Oracle® Enterprise Manager

Microsoft Active Directory Plug-in User's Guide

13.4.0.0
F23296-01
January 2020

Oracle Enterprise Manager Microsoft Active Directory Plug-in User's Guide, 13.4.0.0

F23296-01

Contents

Preface

This document provides installation instructions and configuration information for the Oracle Enterprise Manager plug-in for Microsoft Active Directory.

Audience

This document is intended systems and database administrators tasked with monitoring Microsoft Active Directory through Enterprise Manager Cloud Control.

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 that have purchased support 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.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Microsoft Active Directory Overview and Prerequisites

This chapter provides an overview description of the Oracle system monitoring plug-in for Microsoft Active Directory and summarizes the prerequisites required before configuration.
The following topics are provided:

Microsoft Active Directory Overview

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.

Supported Versions

This plug-in supports the following versions of products:

- Enterprise Manager Cloud Control 13*c* Release 1 (13.1.0.1.0) and higher
- Oracle Management Agent 13*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).

> **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.

Microsoft Active Directory Plug-in Prerequisites

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

1. Microsoft Windows 2003 Active Directory or Microsoft Windows 2008 Active Directory is installed.
2. The following components of Oracle Enterprise Manager Cloud Control 13*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).
3. Ensure that the Windows Management Instrumentation Service is up and running.
4. For remote Agent monitoring, a remote Agent must be properly configured. See Configuring a Remote Agent for the procedure.
5. 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.

6. 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.

Downloading the Plug-in

You can download plug-ins in online or offline mode. *Online mode* refers to an environment where you have Internet connectivity, and can download the plug-in directly through Enterprise Manager from My Oracle Support. *Offline mode* refers to an environment where you do not have Internet connectivity, or where the plug-in is not available from My Oracle Support.

See the *Managing Plug-ins* chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for details on downloading the plug-in in either mode.

Deploying the Plug-in

You can deploy the plug-in to an Oracle Management Service instance using the Enterprise Manager Cloud Control console, or using the EM Command Line Interface (EMCLI). While the console enables you to deploy one plug-in at a time, the command line interface mode enables you to deploy multiple plug-ins at a time, thus saving plug-in deployment time and downtime, if applicable.

See the *Managing Plug-ins* chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for instructions on deploying the plug-in.

Upgrading the Plug-in

The Self Update feature allows you to expand Enterprise Manager's capabilities by updating Enterprise Manager components whenever new or updated features become available. Updated plug-ins are made available via the Enterprise Manager Store, an external site that is periodically checked by Enterprise Manager Cloud Control to obtain information about updates ready for download. See the *Updating Cloud Control* chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for steps to update the plug-in.

Undeploying the Plug-in

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

2

Discover the Microsoft Active Directory Target

This chapter describes how to discover your Microsoft Active Directory target with Enterprise Manager Cloud Control.
The following topics are provided:

- Discovering the Microsoft Active Directory Target
- Verifying and Validating the Plug-in
- Configuring a Remote Agent

Discovering the Microsoft Active Directory Target

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.

> **Note:**
>
> - 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.

Index