Oracle® Enterprise Manager

System Monitoring Plug-in Installation Guide for Check Point Firewall

10*g* Release 2 (10.2)

B28038-01

January 2006

This document provides a brief description about the Oracle System Monitoring Plug-in for Check Point Firewall, 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 Check Point Firewall extends Oracle Enterprise Manager Grid Control to add support for managing Check Point Firewalls. By deploying the plug-in in your Grid Control environment, you gain the following management features for Check Point Firewall:

- Monitor Check Point Firewall devices.
- Gather configuration and track configuration changes for Check Point Firewall instances.
- 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 Check Point Firewall.

Versions Supported

This plug-in supports the following versions of products:

- Enterprise Manager Grid Control 10*g* Release 2 Management Service and Agent
- Check Point Firewall versions:
  - NG- AI (R54)
  - NG-AI (R55)
  - NG-AI (R60)
  - NGX

Prerequisites

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

- Oracle Enterprise Manager Grid Control 10*g* Release 2 or higher system and Agent
- Check Point Firewall instance
- If 'SNMP Community' (other than default community 'public') is configured and required for monitoring the Check Point Firewall Target, you must add the Enterprise Manager Agent's IP address for the particular Simple Network Management Protocol (SNMP) Community.
- Configured Security Policy rules to allow connections from the Enterprise Manager Grid Control system to the Check Point Firewall using the predefined services `snmp` (UDP port 161) and `FW1_snmp` (UDP port 260) as needed.

Table 1 shows the prerequisites for operating systems that use the plug-in.

Table 1 Prerequisites for Operating Systems

Operating System	Prerequisites
Linux	Both the host SNMP daemon (`snmpd`) and Firewall SNMP daemon (`cpsnmpd`) must be running on the Check Point Firewall device. See "Linux Prerequisites Procedure" for more information.
Windows	▪ The standard Windows SNMP Agent must be installed, and SnmpService must be running. ▪ The Firewall SNMP sub-agent/extension agent must be installed. See "Windows Prerequisites Procedure" for more information.
Check Point SecurePlatform	The SNMP service must be enabled. See "SecurePlatform Prerequisites Procedure" for more information.

The sections referenced in Table 1 provide prerequisite procedures to enable SNMP `gets` on the Check Point Firewall device. For additional information, refer to the Check Point documentation.

Deploying the Plug-in

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

1. Download the Check Point Firewall 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 Check Point Firewall 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 Check Point Firewall Plug-in was deployed, select the **Check Point Firewall** target type from the **Add** drop-down list, then click **Go**. The Add Check Point Firewall page appears.
2. Provide the following information for the properties:
   - **Name** — Name for the plug-in, such as My_Check_Point_1
   - **Firewall Hostname or IP Address** — Name/IP Address of the Check Point Firewall device
   - **Check Point SNMP Daemon Port** — Port number where the Check Point SNMP daemon is running. The default is 260 on Linux platforms.
   - **Host SNMP Daemon Port** — Port number where the native OS SNMP daemon is running. The default is 161.
   - **SNMP Community** — Community name for which the Agent IP address is added. The default is Public.
   - **SNMP Timeout** — Timeout value by when the SNMP call should be terminated. A value of 5 is recommended.
   - **Check Point Firewall Web UI URL** — URL of the Check Point Web interface
   - **Telnet Enabled (y/n)** — If telnet is enabled on the Check Point Firewall device, specify the default value of **y**. Otherwise, leave this field blank.
3. Click **Test Connection** to make sure the parameters you entered 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 Check Point Firewall target link from the Agent home page Monitored Targets table. The Check Point Firewall 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.

Linux Prerequisites Procedure

Before proceeding to the "Deploying the Plug-in" section, do the following:

1. Find the `snmpd.conf` file, which is located under `/etc/snmp` or `/etc/SnmpAgent.d`. For more information, see the Directories Searched section in the following SNMP.CONF Website:

   `http://net-snmp.sourceforge.net/docs/man/snmp_config.html`

2. Edit the `snmpd.conf` file to enable SNMP calls for the following OIDs:

```
# Make at least snmpwalk -v 1 localhost -c public system fast again.
#       name           incl/excl     subtree         mask(optional)
view    systemview    included   .1.3.6.1.2.1.1
view    systemview    included   .1.3.6.1.2.1.2
view    systemview    included   .1.3.6.1.4.1.2021.11
view    systemview    included   .1.3.6.1.4.1.2021.4
view    systemview    included   .1.3.6.1.2.1.25
view    systemview    included   .1.3.6.1.2.1.4
```

3. Execute the following commands in sequence on the Check Point Firewall device:

   a. `service snmpd stop`

      If the `snmpd` service is running, the output of the command is:

      `stopping snmpd              [OK]`

      If the `snmpd` service is not running, the output of the command is:

      `stopping snmpd              [FAILED]`

   b. service snmpd start

The output of the command is:

```
starting snmpd              [OK]
```

4. Enable the Check Point SNMP Extension using the `cpconfig` command.

   On Unix platforms, a special Check Point SNMP daemon, `cpsnmpd`, is installed. This daemon provides status information on VPN-1 Pro specific objects. This daemon is not run by default. The daemon is enabled or disabled through `cpconfig`. Once enabled, the daemon listens on port 260.

   Note: The standard Unix SNMP daemon loads before the Check Point daemon and binds to port 161. If the regular daemon is not running, `cpsnmpd` binds to both ports (161 and 260). If both ports are occupied by a previous process, the Check Point daemon does not run. Furthermore, if the Check Point daemon receives a request for an unrecognized OID, it does not forward this to the standard SNMP OS daemon.

Windows Prerequisites Procedure

Before proceeding to the "Deploying the Plug-in" section, refer to the Windows user guides to install and configure the SNMP service.

When the Check Point Firewall is installed, a special Check Point dynamic link library (DLL) is listed in the window's registry. The SNMP service running on the Operating System loads this DLL. The SNMP service listens on port 161 for incoming SNMP requests from the SNMP Network Management Station. The Check Point DLL extends the Windows NT SNMP service to identify the status requests directed at Check Point products.

SecurePlatform Prerequisites Procedure

Check Point SecurePlatform is a prehardened operating system that can be deployed on Intel- or AMD-based open servers. A net-snmp daemon listens on UDP port 161 and provides access to OS-MIB-II. A Check Point AgentX daemon extends access to the Check Point product MIB through the net-snmp daemon listening on UDP port 161.

Before proceeding to the "Deploying the Plug-in" section, do the following:

1. By default, the SNMP service is disabled. Enable it with the following command:

   ```
   snmp service enable [<portnumber>]
   ```

2. Use other `snmp` commands, as shown below, to configure.

   ```
   snmp service stat
   snmp service disable
   snmp user add noauthuser <username> [oidbase <OID>]
   snmp user add authuser <username> pass <passphrase> [priv
   <privacyphrase>] [oidbase <OID>]
   snmp user del <username>
   snmp user show [<username>]
   ```

3. You can provide additional configuration information by editing the following SNMP file:

   `/etc/snmp/snmpd.conf`

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 Check Point Firewall Plug-in target and click **Remove**. You must do this step for all targets 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 Check Point Firewall Plug-in. The Undeploy Management Plug-in page appears.
7. Check all the Agents that are currently deployed with the Check Point Firewall 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 Check Point Firewall 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 Check Point Firewall, Release 2 (10.2)
B28038-01