*c* Release 1 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 *Database Installation Guide for Microsoft Windows* (E24186-04):

  This guide is listed in the Installing and Upgrading section of the Oracle Database Documentation Library at:

  `http://www.oracle.com/pls/db112/homepage`

  Note: If you do not assign the correct privileges for users, the deployment will fail.

- If you want to use version 12.1.0.1.0 of the Microsoft Active Directory plug-in, then install this version on Oracle Management Agent 12*c* Release 1 for Microsoft Windows.

Deploying the Plug-in

See the *Plug-in Manager* chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for steps to deploy the plug-in:

`http://docs.oracle.com/cd/E24628_01/doc.121/e24473/plugin_mngr.htm`

Adding Instances for Monitoring

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

1. Log in to Enterprise Manager Cloud Control.

2. Click **Setup**, then **Add Targets**, and finally **Add Targets Manually**.
3. Select **Add Non-Host Targets by Specifying Target Monitoring Properties**. From the Target Type drop-down, select the **Microsoft Active Directory** target type. Click **Add Manually**.
4. Provide the following information for the properties:
   - **Name** — Unique target name across all the Cloud Control targets, such as ActiveDirectory_Hostname. This name represents this Active Directory target across all user interfaces within Cloud 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.

     Notes:
     - The agent chosen must also be an agent running on a Windows host.
     - The "remote" and "local" identifiers are case-sensitive and should be lowercase.
5. Click Test Connection **to make sure the parameters you entered (such as the password) are correct**. If the test was successful, proceed with adding targets.

   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 a part of.

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 **Targets**, then **All Targets**. On the All Targets page, 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, Cloud 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

See the *Plug-in Manager* chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for steps to undeploy the plug-in:

http://docs.oracle.com/cd/E24628_01/doc.121/e24473/plugin_mngr.htm

Documentation Accessibility

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

Access to Oracle Support

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

System Monitoring Plug-in Installation Guide for Microsoft Active Directory, Release 12.1.0.1.0
E28548-03