This document provides a brief description about the Microsoft Internet Information Services (IIS) 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. The following topics are presented:

- Description
- Supported Versions
- Prerequisites
- Downloading the Plug-in
- Deploying the Plug-in
- Discovering Targets
- Verifying and Validating the Plug-in
- Configuring a Remote Agent
- Upgrading the Plug-in
- Undeploying the Plug-in

1 Description

Microsoft Internet Information Services is a Web server available in all supported versions of Windows Server. The Microsoft Internet Information Services plug-in extends Oracle Enterprise Manager Cloud Control 12c 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.

2 Supported Versions

This plug-in supports the following versions of products:

- Enterprise Manager Cloud Control 12c Release 1 or higher Management Service
- Enterprise Manager Cloud Control 12c Release 1 or higher Agent for Windows
- Microsoft Internet Information Server 6.0.x
- Microsoft Internet Information Services 6.x and 7.x (including IIS 7.5 on Windows Server 2008 R2) 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.

3 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 12c 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 Oracle Enterprise Manager” in Database Installation Guide for Microsoft Windows:

  http://docs.oracle.com/cd/E11882_01/install.112/e24186/postcfg.htm#BABFAEIG

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

http://www.oracle.com/pls/db112/homepage
4 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:

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

5 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:

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

6 Discovering Targets

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.

7 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.

8 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.

---

9 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:

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

10 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:

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

11 Documentation Accessibility

For information about Oracle’s commitment to accessibility, visit the Oracle Accessibility Program website at

Access to Oracle Support