Oracle® Enterprise Manager

System Monitoring Plug-In Installation Guide for Exadata Cisco Switch

Release 11.1.0.1.0

E20084-04

July 2011

The Cisco Switch Plug-in enables Enterprise Manager Grid Control to monitor Cisco Switch targets. This plug-in will be used to monitor the Cisco switch's CPU, memory, temperature, network interfaces, system information, fan, and power supply metrics. Each Cisco switch will have a plug-in instance added to its own OEM GC agent.

Overview of the Plug-In

By deploying the plug-in to your Grid Control environment, you gain the following management features:

- Monitor Cisco Switch targets.
- Raise alerts and violations based on thresholds set on monitoring and configuration data.
- Provide rich out-of-box metrics and reports based on the gathered data.

Versions Supported

This plug-in supports the following versions of products:

- Oracle Exadata Storage Server 11g Release 2 (11.2) and later
- Enterprise Manager Grid Control 11g Release 1 (11.1) and later

Prerequisites

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

- For all Management Agents on which the Cisco switch plug-in is deployed, you must set and validate the preferred credentials in Enterprise Manager.

Deploying the Plug-In

After you ensure that the prerequisites are met, follow these steps to deploy the plug-in to the appropriate Management Agents.

1. Download the Cisco Switch Plug-In archive file to your desktop or computer on which the browser is launched. You can download the archive from Oracle Technology Network (OTN).
2. Log in to Enterprise Manager Grid Control as SYSMAN.

3. Click **Setup** from the upper-right-corner of the Grid Control Home page, then click **Management Plug-ins** from the left-side menu of the Setup page.
4. Click **Import**.
5. Click **Browse.** Navigate to the directory where you have downloaded the plug-in JAR file. Select the JAR file, then click **OK**.
6. Click **List Archive**. The plug-ins within the selected JAR file appear in a list.
7. Select the check box for the Cisco Switch version 1.2 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 plug-in.

   The Deploy Management Plug-in wizard appears.
10. Click **Add Agents**.
11. Select **Agent** from the Target Type pull down menu.
12. Select the Agent(s) you want to deploy the plug-in to, then click **Select**.
13. Click **Next**, then click **Finish.** The plug-in is deployed to the selected Agents.

    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. To go to the Preferences page, click **Preferences** from the top-right corner of the Grid Control page.

Hardware Configuration

Follow the below steps to configure Cisco switch for EM plug-in (the Cisco switch host name in the example below is 'dm01sw-ip'):

1. Login to the Cisco switch and enter Configure mode:

```
# telnet dm01sw-ip
User Access Verification
Password:
dm01sw-ip> enable
Password:
dm01sw-ip# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
dm01sw-ip(config)#
```

2. Enable access to allow the plug-in to poll the switch. In the command, <EMagentIPaddr> is the IP address of the server where the EM Agent is running that has the EM Cisco Switch Management Plug-In deployed. The SNMP community specified must match the value provided during EM Cisco Switch Management Plug-In setup:

```
dm01sw-ip(config)# access-list 1 permit <EMagentIPaddr>
dm01sw-ip(config)# snmp-server community <community_string> ro 1
```

3. Set the EM Cisco Switch Management Plug-In as the location where SNMP traps are delivered. The SNMP community specified must match the value provided during EM Cisco Switch Management Plug-In setup:

```
dm01sw-ip(config)# snmp-server host <EMagentIPaddr> version 1 <community
string> udp-port <EMagentRecvltListenPort>
```

Where *EMagentRecvltListenPort* is the EMD_URL port of emagent or SnmpRecvletListenNIC property value if it is enabled.

4. Configure the switch to send only environmental monitor SNMP traps:

```
dm01sw-ip(config)# snmp-server enable traps envmon
```

5. Verify settings and save the configuration:

```
dm01sw-ip(config)# end
dm01sw-ip# show running-config
dm01sw-ip# copy running-config startup-config
```

Adding Cisco Switch Targets for Monitoring

After successfully deploying the plug-in, follow these steps to add the Cisco Switch target to Grid Control for central monitoring and management:

1. Click the **Targets** tab, the click **All Targets**.
2. Select **Agent** from the "Search" pull down menu. Enter the server hostname of the first database server name in your cluster in the search field, then click **Go**.
3. Click on the Agent you want to add as a target (sclczdb01.us.oracle.com:3872 in the example below). IMAGE
4. Select the **Cisco Switch** target type from the "Add" pull down menu, then click **Go**.
5. Enter the following parameters in the Add Cisco Switch page:
   - Name: Enter the switch name, which should match the Cisco Switch hostname
   - Hostname or IP Address: Enter the switch name
   - SNMP Read Community String: Accept the default value
   - SNMP Timeout: Accept the default value
6. Click **Test Connection** to make sure the parameters you entered are correct.
7. If the test is successful, click **OK**.

Verifying Hardware Configuration

Using the `snmpwalk` command line utility or equivalent tool, Cisco switch configuration can be verified.

Running the following command should fetch the data from the Cisco switch and display them:

```
snmpget -v 1 -c <community_string> <hostname_of_cisco_switch>
1.3.6.1.4.1.9.2.1.56.0
```

Verify the Cisco Switch Plug-in

This section provides the steps to validate that the plug-in can collect the metrics through SNMP queries.

Prerequisites:

- Install the plug-in.
- Configure the Cisco switch for accepting SNMP queries from the EM Agent and send trap information to the EM Agent host and `recvlt` listening ports (default `recvlt` listening port is `EMD_URL` port).

Verify:

To verify the Cisco switch is configured correctly for responding to SNMP queries from the EMAgent:

- In the EM console, go to the Cisco switch target page.
- The *All metrics* link should show all the data collected.
- The *Alert history* link should show the events generated, if any.

Setting Up Alerts

After configuring the Cisco Switch targets to send SNMP alerts, set up alerts in Grid Control.

1. Log in to Enterprise Manager Grid Control as SYSMAN.
2. Click the **Targets** tab, then **All Targets**.
3. In the All Targets page, from the **Search** list, select **Cisco Switch** and click **Go**.
4. Click the target you are interested in. The target home page appears.
5. Click **Metric and Policy Settings** in the Related Links section of the page.
6. In the Metric and Policy Settings page, you can modify metric threshold values, edit monitoring settings for specific metrics, change metric collection schedules, and disable collection of a metric.

   You can modify the thresholds directly in the table or click the edit icon (pencil icon) to access the Edit Advanced Settings page. For more information on the fields displayed in this page and how the thresholds can be modified, click **Help** from the top-right corner of this page.

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 Exadata Cisco Switch, Release 11.1.0.1.0
E20084-04

Copyright © 2011, 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 USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software 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 which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software 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.

The System Monitoring Plug-in allows Oracle Enterprise Manager to monitor Cisco switches. The Plug-is available under the open source BSD license (http://www.opensource.org/licenses/bsd-license.php).

BSD License:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sicredi nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.