

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

ORACLE WHITE PAPER | JULY 2018

ORACLE®

Private Cloud
Appliance

13^c **ORACLE®**
Enterprise Manager



Introduction	2
Configuration of Oracle Enterprise Manager 13c to discover Oracle Private Cloud Appliance and embedded Oracle VM Manager	2
Monitoring the Oracle Private Cloud Appliance Rack	2
Configuring Incident Rules for Oracle Private Cloud Appliance	19
Incident Rules overview	19
Incident Rule for Warnings	20
Incident Rule for Oracle VM Server and ovs-agent down	22
Incident Rule for Oracle PCA Management Node Enterprise Manager Agent	24
Incident Rule to forward critical incidents via SNMP or Management Connector	24
Conclusion	29

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

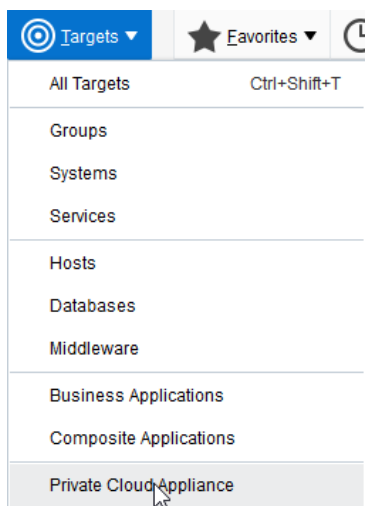
There are some configuration steps required to discover Oracle PCA and embedded Oracle VM Manager by Oracle Enterprise Manager. These steps involve configuration on both Oracle Enterprise Manager and the embedded Oracle VM Manager. The high-level steps are as follows:

- 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.

The Oracle logo, consisting of the word "ORACLE" in white, uppercase letters on a red rectangular background.

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.



Front

Empty Slot 42
 Empty Slot 41
 Empty Slot 40
 Empty Slot 39
 Empty Slot 38
 Empty Slot 37
 Empty Slot 36
 Empty Slot 35
 Empty Slot 34
 Empty Slot 33
 Empty Slot 32
 Empty Slot 31
 Empty Slot 30
 Empty Slot 29
 Empty Slot 28

PRIVATE CLOUD APPLIANCE

192.168.4.114	38°C
192.168.4.113	36°C
192.168.4.205	
192.168.4.200	
192.168.4.203	51°C
192.168.4.202	52°C
192.168.4.204	
192.168.4.112	35°C
192.168.4.111	36°C
192.168.4.110	36°C
192.168.4.109	36°C
192.168.4.108	37°C
192.168.4.107	37°C
192.168.4.106	37°C
192.168.4.105	36°C
192.168.4.104	36°C
192.168.4.103	36°C
192.168.4.2, 192.1...	
192.168.4.2	
192.168.4.1	

View Schematic
 Photo-Realistic
 Table

Zoom 100%
 50%

Label Target Name
 IP Address

Show Temperature
 Empty Slot

Status

- Up
- Down
- Blackout
- Locator Light

Component

- Server
- Switch
- InfiniBand Switch
- Disk Shelf

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.



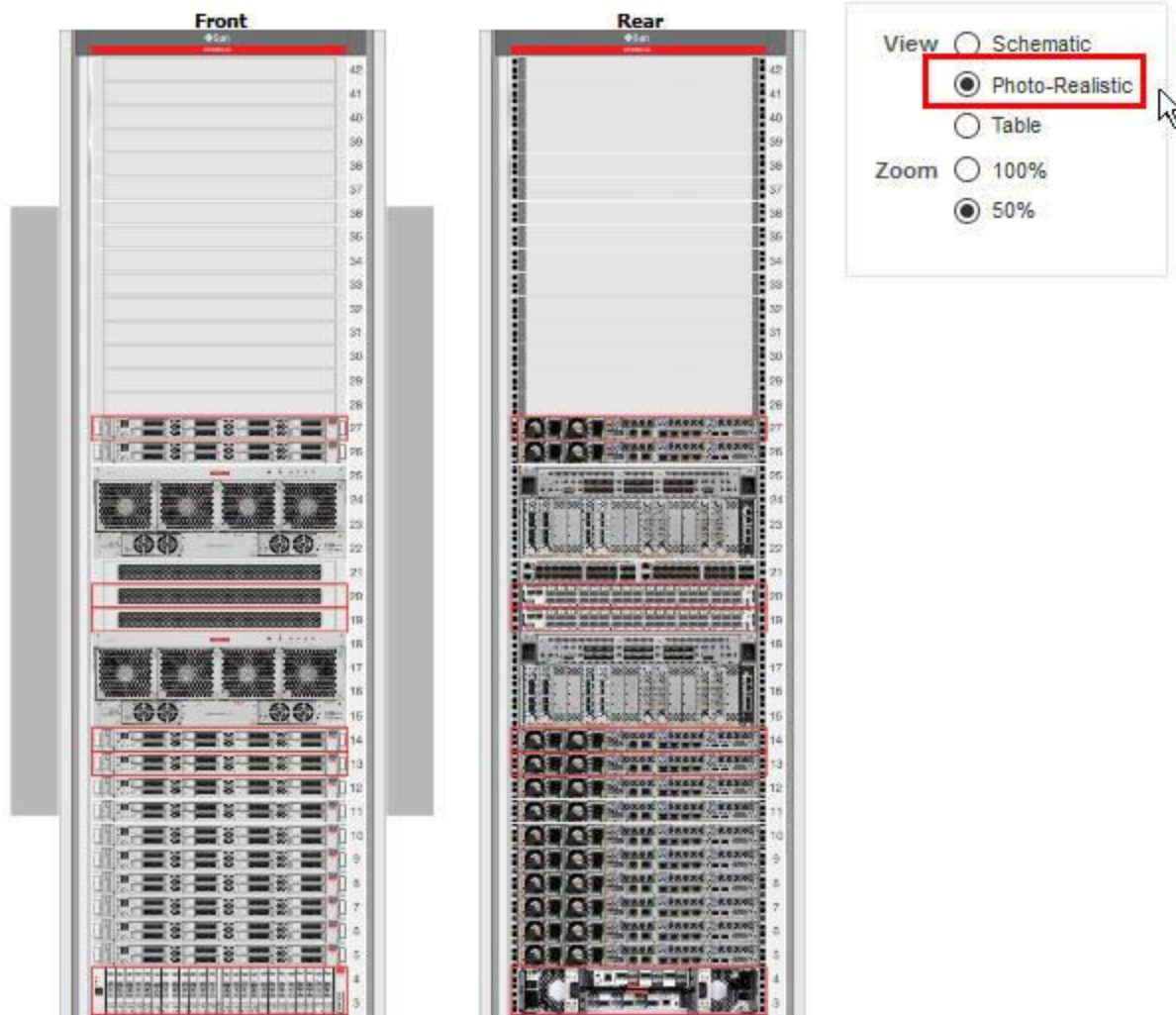


Table view provides the following; note the Incidents at the top of the page as well as a linked number (18) in our case for Infiniband Switches, which indicates critical (red circle with white cross) alerts.



Overview

Racks 1
Incidents 43 48 27 0

Oracle VM Manager PCA

PCA Rack Schematic

Slot Number	Component Name	Component Type	Status	Temperature		
27	itom-ovcaon27r1f	Server	Up	38°C		
26	itom-ovcaon26r1f	Server	Up	36°C		
22-25	ovcasw22r1f	Switch	Up			
21	ovcasw21r1f	Switch	Up			
20	ovcasw20r1f	InfiniBand Switch	Up	51°C	18	
19	ovcasw19r1f	InfiniBand Switch	Up	52°C	18	
15-18	ovcasw15r1f	Switch	Up			
14	itom-ovcaon14r1f	Server	Up	35°C		
13	itom-ovcaon13r1f	Server	Up	36°C		
12	itom-ovcaon12r1f	Server	Up	36°C		
11	itom-ovcaon11r1f	Server	Up	36°C		
10	itom-ovcaon10r1f	Server	Up	37°C		
9	itom-ovcaon09r1f	Server	Up	37°C		
8	itom-ovcaon08r1f	Server	Up	37°C		
7	itom-ovcaon07r1f	Server	Up	36°C		
6	itom-ovcamn06r1f	Server	Up	36°C		
5	itom-ovcamn05r1f	Server	Up	36°C		
3-4	ovcasn01r1f	Disk Shelf	Up			1
2	ovcasn02r1f	Server	Up			
1	ovcasn01r1f	Server	Up			

View Schematic Photo-Realistic Table

Show Empty Slot

Status

- Up
- Down
- Blackout

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](#).





Front

View Schematic
 Photo-Realistic
 Table

Zoom 100%
 50%

Target Details

ovcasw20r1/ [redacted]-pca1-vip.us.oracle.com
Oracle Data Center Infiniband Switch 36

Model: Sun Datacenter InfiniBand Switch 36
IP Address: 192.168.4.203

Incident Critical: ✖ 18

Component

- Server
- Switch
- InfiniBand Switch
- Disk Shelf

Blackout

Locator Light

PRIVATE CLOUD APPLIANCE

43
41
40
39
38
37
36
35
34
33
32
31
30
29
28
27
26
25
24
23
22
21
20
19
18
17
16
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1



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.

The screenshot shows the Oracle Enterprise Manager Cloud Control 13c interface. The main content area displays details for the target 'ilom-ovcasw20r1', which is a Sun Datacenter InfiniBand Switch 36. Key information includes IP: 192.168.4.203, Serial: AK00167554, and Part Number: 7052970. The 'Open Incidents' section shows 18 critical incidents. The 'Switch Throughput' section features a bar chart with data points: Highest (24.2KB/s), Average (6.6KB/s), and Average (3.5KB/s). Hardware views for the rear and front of the switch are shown below, with a red ring highlighting a port on the rear view.

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 'Target Details' dialog box for the IBPort[20] port displays the following information:

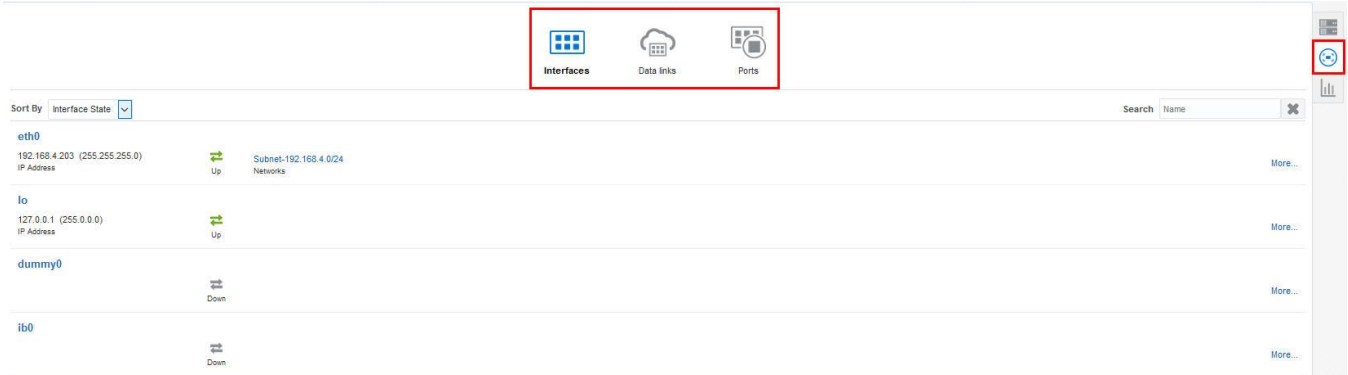
- ID: IBPort[20]
- Connector: 0A
- Type: Sw
- Peer: Data not available
- Peer Port: Data not available
- State: Available
- Errors: 0
- Throughput: 0
- Incident: Critical: 1

The main page for the IB switch is by default set to the hardware view.

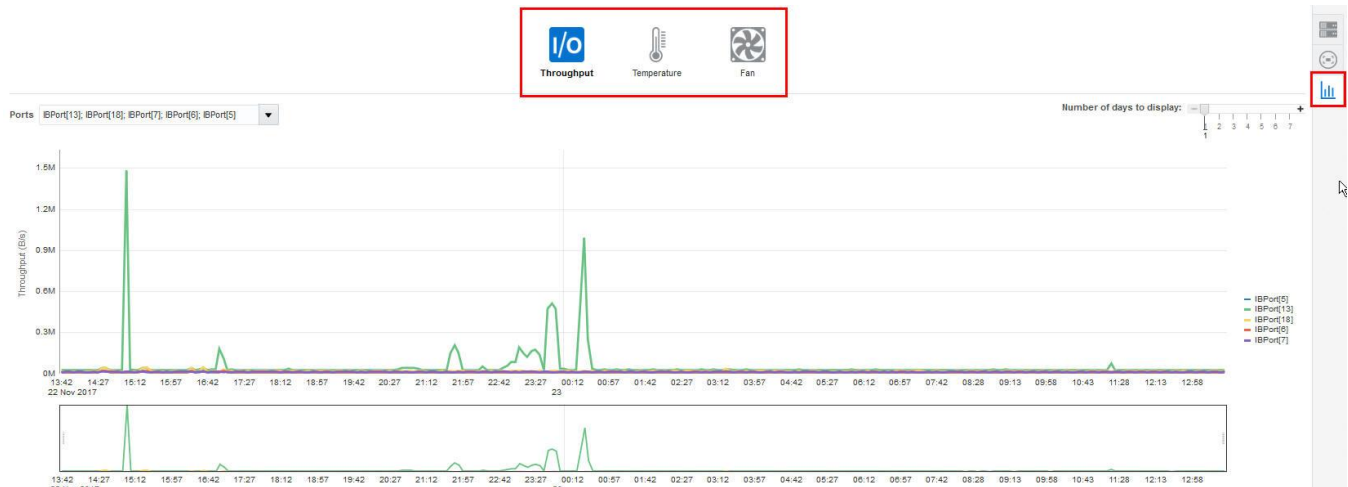


Two other options are available:

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 may be 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.





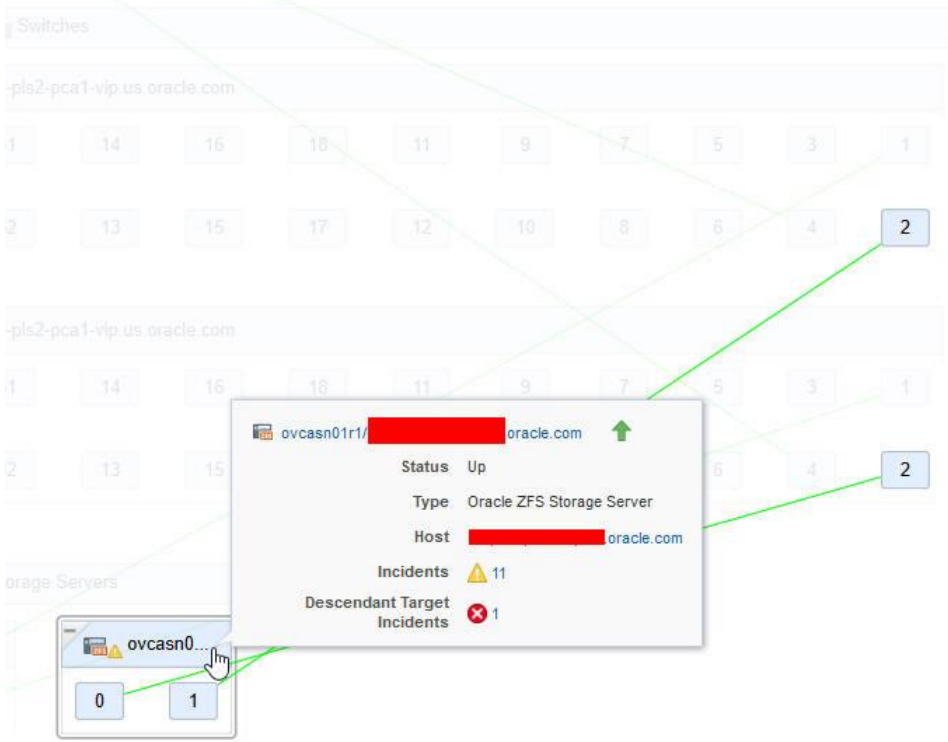
The screenshot shows the Oracle Enterprise Manager Cloud Control 13c interface. The top navigation bar includes 'Enterprise', 'Targets', 'Favorites', 'History', 'Setup', and 'CLOUDADM'. The main content area displays 'Open Incidents' (0 Fatal, 0 Critical, 0 Warning) and 'Ports Occupation' (32 Active, 40 Available, 28 Link types). A left-hand navigation pane is open, with 'Fabric Topology' highlighted under the 'Members' section. Below the navigation pane, there are sections for 'Incidents', 'Ports', and 'Nodes connected to the Fabric'.

From the target page main menu select **Fabric Topology**.

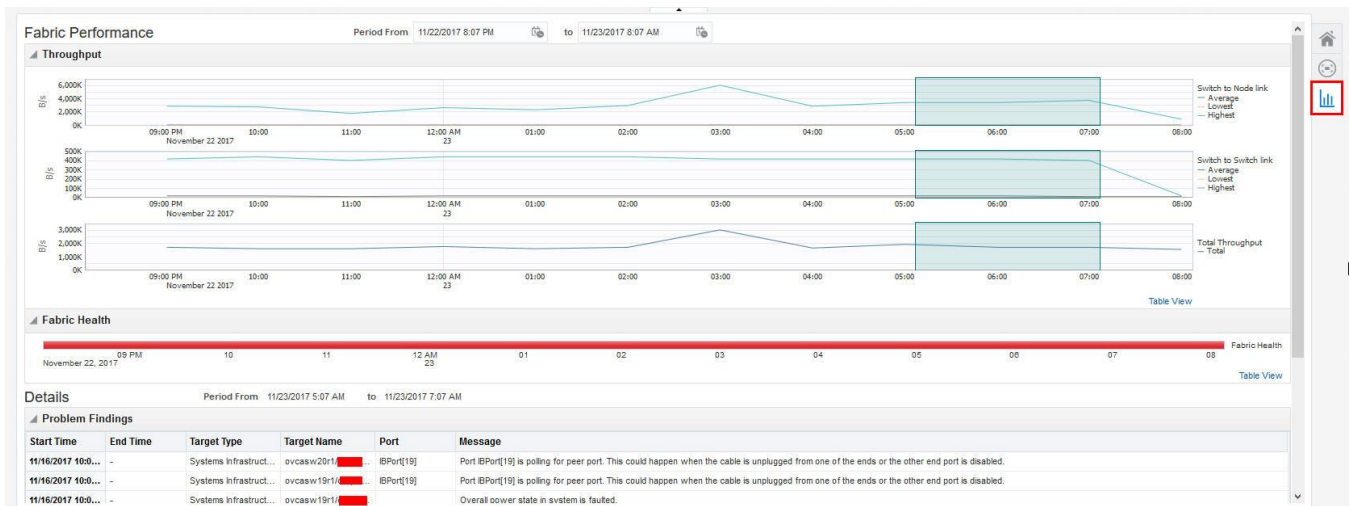
The screenshot shows the Oracle Enterprise Manager Cloud Control 13c interface displaying the Fabric Topology view. The main content area shows a network diagram with three main components: Servers, Switches, and Storage Servers. The Servers component includes a node named 'ilom-ovca...'. The Switches component includes two nodes: 'ovcasw20r1/...' and 'ovcasw19r1/...'. The Storage Servers component includes two nodes: 'ovcasn0...' and 'ovcasn0...'. Green lines represent connections between the Servers, Switches, and Storage Servers components. The top navigation bar and left-hand navigation pane are also visible.

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.

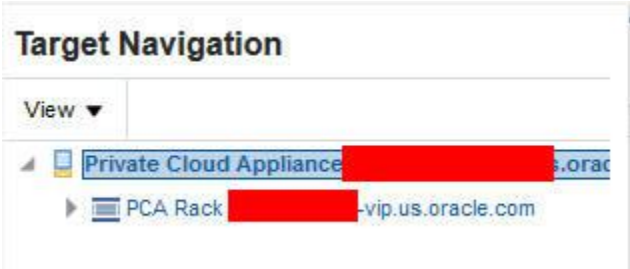


Returning to the Oracle PCA rack home page, we can expose a tabular view of all the components within the rack via the Target Navigation icon.

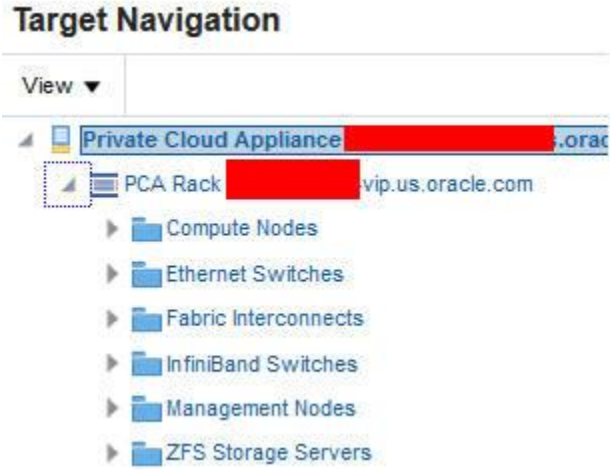




This exposes the top tiers of the Oracle PCA.



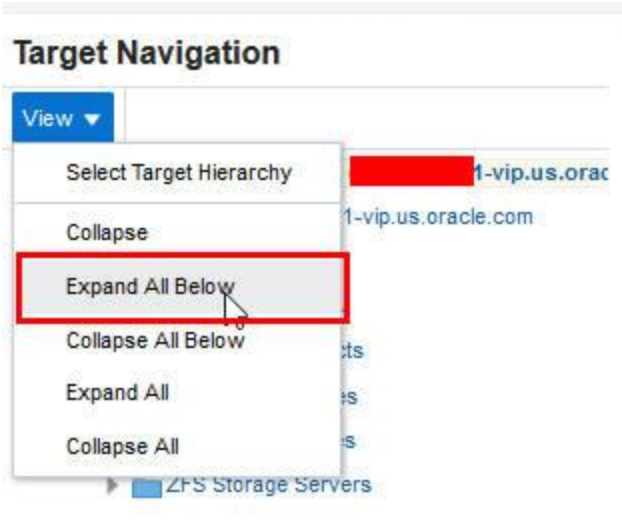
If we click on the > arrow this will expose the other main component areas of the Oracle PCA.



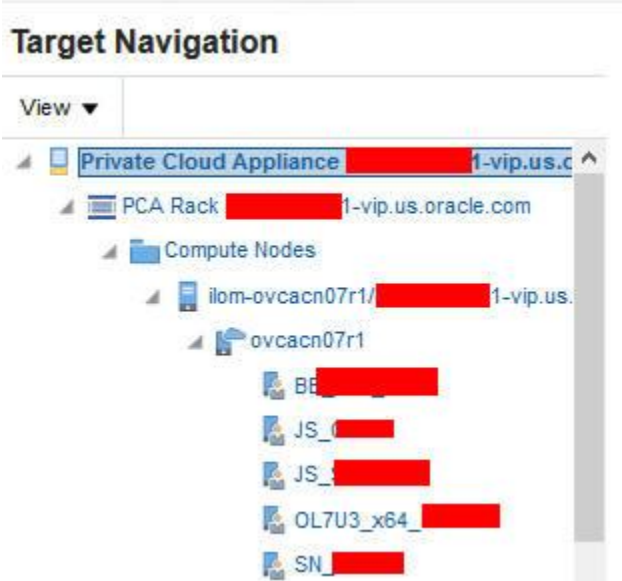
This is a useful and quick method of accessing component areas or separate components. All the component areas have home pages similar in concept to the switch and fabric pages shown earlier. For further details on these home pages, refer [here](#).

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.

Target Name	Target Type	Firmware Type	Firmware Version
ilom-ovcacn07r1f1-1-vip.us.oracle.com	Systems Infrastructure Server	Controller BIOS	3.29.00
ilom-ovcacn07r1f1-1-vip.us.oracle.com	Systems Infrastructure Server	Controller Firmware	2.130.373-2809
ilom-ovcacn07r1f1-1-vip.us.oracle.com	Systems Infrastructure Server	Disk Firmware	A600
ilom-ovcacn07r1f1-1-vip.us.oracle.com	Systems Infrastructure Server	Disk Firmware	A600
ilom-ovcacn07r1f1-1-vip.us.oracle.com	Systems Infrastructure Server	LOM Firmware	3.2.4.72
ilom-ovcacn07r1f1-1-vip.us.oracle.com	Systems Infrastructure Server	System	3.2.4.72
ilom-ovcacn07r1f1-1-vip.us.oracle.com	Systems Infrastructure Server	System BIOS	25010601 (pending: 25030100)
ilom-ovcacn08r1f1-1-vip.us.oracle.com	Systems Infrastructure Server	Controller BIOS	3.29.00
ilom-ovcacn08r1f1-1-vip.us.oracle.com	Systems Infrastructure Server	Controller Firmware	2.130.373-2809
ilom-ovcacn08r1f1-1-vip.us.oracle.com	Systems Infrastructure Server	Disk Firmware	A600
ilom-ovcacn08r1f1-1-vip.us.oracle.com	Systems Infrastructure Server	Disk Firmware	A600
ilom-ovcacn08r1f1-1-vip.us.oracle.com	Systems Infrastructure Server	LOM Firmware	3.2.4.72
ilom-ovcacn08r1f1-1-vip.us.oracle.com	Systems Infrastructure Server	System	3.2.4.72
ilom-ovcacn08r1f1-1-vip.us.oracle.com	Systems Infrastructure Server	System BIOS	25010601 (pending: 25030100)
ilom-ovcacn09r1f1-1-vip.us.oracle.com	Systems Infrastructure Server	LOM Firmware	3.2.4.72
ilom-ovcacn09r1f1-1-vip.us.oracle.com	Systems Infrastructure Server	System	3.2.4.72
ilom-ovcacn09r1f1-1-vip.us.oracle.com	Systems Infrastructure Server	System BIOS	25030100
ilom-ovcacn10r1f1-1-vip.us.oracle.com	Systems Infrastructure Server	LOM Firmware	3.2.4.72
ilom-ovcacn10r1f1-1-vip.us.oracle.com	Systems Infrastructure Server	System	3.2.4.72
ilom-ovcacn10r1f1-1-vip.us.oracle.com	Systems Infrastructure Server	System BIOS	25030100





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.



Incidents

View Category Capacity 0 10 0 0

Summary	Target	Severity	Status	Escalation Level	Type	Time Since Last Update
Oracle VM Server's used space for /OVS/Repositories/0004fb0000030000b034baa33fb6f599 is 87.6083984375%, crossed warning (70) or critical (80) threshold.		✖	New	-	Incident	7 days 19 hours
Oracle VM Server's used space for /OVS/Repositories/0004fb0000030000f3c4cee0549c5b3d is 94.3671875%, crossed warning (70) or critical (80) threshold.		✖	New	-	Incident	7 days 19 hours
Oracle VM Server's used space for /OVS/Repositories/0004fb0000030000f1ce156ef3349a511 is 94.3671875%, crossed warning (70) or critical (80) threshold.		✖	New	-	Incident	7 days 19 hours
Oracle VM Server's used space for /OVS/Repositories/0004fb0000030000f1ce156ef3349a511 is 94.3671875%, crossed warning (70) or critical (80) threshold.		✖	New	-	Incident	7 days 19 hours
Oracle VM Server's used space for /OVS/Repositories/0004fb0000030000b034baa33fb6f599 is 87.6083984375%, crossed warning (70) or critical (80) threshold.		✖	New	-	Incident	7 days 19 hours

Columns Hidden 14 Updated in the last 31 days

Incidents

View Category Fault 0 1 2 0

Summary	Target	Severity	Status	Escalation Level	Type	Time Since Last Update
Fault found in PSU 01 @ 2016-5-10 13:07:21. Description: A sensor indicates that the power supply '1320FIM401DPSU 01' is not operating properly due to some external condition Check to see if the power cord is...		✖	New	-	Incident	7 days 12 hours
Component fault or error in /SYS. FaultUUID of 39893ee4-cf6b-4ccf-c712-d1f35b6abe78 with certainty of 100.		⚠	New	-	Incident	7 days 23 hours
Component fault or error in /SYS. FaultUUID of 13cec6af-4012-c077-a4c1-93db5e3666b1 with certainty of 100.		⚠	New	-	Incident	7 days 23 hours

Columns Hidden 14 Updated in the last 31 days

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.





ORACLE Enterprise Manager Cloud Control 13c

ovcasw15r1

Fabric Interconnect

Status ↑ Up

Fabric Manager Version 4.3.1_OFM

HA Mode active

Servers

Name	Host OS	IO Profile Name	vHBAs	vNICs
ovcamn06r1	Linux/4.1.12-112.14.15.el6uek...	ovcamn06r1	4	4
ovcacn09r1	Linux/4.1.12-103.9.6.el6uekx8...	ovcacn09r1	4	4
ovcacn12r1	Linux/4.1.12-103.9.6.el6uekx8...	ovcacn12r1	4	4
ovcacn08r1	Linux/4.1.12-103.9.6.el6uekx8...	ovcacn08r1	4	4
ovcacn11r1	Linux/4.1.12-103.9.6.el6uekx8...	ovcacn11r1	4	4
ovcacn07r1	Linux/4.1.12-112.14.15.el6uek...	ovcacn07r1	4	4
ovcamn05r1	Linux/4.1.12-112.14.15.el6uek...	ovcamn05r1	4	4
ovcacn10r1	Linux/4.1.12-103.9.6.el6uekx8...	ovcacn10r1	4	4

Devices

Hostname	IP address	Model	Software Version	State
ovcasw15r1	192.168.4.204	VP780-CH-QDR	Build 3.9.0-XGOS - (root) Tue Dec ...	↑

IO Templates

Name	Description	vHBAs	vNICs
No data to display			

Storage Clouds

Name	Ports
Cloud_A	2
discovered-storage-cloud	8
Cloud_C	2
Cloud_D	2
Cloud_B	2

Network Clouds

Name	Lags	Ports
discovered-network-cloud	0	32
vm_public_vlan	0	4
vm_private	0	0
mgmt_public_eth	0	4
mgmt_pvi	0	0

Cumulative Performance

Incidents

Updated in last 7 days: 0

Breakdown of incidents updated in the last 7 days

Category	Availability	Performance	Security	Others
Availability	-	-	-	-
Performance	-	-	-	-
Security	-	-	-	-
Others	-	-	-	-

Problems

Total Open: 0

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).





ORACLE Enterprise Manager Cloud Control 13c

Enterprise Targets

ovcasw15r1 Fabric Interconnect

Page Refreshed Mar 29, 2018 12:42:51 AM GMT

All Metrics

Search

View

- ovcasw15r1
 - Alarms
 - Devices
 - IO Templates
 - Network Clouds
 - Response
 - Servers
 - Stats
 - Storage Cloud
 - Summary

Alarms
 Description : Fabric Interconnect Alarms
 Collection Schedule Every 5 Minutes
 Upload Interval Every Collection
 Last Upload Mar 29, 2018 12:31:08 AM GMT

DN	Chassis Name	Description	Detailed	Severity
system-ovcasw15r1.fault.process.restarted.pm-Process:alarm-system...	ovcasw15r1	The process ha...	num-restarts is 1;	4
system-ovcasw15r1.fault.iOPort.failed.equipment-IOPort:alarm-system...	ovcasw15r1	link lost	admin-state is ...	4
system-ovcasw15r1.fault.iOPort.failed.equipment-IOPort:alarm-system...	ovcasw15r1	link lost	admin-state is ...	4
system-ovcasw15r1.fault.iOPort.failed.equipment-IOPort:alarm-system...	ovcasw15r1	link lost	admin-state is ...	4
system-ovcasw15r1.fault.iOPort.failed.equipment-IOPort:alarm-system...	ovcasw15r1	link lost	admin-state is ...	4

Data shown in above table is collected in real time.

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.

ORACLE Enterprise Manager Cloud Control 13c

Enterprise Targets Favorites History Setup

Incident Rules - All Enterprise Rules

A rule set is a collection of rules that applies to a common set of objects, for example, targets, jobs, and templates. A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents, or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and creating tickets. Rule sets and rules are evaluated and applied in the order specified. You can change the order using the Reorder Rule Sets action.

Page Refreshed Nov 24, 2017 6:35:10 AM MST

Actions View Create Rule Set... View Edit... Delete... E-mail Import... Export... Simulate Rules Reorder Rule Sets... Search

Name	Description	Order	Enterprise Rule Set	Owner	Enable	Email Me	Last Updated On	Last Updated By
Incident management rule set for all targets	Rule set to create and manage incidents for all targets	1	✓	System Generat...	Yes	No	Oct 10, 2016 4:35:21 AM ...	
Event Management Rule set for Self Update	Rule set to manage Self Update events.	2	✓	System Generat...	Yes	No	Oct 10, 2016 4:35:22 AM ...	
OVM_Servpool_Repo_file_system		3	✓	OVMIPM	Yes	No	Nov 14, 2017 1:51:26 AM ...	CLOUDADM
PCA Agent		4	✓	CLOUDADM	Yes	No	Oct 19, 2017 3:50:35 AM ...	CLOUDADM
PCA_Rack_Warnings		5	✓	CLOUDADM	Yes	No	Nov 14, 2017 1:54:30 AM ...	CLOUDADM
PCA_Compute_Node_Down		6	✓	CLOUDADM	Yes	At lea...	Nov 24, 2017 5:18:09 AM ...	CLOUDADM
PCA_OVMM_MySQL		7	✓	CLOUDADM	Yes	At lea...	Nov 24, 2017 1:29:05 AM ...	CLOUDADM



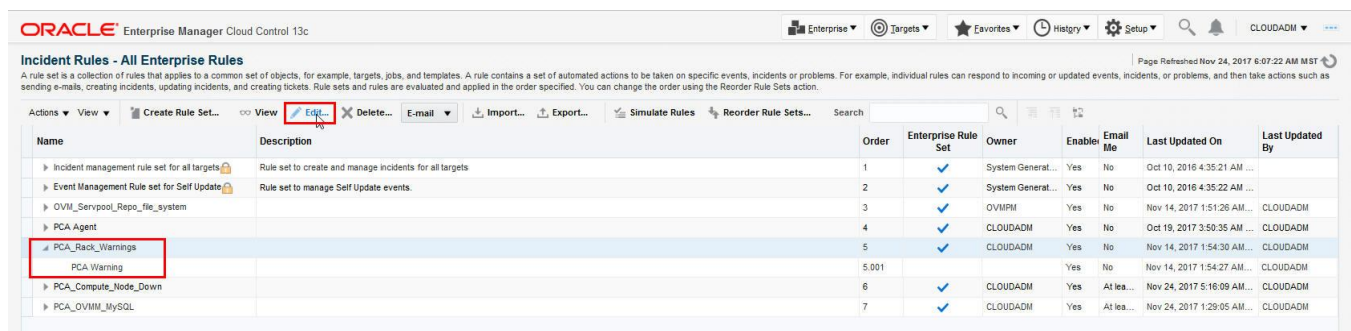
The following actions are available from an Incident Rule:

- 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.



ORACLE Enterprise Manager Cloud Control 13c

Incident Rules - All Enterprise Rules

A rule set is a collection of rules that applies to a common set of objects, for example, targets, jobs, and templates. A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents, or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and creating tickets. Rule sets and rules are evaluated and applied in the order specified. You can change the order using the Reorder Rule Sets action.

Page Refreshed Nov 24, 2017 6:07:22 AM MST

Name	Description	Order	Enterprise Rule Set	Owner	Enable	Email Me	Last Updated On	Last Updated By
Incident management rule set for all targets	Rule set to create and manage incidents for all targets	1	✓	System Generat...	Yes	No	Oct 10, 2016 4:35:21 AM ...	
Event Management rule set for Self Update	Rule set to manage Self Update events.	2	✓	System Generat...	Yes	No	Oct 10, 2016 4:35:22 AM ...	
OVIM_Servpool_Repo_file_system		3	✓	OVMFH	Yes	No	Nov 14, 2017 1:51:26 AM...	CLOUDADM
PCA Agent		4	✓	CLOUDADM	Yes	No	Oct 19, 2017 3:50:36 AM ...	CLOUDADM
PCA_Rack_Warnings		5	✓	CLOUDADM	Yes	No	Nov 14, 2017 1:54:30 AM...	CLOUDADM
PCA Warning		5.001			Yes	No	Nov 14, 2017 1:54:27 AM...	CLOUDADM
PCA_Compute_Node_Down		6	✓	CLOUDADM	Yes	At lea...	Nov 24, 2017 5:16:09 AM...	CLOUDADM
PCA_OVIMM_MySQL		7	✓	CLOUDADM	Yes	At lea...	Nov 24, 2017 1:29:05 AM...	CLOUDADM

We highlight the rule and then click edit.

ORACLE

Oracle Enterprise Manager Cloud Control 13c | CLOUDADM

Incident Rules - All Enterprise Rules

Edit Rule Set

A rule set is a collection of rules that applies to a common set of objects, for example, targets, jobs, and templates. A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents, or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and creating tickets.

* Name: (1)

Description:

Applies To: Targets

Enabled: (2)

Owner: CLOUDADM How is this used?

Type: Enterprise

Steps to define a Rule set

Provide Name, Description and Type
Enterprise rule sets represent business processes to manage events, incidents and problems. It allows all actions including create and update of incidents. Personal notification rule sets for rules to send e-mails to current user only.

Choose source - e.g., Targets, Jobs
Choose set of targets for the events, incidents or problems which would match the rules in the rule set. You can choose sources other than targets as well - e.g., Jobs.

Add Rules
Add rules to define specific conditions to match events, incidents or problems. Rules also identify the actions to be taken when the conditions match - e.g., e-mail, create incident.

Targets

Select targets to which this rule set applies. You can exclude specific targets from the scope - for example, all database targets except 'MyDevDB'.

All targets

All targets of types

Specific targets (3)

Add Groups (4)

Name	Type
PCA_OVM_Server_Pools	Group
PCA	Group

Excluded targets (5)

Name	Type
No target selected	

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

Item	Description
1	Give the Rule Set a unique and meaningful name
2	Enabled is yes
3	The rule can apply to all targets, types of targets or in our case specific targets
4	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 here
5	Here we can exclude any targets from the Rule Set. This may be useful if you have large numbers of targets within a group

Rules

A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents, or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and creating tickets. You can enable or disable a rule using the actions menu. Rules are evaluated and applied in the order specified. You can change the order using the Reorder Rule action. Any changes made to the rules are not saved until the 'Save' button is clicked.

Actions

Name	Description	Applies To	Action Summary	Enabled	Last Updated On	Last Updated By	Type
PCA Warning (1)	(2)	All Metric Alert events that match the following conditions: (3) • Severity is Warning	• Create Incident (4)	Yes (5)	Nov 14, 2017 1:54:27 AM MST (6)	CLOUDADM (7)	Events (8)

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

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

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.

ORACLE Enterprise Manager Cloud Control 13c

Incident Rules - All Enterprise Rules

A rule set is a collection of rules that applies to a common set of objects, for example, targets, jobs, and templates. A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents, or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and creating tickets. Rule sets and rules are evaluated and applied in the order specified. You can change the order using the Reorder Rule Sets action.

Name	Description	Order	Enterprise Rule Set	Owner	Enable	Email Me	Last Updated On	Last Updated By
Incident management rule set for all targets	Rule set to create and manage incidents for all targets	1	✓	System Generat...	Yes	No	Oct 10, 2016 4:35:21 AM ...	
Event Management Rule set for Self Update	Rule set to manage Self Update events.	2	✓	System Generat...	Yes	No	Oct 10, 2016 4:35:22 AM ...	
OVIM_Servpool_Repo_file_system		3	✓	OVMPM	Yes	No	Nov 14, 2017 1:51:26 AM ...	CLOUDADM
PCA_Agent		4	✓	CLOUDADM	Yes	No	Oct 19, 2017 3:50:35 AM ...	CLOUDADM
PCA_Rack_Warnings		5	✓	CLOUDADM	Yes	No	Nov 14, 2017 1:54:30 AM ...	CLOUDADM
PCA_Compute_Node_Down OVIM Server Down		6	✓	CLOUDADM	Yes	At lea...	Nov 24, 2017 5:16:09 AM ...	CLOUDADM
		6.001			Yes	Yes	Oct 12, 2017 12:07:37 P...	CLOUDADM
PCA_OVMM_MySQL		7	✓	CLOUDADM	Yes	At lea...	Nov 24, 2017 1:29:05 AM ...	CLOUDADM

ORACLE

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

Item	Description
1	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
2	Rules name
3	This Rule applies to the targets availability status
4	This is the action which in our case is to email the Cloudadm user

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**.

Incident Rules - All Enterprise Rules

A rule set is a collection of rules that applies to a common set of objects, for example, targets, jobs, and templates. A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and creating tickets. Rule sets and rules are evaluated and applied in the order specified. You can change the order using the Reorder Rule Sets action.

Name	Description	Order	Enterprise Rule Set	Owner	Enabled	Email Me	Last Updated On	Last Updated By
Incident management rule set for all targets	Rule set to create and manage incidents for all targets	1	✓	System Generat...	Yes	No	Oct 10, 2016 4:35:21 AM ...	
Event Management Rule set for Self Update	Rule set to manage Self Update events.	2	✓	System Generat...	Yes	No	Oct 10, 2016 4:35:22 AM ...	
OVMM_Servpool_Repo_file_system		3	✓	OVMPM	Yes	No	Nov 14, 2017 1:51:26 AM...	CLOUDADM
PCA Agent		4	✓	CLOUDADM	Yes	No	Oct 19, 2017 3:50:35 AM ...	CLOUDADM
PCA_Rack_Warnings		5	✓	CLOUDADM	Yes	No	Nov 14, 2017 1:54:30 AM...	CLOUDADM
PCA_Compute_Node_Down		6	✓	CLOUDADM	Yes	At lea...	Nov 24, 2017 5:16:09 AM...	CLOUDADM
PCA_OVMM_MySQL		7	✓	CLOUDADM	Yes	At lea...	Nov 24, 2017 1:29:05 AM...	CLOUDADM

Incident Rules - All Enterprise Rules

Create Rule Set

A rule set is a collection of rules that applies to a common set of objects, for example, targets, jobs, and templates. A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents, or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and creating tickets.

* Name: Send_Critical_to_SHMP_Connector (1)

Description: Rule set to send Oracle PCA alerts via SNMP and a Management Connector (2)

Applies To: Targets (3)

Enabled:

Owner: CLOUDADM

Type: Enterprise
 Personal Notification

Steps to define a Rule set

Provide Name, Description and Type
Enterprise rule sets represent business processes to manage events, incidents and problems. It allows all actions including create and update of incidents. Personal notification rule set is for rules to send e-mails to current user only.

Choose source - e.g., Targets, Jobs
Choose set of targets for the events, incidents or problems which would match the rules in the rule set. You can choose sources other than targets as well - e.g., Jobs.

Add Rules
Add rules to define specific conditions to match events, incidents or problems. Rules also identify the actions to be taken when the conditions match - e.g., e-mail, create incident.

Targets

Select targets to which this rule set applies. You can exclude specific targets from the scope - for example, all database targets except MyDev0B:

All targets

All targets of types (4)

Specific targets

Add Groups:

Name	Type
PCA	Group

Excluded targets

Name	Type
No target selected	

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

Item	Description
1	Give the Rule Set a unique and meaningful name..
2	Any meaningful description is helpful
3	This Rule Set applies to Targets, other choices are Job, Metric Extensions or Self Update
4	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.

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



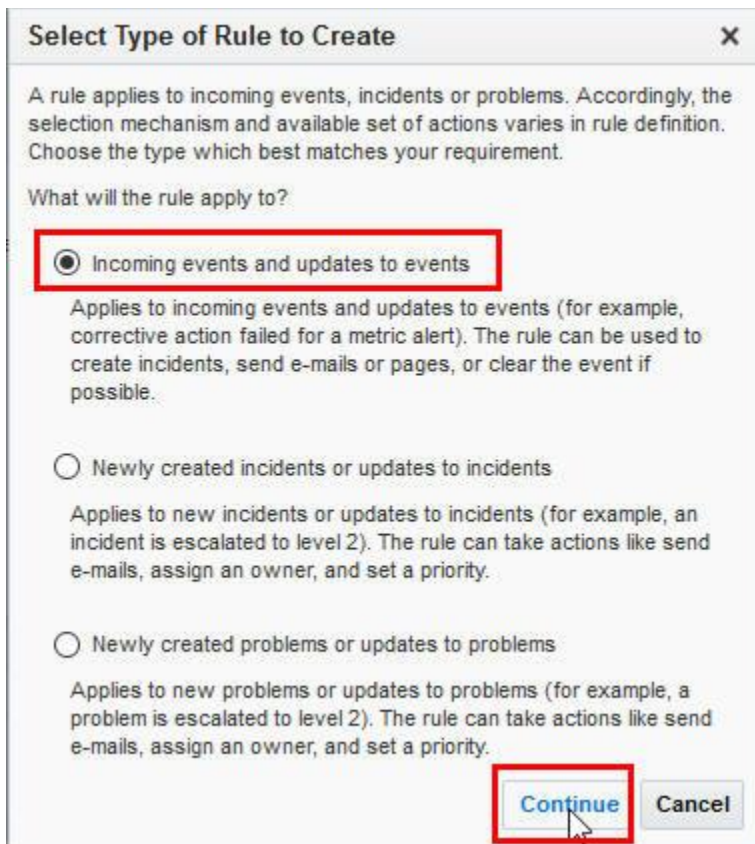
Rules

A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents, or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and creating tickets. You can enable or disable a rule using the actions menu. Rules are evaluated and applied in the order specified. You can change the order using the Reorder Rule action. Any changes made to the rules are not saved until the 'Save' button is clicked.

Actions ▾ View ▾ **Create...** Edit... Remove

Name	Description	Applies To	Action Summary	Enabled	Last Updated On	Last Updated By	Type
No data found							

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**.



Select Type of Rule to Create

A rule applies to incoming events, incidents or problems. Accordingly, the selection mechanism and available set of actions varies in rule definition. Choose the type which best matches your requirement.

What will the rule apply to?

Incoming events and updates to events

Applies to incoming events and updates to events (for example, corrective action failed for a metric alert). The rule can be used to create incidents, send e-mails or pages, or clear the event if possible.

Newly created incidents or updates to incidents

Applies to new incidents or updates to incidents (for example, an incident is escalated to level 2). The rule can take actions like send e-mails, assign an owner, and set a priority.

Newly created problems or updates to problems

Applies to new problems or updates to problems (for example, a problem is escalated to level 2). The rule can take actions like send e-mails, assign an owner, and set a priority.

Continue Cancel

The Create Rule Set wizard runs starting with Step1 of 4.

ORACLE

ORACLE Enterprise Manager Cloud Control 13c CLOUDADM

Create Rule Set - Send Critical to SNMP Connector

Progress: Select Events (1/4), Add Actions (2/4), Specify Name and Description (3/4), Review (4/4)

Create New Rule: Select Events

Type: Metric Alert (Info icon)

- All events of type Metric Alert
- Specific events of type Metric Alert

Advanced Selection Options

- Severity: In Critical Clear
- Target type
- Target Lifecycle Status
- Category
- Associated with incident
- Associated incident acknowledged
- Event name
- Total occurrence count
- Diagnostic incident
- Causal analysis update
- Comment added
- Corrective action completed

Buttons: Back, Step 1 of 4, **Next**, Cancel

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.

ORACLE Enterprise Manager Cloud Control 13c CLOUDADM

Add Actions

Add Conditional Actions

Define actions to be taken when an event matches this rule.

Conditions for actions
You can define the actions to apply whenever the rule matches or apply them conditionally.

- Always execute the actions
- Only execute the actions if specified conditions match

Create Incident or Update Incident
If there is no incident associated with the event, you could create one and optionally, set the incident owner and priority. If an incident exists, you could update the incident.

- Create Incident (if not associated with one)
- Update Incident

Send Notifications
Assign recipients for notifications. Recipients for the "To" list can only be added or removed in this section. Users who subscribe to this rule will be added to the "Cc" list; users who unsubscribe to this rule will be removed from the "Cc" list. You could specify multiple users separated by commas. Recipients could be Enterprise Manager users, direct E-mail address or [predefined variables](#).

Basic Notifications

E-mail To:

E-mail Cc:

Page:

Advanced Notifications
The "Manage Target Event" privilege is required to trigger advanced notification for targets.

Name	Description	Supports Repeat
<input checked="" type="checkbox"/> Simon_test_ESM (SNMPv1 Trap)	Simon's test ESM SNMPV1 Station	
<input checked="" type="checkbox"/> Myguest199 (SNMPv3 Trap)		

Buttons: Continue, Cancel

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.

Repeat Notifications

Both basic and advanced notifications can be sent repeatedly. The repeat notifications will stop only when one of the following conditions is met: The incident is acknowledged, the incident has cleared, or the maximum number of repeat notifications has been reached. Repeat notification is not supported for corrective action job status updates and causal analysis status updates on events.

Send Repeat notifications

Warning

Repeat notification is turned off globally. Even if you choose to get repeat notification from this rule, no repeat notification will be sent out until the capability is turned on in Notification Methods page (accessible by menu Setup > Notifications > Notification Methods)

Use global notification settings Use rule specific notification settings

Frequency (Minutes) 15

Maximum Repeat Notification 3

Submit Corrective Action

Select a corrective action to be run when rule conditions are met. Only one corrective action is allowed.

Corrective action will use preferred credentials of CLOUDADM (rule set owner) to execute scripts on respective targets.

Clear events

For most events, Enterprise Manager detects when the underlying issue is cleared and will generate a clear event. These types of events cannot be cleared using this option. However, for some events, such as metric alerts that are generated by mining a log file, it is not feasible for Enterprise Manager to detect when the underlying issue is cleared. This type of events must be manually cleared by administrators. This action can be used to automate this behavior.

Clear permanently

Forward to Event Connectors

Events can be forwarded to third party event management systems.

Available Connectors	Selected Connectors
	Test_Tivoli_Connector_dev(BM Tivoli Netcool/OMNibus Connector)

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.

ORACLE Enterprise Manager Cloud Control 13c

CloudADM

Create Rule Set - Send Critical to SNMP Connector

Select Events Add Actions Specify Name and Description Review

Create New Rule: Specify Name and Description

* Name SNMP_Connector

Description

Enter 1 or more characters.

Back Step 3 of 4 Next Cancel

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.



ORACLE Enterprise Manager Cloud Control 13c CLOUDADM

Create Rule Set - Send_Critical_to_SNMP_Connector

Select Events Add Actions Specify Name and Description **Review**

Create New Rule: Review Back Step 4 of 4 Next **Continue** Cancel

Please review your selections here, click "Back" if you need to modify the selections.

Selected Events
All Metric Alert events that match the following conditions:

- Severity In (Clear,Critical)

Actions

Order	Condition Summary	Action Summary
1	No additional condition specified	<ul style="list-style-type: none"> Call Simon_test_ESM Call Myguest199 Forward to event connector:Test_Tivoli_Connector_dev

Name and Description
Name: SNMP_Connector
Description:

At the Review page, click **Continue**, then **Save** to complete the Rule Set. The new Rule set will now appear in the main Rule Set page.

Name	Description	Order	Status	Environment	Created By	Created Date	Last Modified By
Send_Critical_to_SNMP_Connector	Rule set to send Oracle PCA alerts via SNMP and a Management Connector	8	✓	CLOUDADM	Yes	No	Nov 27, 2017 10:19:17 A... CLOUDADM

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](#).









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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

-  blogs.oracle.com/oracle
-  facebook.com/oracle
-  twitter.com/oracle
-  oracle.com

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.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0116

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

Integrated Cloud Applications & Platform Services

