

Oracle® Enterprise Manager

System Monitoring Plug-In Installation Guide for Exadata Avocent MergePoint Unity Switch

Release 11.1.0.2.0

E20086-03

March 2011

Overview of the Plug-In

The Avocent MergePoint Unity Switch Plug-in enables Enterprise Manager Grid Control to monitor KVM (keyboard, video or visual display unit, mouse) targets. The plug-in provides status of the KVM and the event occurrences like Factory Defaults Set, Fan Failure, Aggregated Target Device Status, Power Supply Failure, Power Supply Restored, Reboot Started, Temperature Out of Range on the KVM target.

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 (Oracle Management Service and Oracle Management Agent)
- Oracle Management Agent 11g Release 1 (11.1) and later

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 KVM 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 KVM plug-in Release 11.1.0.2.0 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.

Adding KVM Targets for Monitoring

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

1. Click the **Targets** tab, then 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.
4. Select the **KVM** target type from the "Add" pull down menu, then click **Go**.
5. Enter the following parameters in the Add KVM page:
 - Name: Enter the switch name
 - KVM hostname or IP Address: Enter the IP address or DNS name
 - KVM console URL (optional) : URL for the KVM console
6. Click **Test Connection** to make sure the parameters you entered are correct.
7. If the test is successful, click **OK**.

KVM Device Configuration

After deploying the KVM plug-in to your Management Agent(s), you must configure KVM to send SNMP traps to the Agent host. As part of this exercise, you must set the device Application software version must be 1.2.8 or later. The current version can be obtained by logging into the web interface of the KVM. On the left side of the screen under Unit View, Appliance, Appliance Settings, click Versions to view the Application software version. Software updates for the KVM are available at:

http://www.avocent.com/Support_Firmware/MergePoint_Unity/MergePoint_Unity_Switch.aspx

Configure the KVM to send traps to EMAGENT host and recvlt listening port (i.e port value of EMD_URL property from \$ORACLE_HOME/sysman/config/emd.properties.

Say the port value is 3872.

1. Login to the management console.
2. Click on the **SNMP** link under Target Devices in the left-hand navigation bar.
3. Select the **Enable SNMP** check box and enter the appropriate community name in the "Read" "Write" and "Trap" fields ("public" in this example).
4. Click **Save**.
5. Click the **Destinations** link under SNMP in the left-hand navigation bar.
6. Enter the IP address of the database server hosting the Management Agent the KVM plug-in has been deployed to.
7. Click **Save**.

Now you must manually configure SNMP traps on the host where the plug-in is configured. The Agent receivelet port is specified as the value of the EMD_URL property in the \$ORACLE_HOME/sysman/config/emd.properties file.

For the Enterprise Manager Agent to receive traps, an SNMP trap forwarder must be set up on the host where the Enterprise Manager Agent is running; so, that this forwarder utility can receive traps using port 162 and forward the same to agent recvlt's listening port.

Follow the steps on the system running the Enterprise Manager Agent. These commands must be run as root user.

1. Get the port value from EMD_URL property in the \$ORACLE_HOME/sysman/config/emd.properties file. This is the port at which recvlt will listen over UDP for traps (for this example, the port value is 3872).
2. Confirm if recvlt is listening on this port over UDP. An entry should be seen in the below command's output:

```
netstat -an | grep 3872 | grep udp
```

3. Run the following command:

```
service snmptrapd stop
```

Typically the service command will be located in /sbin directory.

4. Add the following entry in /etc/snmp/snmptrapd.conf:

```
forward default udp:localhost:3872
```

5. Run the following command:

```
chkconfig snmptrapd on
```

6. Run the following command:

```
service snmptrapd start
```

Setting Up Alerts

After configuring the KVM 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. Select **KVM** from the search list, then 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.

Note: Except for the Response metric, all other KVM metrics are push-based. For push-based metrics, threshold values are dealt on the KVM target side. The KVM target will generate traps to the Enterprise Manager Agent, and the same will be converted as EM events.

So, it is not necessary for the user to modify the threshold or collection schedules values for push-based metric in the Enterprise Manager console.

Verify Configuration

Using the `snmptrapd` command line utility or equivalent tool, the KVM configuration can be verified.

Follow the below steps on the emagent box by login as root:

1. Run the following command:

```
service snmptrapd stop
```
2. Rename the file `/etc/snmp/snmptrapd.conf` to be `/etc/snmp/snmptrapd.conf_bk`
3. Run the following command:

```
snmptrapd -p 162
```
4. Reboot the KVM to generate the SNMP traps.
5. The terminal where the `snmptrapd` command was run should display the received trap which is generated by KVM for reboot.

If step 5 is confirmed, then KVM has been configured correctly. Rename the back-up file and restart the `snmptrapd` service:

1. Stop the `snmptrapd` command that was started in step 3 above (use `Ctrl+c` to stop the command).

2. Rename the file `/etc/snmp/snmptrapd.conf_bk` to be `/etc/snmp/snmptrapd.conf`
3. Run the following command:

```
service snmptrapd start
```

Verify the KVM Plug-in

This section provides the steps to validate that the plug-in can receive SNMP traps that is generated by KVM and convert the received traps to EM events.

Prerequisites:

- Install the plug-in.
- Configure the KVM to deliver SNMP traps to the plug-in.

Verify:

To verify the KVM is configured correctly to send and the plug-in is configured correctly to receive a sample SNMP traps, reboot the KVM as mentioned below:

1. Log in to the KVM.
2. On the left side of the screen under Unit View, Appliance, click Overview.
3. Click Reboot.
4. Confirm KVM reboot by clicking OK in the window that asks if you want to continue.
5. In the EM console, go to the KVM target page and click the Alert history link. You should see the EM event for the generated trap.

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 Exadata Avocent MergePoint Unity Switch, Release 11.1.0.2.0
E20086-03

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 software or related documentation 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.