

Oracle® Enterprise Manager

System Monitoring Plug-in Installation Guide for F5 BIG-IP Local Traffic Manager

Release 4 (2.2.1.1.0)

E12533-01

May 2008

This document provides a brief description about the Oracle System Monitoring Plug-in for F5 BIG-IP Local Traffic Manager, details on the versions 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

The System Monitoring Plug-in for F5 BIG-IP Local Traffic Manager extends Oracle Enterprise Manager Grid Control to add support for managing the F5 BIG-IP Local Traffic Manager. By deploying the plug-in in your Grid Control environment, you gain the following management features:

- Monitor the F5 BIG-IP Local Traffic Manager.
- Gather configuration data and track configuration changes for the BIG-IP Local Traffic Manager.
- Raise alerts and violations based on thresholds set on monitoring and configuration data.
- Provide rich out-of-box reports for the user interface based on the gathered data.
- Support monitoring by a remote Agent. For remote monitoring, the Agent does not need to be on the same computer as F5 BIG-IP.

Versions Supported

This plug-in supports the following versions of products:

- Enterprise Manager Grid Control 10g Release 2 or higher Management Service and Agent
- F5 BIG-IP Local Traffic Manager v9.1.x

Prerequisites

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

- Oracle Enterprise Manager Grid Control 10g Release 2 or higher Management Service and Agent
- F5 BIG-IP Local Traffic Manager configured to accept iControl web services calls from the Agent computer

- F5 BIG-IP Local Traffic Manager configured to allow pings from the Agent computer
- User configured on F5 BIG-IP Local Traffic Manager with Web User Role `guest` or higher. No https monitor should block the https calls for this user.
- Preferred credentials are set on all Agents where you want to deploy the plug-in. Unless you assign correct privileges, the deployment will fail.

Deploying the Plug-in

After you ensure that the prerequisites are met, follow these steps to deploy the plug-in:

1. Download the F5 BIG-IP Local Traffic Manager 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.
9. In the Management Plug-ins page, click the icon in the **Deploy** column for the F5 BIG-IP plug-in. The Deploy Management Plug-in wizard appears.
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 plug-in was deployed, select the **BIG-IP Local Traffic Manager** target type from the **Add** drop-down list, then click **Go**. The Add BIG-IP Local Traffic Manager page appears.
2. Provide the following information for the parameters:
 - **Name** — Name for the plug-in
 - **Host Name** — F5 BIG-IP Local Traffic Manager host name or IP address.

- **Port** — Port where the F5 BIG-IP plug-in can receive traffic, which is 443 by default for https
 - **Username** — Name of the user with `guest` or higher privilege for enabling the plug-in to access data
 - **Password** — Password for the login
3. Click **Test Connection** to make sure the parameters you entered (such as password) are correct.
 4. Reenter the encrypted parameters from step 2 if the connection test was successful, then click **OK**.

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 the F5 BIG-IP Local Traffic Manager target link from the Agent home page Monitored Targets table. The F5 BIG-IP Local Traffic Manager 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.
4. Ensure that configuration data can be seen by clicking the **View Configuration** link in the Configuration section. If configuration data does not immediately appear, click **Refresh** in the View Configuration page.

Upgrading the Plug-in

1. Download the F5 BIG-IP Local Traffic Manager 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 into 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 that you have downloaded for upgrading.
6. Click **List Archive**.
7. Select the plug-in and click **OK**.

8. Verify that preferred credentials are set on all Agents to which you want to deploy the plug-in.
9. Blackout the F5 BIG-IP Local Traffic Manager targets for agents to which you want to deploy higher version of the plug-in. Ensure that you select immediate blackout.
10. In the Management Plug-ins page, click the icon in the **Deploy** column for the F5 BIG-IP Local Traffic Manager plug-in. The Deploy Management Plug-in wizard appears.
11. 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.
12. 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.
13. Remove blackout for the targets (required only if Step 9 applies).

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 F5 BIG-IP Local Traffic Manager and click **Remove**. You must do this step for all instances of the plug-in.
4. Make sure that the preferred credentials are set on the Agents where the plug-in is deployed.
5. 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.
6. Click the icon in the **Undeploy** column for the F5 BIG-IP Plug-in. The Undeploy Management Plug-in page appears.
7. Check all the Agents that are currently deployed with the F5 BIG-IP Management Plug-in and click **OK**.

You must undeploy the plug-in from every Agent in the system to completely remove it from the enterprise.
8. Select the F5 BIG-IP Local Traffic Manager Management Plug-in on the Management Plug-ins page and click **Delete**.

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.

System Monitoring Plug-in Installation Guide for F5 BIG-IP Local Traffic Manager, Release 4 (2.2.1.1.0)
E12533-01

Copyright © 2008 Oracle. All rights reserved.

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States 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, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software—Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

