Oracle® Enterprise Manager

System Monitoring Plug-in Installation Guide for Microsoft Internet Information Services

Release 12.1.0.1.0

E28547-03

September 2012

This document provides a brief description about the Microsoft Internet Information Services plug-in, details on the Internet Information Services 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 Internet Information Services is a Web server available in all versions of Windows Server 2003. The Microsoft Internet Information Services Plug-in extends Oracle Enterprise Manager Cloud Control 12*c* to add support for managing Microsoft Internet Information Services 6.x and 7.x. By deploying the plug-in within your Cloud Control environment, you gain the following management features:

- Monitor availability and receive Internet Information Services data for the following performance areas:
  - WWW service
  - ASP.NET applications
  - ASP applications
  - FTP service
  - NNTP service
  - SMTP service
- 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 remote Agent. For remote monitoring, the Agent does not need to be on the same computer as Internet Information Services.

Versions Supported

This plug-in supports the following versions of products:

- Enterprise Manager Cloud Control 12*c* Release 1 or higher Management Service
- Enterprise Manager Cloud Control 12*c* Release 1 or higher Agent for Windows

- Microsoft Internet Information Server 6.0.x
- Microsoft Internet Information Services 6.x and 7.x running on Microsoft Windows Server 2003 (see note below)

> **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.

Prerequisites

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

- Microsoft Internet Information Services 6.x or 7.x is installed.
- The following components of Oracle Enterprise Manager Cloud Control 12*c* Release 1 or higher are installed:
  - Oracle Management Services with Oracle Management Repository
  - Oracle Management Agent for Windows

    You can install the Agent on the same computer as Internet Information Services (referred to as local Agent monitoring), or you can install the Agent on a different computer from Internet Information Services (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 Internet Information Services plug-in, you need to do one of the following:
  - Install this version on Oracle Enterprise Manager Windows Agent version 12.1.0.1.

    or
  - Apply a one-off patch on Oracle Enterprise Manager Windows Agent version 12.1.0.1. Refer to Oracle bug #5349647 for more information. You can access this bug through My Oracle Support:

    `https://support.oracle.com`

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 Internet Information Services** 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 iis_Hostname. The name represents this Microsoft Internet Information Services target across all user interfaces within Cloud Control.
   - **Host** — Full name (inclusive of domain, such as machineA.com) or the IP address of the host
   - **Username** — Host user name that must be an Administrator user. 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 Internet Information Services 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 **Internet Information Services Server** target link from the Monitored Targets table. The Microsoft Internet Information Services Server 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 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 a remote Agent, the platform to which the Agent is installed can be any Windows type that may not be supported for the Internet Information Services. For example, if the Internet Information Services 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 Internet Information Services, Release 12.1.0.1.0
E28547-03

Copyright © 2012, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.