Introduction

Configuration of Oracle Enterprise Manager 13c to discover Oracle Private Cloud Appliance and embedded Oracle VM Manager

Monitoring the Oracle Private Cloud Appliance Rack

Configuring Incident Rules for Oracle Private Cloud Appliance

Incident Rules overview

Incident Rule for Warnings

Incident Rule for Oracle VM Server and ovs-agent down

Incident Rule for Oracle PCA Management Node Enterprise Manager Agent

Incident Rule to forward critical incidents via SNMP or Management Connector

Conclusion
Introduction

We will discuss the monitoring features of Oracle Enterprise Manager 13c with Oracle Private Cloud Appliance (PCA). Oracle Enterprise Manager 13c, using the Virtualization Plug-in can monitor Oracle Private Cloud Appliance rack and components. From the Oracle PCA rack view, we can monitor and manage Oracle PCA embedded Oracle VM Server. Oracle Enterprise Manager 13c provides an incident management framework where any events are actioned based upon incident rules or corrective actions. This paper will discuss and define an approach to monitoring Oracle PCA and provide examples of incident rules.

Configuration of Oracle Enterprise Manager 13c to discover Oracle Private Cloud Appliance and embedded Oracle VM Manager

There are some configuration steps required to discover Oracle PCA and embedded Oracle VM Manager by Oracle Enterprise Manager. These steps involve configuration on both Oracle Enterprise Manager and the embedded Oracle VM Manager. The high-level steps are as follows:

- Install the Oracle Enterprise Manager 13c agent on the Oracle PCA management nodes
- Install the Oracle Enterprise Manager VT Plug-in
- Discover Oracle PCA
- Register Oracle PCA embedded Oracle VM Manager with Oracle Enterprise Manager 13c

The following whitepaper fully covers the steps and configuration. The remainder of this whitepaper assumes you have followed the referenced whitepaper, and have successfully discovered the Oracle PCA rack and embedded Oracle VM Manager.

Monitoring the Oracle Private Cloud Appliance Rack

Oracle Enterprise Manager is capable of managing multiple Oracle PCA’s as well as multiple Oracle VM Managers. To access individual PCA’s via the Oracle Enterprise Manager UI go to Targets=> Private Cloud Appliance.

From here, we see a list of Oracle PCA’s discovered from Oracle Enterprise Manager. Select the Oracle PCA by clicking on the link; this will take you to the home page for that Oracle PCA.
This is the default view, which is Schematic. The colored Components view allows us to see the types of components. Servers are dark blue and switches light blue. Notice red rings around some of the components; this indicates an alert, which we will discuss later. The default view is for component hostnames; however, we can change to an IP addresses, adding temperature and exposing empty slots.
Two further views are possible: Photo-realistic or table. Photo-realistic provides a view of the front and back of the Oracle PCA; note we still see the red rings around components that have incidents.
Table view provides the following; note the Incidents at the top of the page as well as a linked number (18) in our case for Infiniband Switches, which indicates critical (red circle with white cross) alerts.
The Overview panel is common to each of the three views providing a view of all Incidents and on the right hand side of the panel a link to the Oracle PCA embedded Oracle VM Manager.

Returning to the default Schematic view and the components with an alert. If we click on the component with a red ring we see high-level information regarding the component as well as a numbered link that when clicked will take us directly to the Oracle Enterprise Manager Incident Manager. The Incident Manager framework allows us to assign and work on open incidents as well as searching My Oracle Support knowledge bases and open Service Requests. Further information for the Oracle Enterprise Manager 13c Incident Manager is here.
The link underneath Target Details will take us to the home page of this component if clicked. In this example, this is one of the Infiniband switch home pages.

Notice the red rings around certain ports. This indicates that there are incidents at the port level. Similarly, if we click on a port with a red ring we have the same view as we had for the switch with a numbered link to the Incident within Incident Manager.

The main page for the IB switch is by default set to the hardware view.
Two other options are available:

1. **Network Connectivity**, which provides monitoring of the IB Interfaces, Data Links and Ports.

2. **Performance**, which provides monitoring of I/O Throughput, Temperature and Fans

For a view of the Fabric Topology from the Oracle Enterprise Manager UI go to **Targets => All Targets**

From the left hand menu, select **Ethernet/Infiniband Fabric** then **Systems Infrastructure Switch**

In our example, we have a single fabric, however there maybe multiple fabrics, therefore select the fabric you are interested in. This will take you to the home page of the fabric with a similar view to that of the physical switch shown earlier.
From the target page main menu select **Fabric Topology**.

If we hover our mouse over any link or component this will show further information regarding the component or relationship within the fabric.
As with the physical switch view, you can display date based Performance and Problems from the Fabric home page.

Returning to the Oracle PCA rack home page, we can expose a tabular view of all the components within the rack via the Target Navigation icon.
This exposes the top tiers of the Oracle PCA.

If we click on the > arrow this will expose the other main component areas of the Oracle PCA.

This is a useful and quick method of accessing component areas or separate components. All the component areas have home pages similar in concept to the switch and fabric pages shown earlier. For further details on these home pages, refer here.

We can also use the View menu to expose all elements.
This provides the following view, which in the case of the Oracle PCA compute node shows the Oracle VM Hypervisor and Oracle VM Guests.

Using the View menu, we can also collapse all to return to the original view. If we click on the PCA Rack link, we have a similar view to the switch home page with useful information such as the Oracle PCA System ID.
The default view for this page in the photo-realistic view, however as with the main Oracle PCA page you can change the view to schematic or table. Currently we do not monitor the Power Distribution Units (PDU’s); this is planned for a future release.

As with the switch home page, the Hardware view is default with options to access Firmware, Power and Temperature. The other tabs are on the right hand side as with the switch and other component target pages.
The Oracle PCA Incidents panel by default shows all Incidents for all components of the Oracle PCA. Each component home page has its own Incidents panel.

By accessing the Category menu shown in a red ring above we can filter types of incidents. Interesting areas are Availability, Capacity and Fault.
The release of Oracle Enterprise Manager 13.3 provides enhanced monitoring for the Oracle Fabric Interconnect switches within the Oracle PCA.

These new monitoring features are:

- Cumulative fabric performance
- Managed devices
- Discovered PCA compute nodes
- Configured IO templates
- Network and storage clouds
- Alarms tracked by the Oracle Fabric Manager

To view this enhanced information select the Fabric Interconnect Target from the All Targets Menu or click on the Fabric Interconnects on the PCA target Navigation tree.
The following regions are available:

Summary

The summary section of the Fabric Interconnect home page lists the current Oracle Fabric Manager's status and version, and the high availability mode. Oracle Fabric Manager supports high availability mode, in which multiple Fabric Manager servers are associated with each other to provide a system of Fabric Manager servers that operate in active or passive roles.

Cumulative Performance

When vNICs and vHBAs are configured and deployed on the PCA compute nodes it can be seen in the graph of the network and storage total throughput.
Devices
Information about the Oracle Fabric Interconnect chassis and the Oracle Software Defined Networking (SDN) that are managed through the Oracle Fabric Manager is displayed in the Fabric Interconnect home page. The Devices table displays the host name of each managed device, the device IP address, the software version currently installed on each managed device, the current state of the managed device and the model of the device.

Servers
Oracle Fabric Manager discovers servers that are connected through the devices and have Oracle Virtual Networking Drivers installed. This table lists the host name of each PCA compute node that Oracle Fabric Manager has discovered, the operating system currently in use, the name of the I/O profile and the total number of vNICs and vHBAs that are configured.

I/O Templates
When I/O templates are configured, they are listed in the Fabric Interconnect home page regardless of whether they are deployed to a host server or not. This table lists the name of each configured I/O template, the total number of vNICs and vHBAs configured in each I/O template, and the description that was applied to the I/O template. For PCA we currently do not use I/O templates, however added for completeness.

Network Clouds
Information about the Private Virtual Interconnect (PVI) clouds is displayed. This table lists the name of each configured cloud, the number of Ethernet ports, and link aggregation groups (LAGs) in the cloud. Currently PCA does not support LAG’s. However added for completeness.

Storage Clouds
Information about the configured storage clouds is displayed. This table lists the name of each configured cloud, and the number of Fibre Channel ports in the storage cloud.

Alarms
The Oracle Fabric Interconnect target monitors system events and network management alarms tracked by the Oracle Fabric Manager. The alarms shown in the Fabric Interconnect home page are of one of the following severities:

- Critical
- Major
- Minor
- Warning

To view critical, major, minor, and warning alarms go to the Oracle Fabric Interconnect's All Metrics page, and select the Alarms metric. Critical alarms are displayed in the Incidents and Problems section of the Fabric Interconnect home page. Major, warning and minor alarms can also appear on the Incidents and Problems section, if the user activates a rule for this purpose (see the next section).
Configuring Incident Rules for Oracle Private Cloud Appliance

Incident Rules overview

You can take action on events or incidents; an example of an event could be a metric within a target exceeding a set threshold. An incident is useful as it can address complex situations where a number of events that are related may indicate a higher-level issue.

To access the Incident Rules framework from the Oracle Enterprise Manager UI, navigate to **Setup > Incidents > Incident Rules**. There are some system-defined rules, which have a padlock beside them indicating they are fixed.
The following actions are available from an Incident Rule:

- Send an email (the email server must be enabled within Oracle Enterprise Manager and email addressed defined for Administrators)
- Page someone
- Send an SNMP V1 or V3 trap (these SNMP targets need to be configured within Oracle Enterprise Manager)
- Run an OS command
- Run a PL/SQL procedure
- Create an incident
- Send the information to an external connector (these connectors must be available and configured within Oracle Enterprise Manager)

The first system generated rule (Incident management rule set for all targets) sets a series of rules, one of which creates an incident for any critical or fatal events.

Incident Rule for Warnings

In the previous section, we discussed that by default all critical and fatal events create an incident. Warnings by default do not create an incident. We can address this by creating an Incident Rule similar to the system provided one for critical and fatal events. One point to bear in mind is that this may generate many incidents within your Incident view. However, Warnings may be useful as a sign that things are starting to become urgent and may escalate causing a critical or fatal incident. The Incident Rule framework is very flexible and if you do not want to see Warnings in the Oracle PCA Incident panel, you can set a rule to email an Admin, run a script, send an SNMP trap or forward to a connector to another management system. The following example shows an Incident rule, which creates an incident when any Oracle PCA component creates a warning.

We highlight the rule and then click edit.
HOW TO MONITOR ORACLE PRIVATE CLOUD APPLIANCE WITH ORACLE ENTERPRISE MANAGER 13C

Refer to the table below for detailed explanations about each of the fields indicated by the callouts in the screen shot of the top of the edit Rule Set page.

**EXPLANATION OF NUMBERED ITEMS**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Give the Rule Set a unique and meaningful name</td>
</tr>
<tr>
<td>2</td>
<td>Enabled is yes</td>
</tr>
<tr>
<td>3</td>
<td>The rule can apply to all targets, types of targets or in our case specific targets</td>
</tr>
<tr>
<td>4</td>
<td>In our example, we have two Groups. Groups are a concept within Enterprise Manager where targets of similar or identical types can be grouped together for group-based management and monitoring. For further information on Groups refer <a href="#">here</a></td>
</tr>
<tr>
<td>5</td>
<td>Here we can exclude any targets from the Rule Set. This may be useful if you have large numbers of targets within a group</td>
</tr>
</tbody>
</table>

Refer to the table below for detailed explanations about each of the fields indicated by the callouts in the screen shot of the bottom of the edit Rule Set page. Here we see a single rule; however, there could be multiple rules within a single Rule Set.
EXPLANATION OF NUMBERED ITEMS

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Give the Rule a unique and meaningful name. By default when created rules are given numbers.</td>
</tr>
<tr>
<td>2</td>
<td>Any meaningful description is helpful</td>
</tr>
<tr>
<td>3</td>
<td>This Rule applies if the severity received is Warning</td>
</tr>
<tr>
<td>4</td>
<td>This is the action which in our case is to create an incident</td>
</tr>
<tr>
<td>5</td>
<td>States this rule is enabled</td>
</tr>
<tr>
<td>6</td>
<td>When the rule was last updated</td>
</tr>
<tr>
<td>7</td>
<td>Which user last updated the rule</td>
</tr>
<tr>
<td>8</td>
<td>What type of rule this is, in our case it is an event</td>
</tr>
</tbody>
</table>

Once we have completed any edits we should click the **Save** button to exit.

Incident Rule for Oracle VM Server and ovs-agent down

It is particularly useful to know when an Oracle VM Server is down. When this happens an availability incident appears in the Oracle PCA Incident panel. The same happens when an Oracle VM Server may be up but for some reason the ovs-agent service is not running. The following example shows an Incident rule, which sends an email when a server down and up event happens.
We highlight the rule and then click edit.

Refer to the table below for detailed explanations about each of the fields indicated by the callouts in the screen shot of the bottom of the edit Rule Set page.

### EXPLANATION OF NUMBERED ITEMS

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Our example uses specific targets, which in our case is a Group. This group is Oracle VM Servers within the Sales and Accounts private clouds</td>
</tr>
<tr>
<td>2</td>
<td>Rules name</td>
</tr>
<tr>
<td>3</td>
<td>This Rule applies to the targets availability status</td>
</tr>
<tr>
<td>4</td>
<td>This is the action which in our case is to email the Cloudadm user</td>
</tr>
</tbody>
</table>

An example of the email alert for down:

Host=**my_pca_management_vip.oracle.com**
Target type=**Oracle VM Server**
Target name=**ovcacn12r1**
Categories=**Availability**
Message=**Oracle VM Server ovcacn12r1 is down**
Severity=**Fatal**
Event reported time=**Nov 24, 2017 8:33:46 AM GMT**
Operating System=**Linux**
Platform=**x86_64**
Associated Incident Id=21656
Associated Incident Status=**New**
Associated Incident Owner=  
Associated Incident Acknowledged By Owner=**No**
Associated Incident Priority=**None**
Associated Incident Escalation Level=0
Event Type=**Target Availability**
Event name=**Status**
Availability status=**Down**
Root Cause Analysis Status=**Neither Cause Nor Symptom**
Causal analysis result=**Neither a cause nor a symptom**
Rule Name=**PCA_Compute_Node_Down,OVM Server Down**
Rule Owner=**CLOUDADM**
Update Details: Oracle VM Server ovcacn12r1 is down
Incident created by rule (Name = Incident management rule set for all targets, Incident creation rule for a Target Down availability status [System generated rule]).

An example of the email alert when a server returns to service:

Host= my_pca_management_vip.oracle.com
Target type= Oracle VM Server
Target name= ovcacn12r1
Categories= Availability
Message= Oracle VM Server ovcacn12r1 is up
Severity= Clear
Event reported time= Nov 24, 2017 8:53:46 AM GMT
Operating System= Linux
Platform= x86_64
Associated Incident Id= 21656
Associated Incident Status= Closed
Associated Incident Owner=
Associated Incident Acknowledged By Owner= No
Associated Incident Priority= None
Associated Incident Escalation Level= 0
Event Type= Target Availability
Event name= Status
Availability status= Up
Rule Name= PCA_Compute_Node_Down, OVM Server Down
Rule Owner= CLOUDADM
Update Details:
Oracle VM Server ovcacn12r1 is up

Incident Rule for Oracle PCA Management Node Enterprise Manager Agent

The Enterprise Manager Agent on the Oracle PCA Management node runs in a shared location to enable service to continue in the event of a management node failover. There is a Virtual IP address, which the Enterprise Manager Agent uses to enable failover. In order to monitor the health of this key Agent we create an Incident Rule to email the Cloudadm user when the Agent is both unreachable and when it becomes reachable. This approach is similar in approach to the previous example for Oracle VM Server monitoring.

Although we cannot explicitly monitor each Oracle PCA Management node, we can use the health of the Enterprise Manager Agent on the management node as an indicator. For example, using this rule, if we receive an email stating the Agent is down and then we receive a second email stating the Agent is up this could indicate a management node failover has occurred. In this event, the Cloudadm should investigate the health of the passive management node. If we receive an email stating the Agent is down and receive no Agent up email then the Cloudadm should investigate the health of both management nodes.

Incident Rule to forward critical incidents via SNMP or Management Connector

Many customers have multiple monitoring systems and wish to send alerts from Oracle Enterprise Manager to external monitoring systems. For high level monitoring sending critical incidents is essential. The following example shows the creation of an Incident rule, which sends an alert via SNMP and a Management Connector when a critical event happens. The SNMP configuration is a separate task and will be dependent on the requirements of the external SNMP receiver. Refer here for how Oracle Enterprise Manager supports SNMP. Similarly, the installation and configuration of the Management Connector is a separate task and based upon the appropriate Management Connector being available. Refer here for further details on supported Management Connectors.
From the Oracle Enterprise Manager UI, navigate to Setup > Incidents > Incident Rules and click on Create Rule Set.

Refer to the table below for detailed explanations about each of the fields indicated by the callouts in the screen shot of the top of the Create Rule Set page.
EXPLANATION OF NUMBERED ITEMS

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Give the Rule Set a unique and meaningful name.</td>
</tr>
<tr>
<td>2</td>
<td>Any meaningful description is helpful</td>
</tr>
<tr>
<td>3</td>
<td>This Rule Set applies to Targets, other choices are Job, Metric Extensions or Self Update</td>
</tr>
<tr>
<td>4</td>
<td>I have selected Specific Targets and used a Group I created with target type of Oracle PCA. We need to take this approach rather than specify the Oracle PCA target.</td>
</tr>
</tbody>
</table>

We now need to scroll down the page until we reach the Rules panel, which for a new Rule set should be empty.

We click **Create** to create our Rule. We want Incoming and updates to events so take the default for the Rule Type and click **Continue**.

The Create Rule Set wizard runs starting with Step1 of 4.
We need all events of type Metric Alert and need to expand the Advanced Selection Option arrow. Once these fields are expanded click Severity, then in the far right drop down menu click Critical and Clear. By selecting both means we will send SNMP and to the Management Connector for both a Critical and Clear event.

Click Next to continue.

At Step 2 of 4 (Add Actions) we need to click + Add. This will define what actions run when an event matches this rule.

Under Conditions for actions, we leave this at the default where we always execute the actions.

Create Incident we leave blank as the system provided rule does this.

Send Notifications we leave blank unless we want to send an email, in our case no.
Under **Advanced Notifications** will be our pre-configured SNMPV1 and SNMPV3 entities. In our example, we click both.

We then scroll to the bottom of the page.

The **Submit Corrective Action** box would contain any pre-configured actions. Examples of these could be scripts to perform functions and run when an event comes in.

The **Forward to Event Connectors** box would contain any pre-configured Connectors.

To activate these, click on the **Available Connector** and then use the arrow keys to move them to the right under **Selected Connectors**. Once all is select click **Continue** then **Next** at Step 2 of 4.

We have an opportunity at Step 3 of 4 to change the system created rule name to something meaningful. The system will provide a rule such as "rule XX"; in our example, we change it to be meaningful to the rule. Click **Next** to continue.
Conclusion

This paper describes how to monitor an Oracle PCA including all the key components and discusses how to use Oracle Enterprise Manager Incident Rules. For further information on Oracle Enterprise Manager 13.3 refer here, and for further information on the Oracle Private Cloud Appliance 2.3 refer here.
Integrated Cloud Applications & Platform Services

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

How to Monitor Oracle Private Cloud Appliance with Oracle Enterprise Manager 13c

Author: Simon Hayler

Oracle is committed to developing practices and products that help protect the environment.