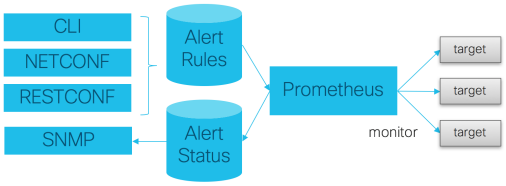
Notification and Alert

Architectural Overview

A Cisco Policy Suite (CPS) vDRA deployment comprises multiple virtual machines (VMs) with multiple running containers deployed for scaling and high availability (HA) purposes. The monitoring and alerting system of the CPS vDRA deployment is centered around alert definition, metric gathering, and SNMP trap forwarding. The high-level architecture is shown below:

Figure 1: High-Level Architecture



Major Components

Alert Definition

Alert definition occurs when an end user (or external system) configures the system via CLI, NETCONF, or RESTCONF interfaces with Alert rules. The system takes these alert rules and pushes the definitions into the

Prometheus processes running within the cluster. The system does not provide a fixed set of alerts but provides a sample list of common alerts an operator may want to configure.

Metric Gathering

At the core of the alerting framework, the system runs multiple Prometheus processes (http://prometheus.io) which monitors the system and track metrics which can be used for triggering alerts. The default Prometheus instance that monitors the system tracks metrics at a 5 second interval for 24 hours.

SNMP Trap Forwarding

Once an alert is triggered the Prometheus server forwards that alert to the active control/Cluster Manager node. These alerts are forwarded based on configuration to external NMS systems using either SNMPv2 or SNMPv3.

Technical Architecture

Cisco Policy Suite is deployed as a distributed virtual appliance. The standard architecture uses Hypervisor virtualization. Multiple hardware host components run Hypervisors and each host runs several virtual machines. Within each virtual machine, one-to-many internal CPS components can run. CPS monitoring and alert notification infrastructure simplifies the virtual physical and redundant aspects of the architecture.

Protocols

The CPS monitoring and alert notification infrastructure provides a simple standards-based interface for network administrators and NMS (Network Management System). SNMP is the underlying protocol for all alert notifications. Standard SNMP notifications (traps) are used throughout the infrastructure.

Alerts are triggered from either the Cluster Manager or Control virtual machines if the Cluster Manager is not active.

SNMP Object Identifier and Management Information Base

Cisco has a registered private enterprise Object Identifier (OID) of 26878. This OID is the base from which all the aggregated CPS metrics are exposed at the SNMP endpoint. The Cisco OID is fully specified and made human-readable through a set of Cisco Management Information Base (MIB-II) files.

The current MIBs are defined as follows:

Table 1: MIBs

MIB Filename	Purpose
BROADHOP-MIB.mib	Defines the main structure include structures and codes.
BORADHOP-NOTIFICATION-MIB.mib	Defines Notifications/Traps available.

SNMP Notifications

SNMP Notifications in the form of traps (one-way) are provided by the infrastructure. CPS notifications do not require acknowledgments. The traps provide both:

- Proactive alerts that the predetermined thresholds have been passed. For example, a disk is nearing capacity or CPU load is too high.
- Reactive alerting when system components fail or are in a degraded state. For example, a process died or network connectivity outage has occurred.

Notifications and traps are categorized by a methodology similar to UNIX System Logging (syslog) with both Severity and Facility markers. All event notifications (traps) contain these markers.

- Facility
- Severity
- Source (device name)
- Device time

These objects can be used to identify where the issue lies and the Facility (system layer) and the Severity (importance) of the reported issue.

Facility

The generic syslog facility has the following definitions:

Note Facility defines a system layer starting with physical hardware and progressing to a process running in a particular application.

Table 2: Syslog Facility

Number	Facility	Description
0	Hardware	Physical Hardware - Servers SAN NIC Switch and so on
1	Networking	Connectivity in the OSI (TCP/IP) model
2	Virtualization	VMware ESXi (or other) virtualization
3	Operating System	Linux OS
4	Application	Application (CPS Session Manager, CPS Binding Database, and so on)
5	Process	Specific process

There may be overlaps in the Facility value as well as gaps if a particular SNMP agent does not have full view into an issue. The Facility reported is always shown as viewed from the reporting SNMP agent.

Severity

In addition to Facility each notification has a Severity measure. The defined severities are directly from UNIX syslog and defined as follows:

Table 3: Severity Levels

Number	Severity	Description
0	Emergency	System is unusable.
1	Alert	Action must be taken immediately.
2	Critical	Critical conditions.
3	Error	Error conditions.
4	Warning	Warning conditions.
5	Notice	Normal but significant condition.
6	Info	Informational message.
7	Debug	Lower level debug message.
8	None	Indicates no severity.
9	Clear	The occurred condition has been cleared.

For the purposes of the CPS Monitoring and Alert Notifications system, Severity levels of Notice Info and Debug are usually not used.

Warning conditions are often used for proactive threshold monitoring (for example, Disk usage or CPU Load) which requires some action on the part of administrators but not immediately.

Conversely, Emergency severity indicates that some major component of the system has failed and that either core policy processing session management or major system functionality is impacted.

Categorization

Combinations of Facility and Severity create many possibilities of notifications (traps) that might be sent. However, some combinations are more likely than others. The following table lists some Facility and Severity categorizations:

Table 4: Severity Categorization

Facility.Severity	Categorization	Possibility
Process.Emergency	A single part of an application has failed.	Possible but in an HA configuration very unlikely.
Hardware.Debug	A hardware component has sent a NA debug message.	NA

Facility.Severity	Categorization	Possibility
Operating System.Alert	An Operating System (kernel or resource level) fault has occurred.	Possible as a recoverable kernel fault (on a vNIC for instance).
Application.Emergency	An entire application component has failed.	Unlikely but possible (load balancers failing for instance).

It is not possible to quantify every Facility and Severity combination. This is primarily driven by the fact that the alert rules can be configured to meet each operator's environment. However, greater experience with CPS leads to better diagnostics. The CPS Monitoring and Alert Notification infrastructure provides a baseline for event definition and notification by an experienced engineer.

Emergency Severity Note

Caution Emergency severities are very important! As a general principle, alerts should only be defined with an Emergency-severity trap if the system becomes inaccessible or unusable in some way. An unusable system is rare but might occur if multiple failures occur in the operating system virtualization networking or hardware facilities.

Notifications and Alerting

The CPS Monitoring and Alert Notification framework provides the following SNMP notification traps (one-way). Traps are either proactive or reactive. Proactive traps are alerts based on system events or changes that require attention (for example, Disk is filling up). Reactive traps are alerts that an event has already occurred (for example, an application process failed).

Component Notifications

Components are devices that make up the CPS system. These are systems level traps. They are generated when some predefined thresholds is crossed and are defined in the alerting configuration of the system. User can modify and change these using the alert definition commands.

Component notifications are defined in the BROADHOP-NOTIFICATION-MIB as follows:

```
 broadhopQNSComponentNotification NOTIFICATION-TYPE OBJECTS {
   broadhopComponentName,
   broadhopComponentTime,
   broadhopComponentNotificationName,
   broadhopNotificationFacility,
   broadhopNotificationSeverity,
   broadhopComponentAdditionalInfo }
STATUS current
DESCRIPTION "
Trap from any QNS component - i.e. device.

"
::= { broadhopProductsQNSNotifications 1 }
```

Each Component Notification contains:

- Name of the Notification being thrown (broadhopComponentNotificationName)

- Name of the device throwing the notification (broadhopComponentName)
- Time the notification was generated (broadhopComponentTime)
- Facility or which layer the notification came from (broadhopNotificationFacility)
- Severity of the notification (broadhopNotificationSeverity)
- Additional information about the notification, which might be a bit of log or other information.

The following table provides the list of supported alarms:

Table 5: Component Notifications

Notification Name	Severity	Message Text	Description
DISK_FULL	Critical	Disk filesystem / usage is more than the 90%	Disk usage is monitored.
	Clear	Disk filesystem / usage is greater than 10%	
HIGH_LOAD	Major	load average value for 5 min is greater than 3 current value is {{ $value }}	Load on the CPU is measured as per the linux operating system load.
	Clear	load average value for 5 min is lower than 3	
LINK_STATE	Critical	{{ $labels.interface }} is down on {{ $labels.instance }}	Indicates if any interface (ens***) has gone down.
	Clear	{{ $labels.interface }} is up on {{ $labels.instance }}	
LOW_MEMORY	Critical	Available RAM is less than 80% current value is {{ $value }}	Monitors memory usage on the VMs. When free memory goes down, the threshold alarm is raised.
	Clear	Available RAM is more than 80%	
PROCESS_STATE	Critical	{{ $labels.service_name }} instance {{ $labels.module_instance }}of module {{ $labels.module }} is in Aborted state.	Monitors process restarts.
	Clear	{{ $labels.service_name }} instance {{ $labels.module_instance }}of module {{ $labels.module }} is moved from Aborted state	
HIGH_CPU_USAGE	Critical	CPU usage in last 10 sec is more than 30% current value {{ $value }}	Monitors CPU usage.
	Clear	CPU usage in last 10 sec is lower than 30%	

Notification Name	Severity	Message Text	Description
QNS_JAVA_STARTED	Error	{{ $labels.service_name }} instance {{ $labels.module_instance }} of module {{ $labels.module }} is in Started state.	Indicates Java process restart.
	Clear	{{ $labels.service_name }} instance {{ $labels.module_instance }} of module {{ $labels.module }} is moved from started state	
IP_NOT_REACHABLE	Critical	VM/VIP IP {{$labels.instance }} is not reachable	When IP is not reachable, this alarm is raised.
	Clear	VM/VIP IP {{$labels.instance }} is reachable	
DIAMETER_PEER_DOWN	Error	Diameter peer is down.	Any peer connected to PAS is monitored.
	Clear	Diameter peer is up	
DRA_PROCESS_UNHEALTHY	Critical	{{ $labels.service_name }} instance {{ $labels.module_instance }} of module {{ $labels.module }} is not healthy	Process state is monitored.
	Clear	{{ $labels.service_name }} instance {{ $labels.module_instance }}of module {{ $labels.module }} is healthy	
DB_SHARD_DOWN	Critical	All DB Members of a replica set {{ $labels.shard_name }} are down	Alarm raised when both primary and secondary replica set members are down.
	Clear	All DB Members of a replica set {{ $labels.shard_name }} are not down	
NO_PRIMARY_DB	Critical	Primary DB member not found for replica set {{ $labels.shard_name }}	Alarm raised when primary database is not up.
	Clear	Primary DB member found for replica set {{ $labels.shard_name }}	
SECONDARY_DB_DOWN	Critical	Secondary Member {{ $labels.name }} of replica set {{ $labels.shard_name }} is down	Alarm raised when secondary database is not up.
	Clear	Secondary Member {{ $labels.name }} of replica set {{ $labels.shard_name }} is up	
LOW_SWAP	Critical	{{ $labels.instance }} has less than 80% swap memory .	Monitors the swap memory.
	Clear	{{ $labels.instance }} has greater than 80% swap memory .	

Note By default, no alert rules are configured in the system.

Application Notifications

The following table describes the application notifications:

Table 6: Application Notifications

Notification Name	Severity	Message Text	Description
DRA_MESSAGE_ PROCESSING_FAILURE_ TPS_EXCEEDED	Critical	Message Processing Failure TPS exceeded, current value is {{ $value }}.	TPS of rejected messages from DRA Director (Any messages with Result code !=2001)
	Clear	Message Processing Failure TPS in control.	
DRA_DIRECTOR_ TPS_EXCEEDED	Critical	{{ $labels.instance }} Director TPS exceeded, current value is {{ $value }}.	Success TPS of Total DRA Director (ResultCode=2001)
	Clear	{{ $labels.instance }} Director TPS in control .	
DRA_WORKER_ TPS_EXCEEDED	Critical	{{ $labels.instance }} Worker TPS exceeded, current value is {{ $value }}.	TPS of Total Worker
	Clear	{{ $labels.instance }} Worker TPS in control.	
DRA_DB_ TPS_EXCEEDED	Critical	{{ $labels.instance }} Persistence DB TPS exceeded , current value is {{ $value }}.	TPS of DB TPS (Query and Update)
	Clear	{{ $labels.instance }} Persistence DB TPS in control.	
DIAMETER_UNABLE _TO_DELIVER_ TPS_EXCEEDED	Critical	UNABLE_TO_DELIVER TPS exceeded, current value is {{ $value }}.	TPS of Diameter 3002
	Clear	UNABLE_TO_DELIVER in control.	
DIAMETER_TRANSIENT _FAILURE_TPS_ EXCEEDED	Critical	TRANSIENT_FAILURE TPS exceeded, current value is {{ $value }}.	TPS of Diameter 4xxx
	Clear	TRANSIENT_FAILURE in control.	
DIAMETER_UNKNOWN _SESSIONS_TPS _EXCEEDED	Critical	UNKNOWN_SESSIONS TPS exceeded, current value is {{ $value }}.	TPS of Diameter 5002
	Clear	UNKNOWN_SESSIONS in control.	

Notification Name	Severity	Message Text	Description
MISMATCH_REQUEST _RESPONSE	Critical	{{ $labels.remote_peer }} MISMATCH_REQUEST _RESPONSE exceeded, current value is {{ $value }}.	Mismatch in Rate of Request and Response (Discrepancy in ingress and egress)
	Clear	{{ $labels.remote_peer }} MISMATCH_REQUEST _RESPONSE in control.	
KEEP_ALIVE_RAR _ROUTING_FAILURE_ TPS_EXCEEDED	Critical	Keep Alive RAR TPS exceeded, current value is {{ $value }}.	TPS of Keep Alive RAR Routing (Stale RAR)
	Clear	Keep Alive RAR TPS in control.	
EGRESS_RATE_ LIMITED_SESSION_ ERR_RESP_TPS_ EXCEEDED	Critical	{{ $labels.local_peer }} {{ $labels.remote_peer }} Egress rate limited messages with error response TPS exceeded, current value is {{ $value }}.	TPS of Rate Limited Response for Error
	Clear	{{ $labels.local_peer }} {{ $labels.remote_peer }} Egress rate limited messages with error response TPS in control.	
EGRESS_RATE_ LIMITED_SESSION_ REJECT_TPS_ EXCEEDED	Critical	{{ $labels.local_peer }} {{ $labels.remote_peer }} Egress rate limited messages dropped without error TPS exceeded, current value is {{ $value }}.	TPS of Rate Limited Response Rejected
	Clear	{{ $labels.local_peer }}{{ $labels.remote_peer }} Egress rate limited messages dropped without error TPS in control.	
INGRESS_RATE_ LIMITED_SESSION_ ERR_RESP_TPS_ EXCEEDED	Critical	{{ $labels.local_peer }} {{ $labels.remote_peer }} Ingress rate limited messages with error response TPS exceeded, current value is {{ $value }}.	TPS of Rate Limited Response Error - Ingress
	Clear	{{ $labels.local_peer }}{{ $labels.remote_peer }} Ingress rate limited messages with error response TPS in control.	

Notification Name	Severity	Message Text	Description
INGRESS_RATE_ LIMITED_SESSION_ REJECT_TPS_ EXCEEDED	Critical	{{ $labels.local_peer }} {{ $labels.remote_peer }} Ingress rate limited messages dropped without error response TPS exceeded, current value is {{ $value }}.	TPS of Rate Limited Response Rejected - Ingress
	Clear	{{ $labels.local_peer }}{{ $labels.remote_peer }} Ingress rate limited messages dropped without error response TPS in control.	
BINDING_STORAGE _ERRORS_TPS_ EXCEEDED	Critical	Binding Store Error TPS exceeded, current value is {{ $value }}.	TPS Binding Storage Errors (Binding storage failed because of high load/any other database error)
	Clear	Binding Store Error TPS in control.	
BINDING_LOOKUP_ ERROR_TPS_ EXCEEDED	Critical	Binding Lookup Error TPS exceeded, current value is {{ $value }}.	TPS Binding Lookup Errors (Binding retrieval failure because of internal error)
	Clear	Binding Lookup Error TPS in control.	
DB_ERR_ TPS_EXCEEDED	Critical	All DB Errors TPS exceeded, current value is {{ $value }}.	TPS All database errors
	Clear	All DB Errors TPS in control.	
DB_RESPONSE_ TIME_EXCEEDED	Critical	{{ $labels.instance }} DB Response Time exceeded, current value is {{ $value }}.	Response Time Exceeds (Database Query/Update operation time exceeds)
	Clear	{{ $labels.instance }} DB Response Time in control, current value is {{ $value }}.	
BINDING_KEY_ NOT_FOUND_IN_ AAR_TPS_ EXCEEDED	Critical	{{ labels.origin_host }} Binding Key not found in AAR TPS exceeded, current value is {{ $value }}.	TPS Binding Key Not Found in AAR (When AAR received with no "imsi+apn/msisdn/ipv6")
	Clear	{{ labels.origin_host }} Binding Key not found in AAR TPS in control.	
BINDING_KEY_ NOT_FOUND_IN_ CCR_I_TPS_ EXCEEDED	Critical	{{ labels.origin_host }} Binding Key not found in CCR(I) TPS exceeded, current value is {{ $value }}.	TPS Binding Key Not Found in CCR-I(When CCR-I received with no "imsi+apn/msisdn/ipv6"
	Clear	{{ labels.origin_host }} Binding Key not found in CCR(I) TPS in control.	
BINDING_NOT _FOUND_TPS_ EXCEEDED	Critical	{{ labels.origin_host }} Binding not found TPS exceeded, current value is {{ $value }}.	TPS Binding Not Found
	Clear	{{ labels.origin_host }} Binding not found TPS in control,.	

Notification Name	Severity	Message Text	Description
BINDING_DB_ INCONSISTENT_ TPS_EXCEEDED	Critical	TPS AAR with Result Code 5065 exceeded, current value is {{ $value }}.	TPS AAR with Result Code 5065
	Clear	TPS AAR with Result Code 5065 in control.	
BINDING_SESSION _DB_SIZE_ EXCEEDED	Critical	{{ $labels.db }} size exceeded, current value is {{ $value }}.	Total Size of Session DB Exceeded
	Clear	{{ $labels.db }} size in control.	
BINDING_IMSI_ APN_DB_SIZE _EXCEEDED	Critical	{{ $labels.db }} size exceeded, current value is {{ $value }}.	Total Size of IMSI / APN DB Exceeded
	Clear	{{ $labels.db }} size in control.	
BINDING_MSISDN _APN_DB_SIZE _EXCEEDED	Critical	{{ $labels.db }} size exceeded, current value is {{ $value }}.	Total Size of MSISDN / APN DB Exceeded
	Clear	{{ $labels.db }} size in control	
BINDING_IPV6 _DB_SIZE_ EXCEEDED	Critical	{{ $labels.db }} size exceeded, current value is {{ $value }}.	Total Size of IPv6 DB Exceeded
	Clear	{{ $labels.db }} size in control	
PEER_TPS _EXCEEDED	Critical	{{ $labels.instance }} Peer Connection {{ $labels.local_peer}} {{ $labels.remote_peer }} TPS exceeded, current value is {{ $value }}.	Peer TPS Exceeded (Per peer TPS thresholds)
	Clear	{{ $labels.instance }} Peer Connection {{ $labels.local_peer}} {{ $labels.remote_peer }} TPS in control.	
NO_RESPONSE_ PEER_FOR_ ANSWER_TPS _EXCEEDED	Critical	{{ $labels.instance }} No Response From Peer Connection TPS exceeded for {{ $labels.message_type}} , current value is {{ $value }}.	TPS No Response From Peer (timeouts from PCRF/any peer)
	Clear	{{ $labels.instance }} No Response From Peer Connection TPS in control for {{ $labels.message_type}} .	
PEER_RESPONSE _TIME_EXCEEDED	Critical	message_duration_seconds {type=~"peer_.*"} [labels: type]	Peer Response Time Exceeded (Response time of peer exceeds)
	Clear	Response time in control.	
NO_PEER_GROUP _MEMBER _AVAILABLE	Critical	{{ $labels.peer_group }} not available.	Peer Group is not Available (All peers in peer_group down)
	Clear	{{ $labels.peer_group }} available.	

Notification Name	Severity	Message Text	Description
PCRF_NOT_CREATING _SESSIONS_TPS _EXCEEDED	Critical	Failed CCR-I TPS exceeded, current value is {{ $value }}.	TPS Rate of Failed CCR-I(ResultCode !=2001)
	Clear	Failed CCR-I TPS in control.	
FORWARDING_LOOP _FOUND_TPS _EXCEEDED	Critical	{{ $labels.remote_peer}} Loop Detected TPS exceeded , current value is {{ $value }}.	TPS Rate of Diameter Message Loop
	Clear	{{ $labels.remote_peer }} Loop Detected TPS in control.	
RELAY_LINK _TPS_GT_0	Critical	{{ $labels.remote_peer}} Relay Started, current value is {{ $value }}.	TPS Rate of Relay Peer > 0 (When relay peers start exchanging control plane messages)
	Clear	{{ $labels.remote_peer}} Relay Stated.	
RELAY_LINK _TPS_EXCEEDED	Critical	{{ $labels.remote_peer}} Relay Link TPS exceeded, current value is {{ $value }}.	TPS Rate of Relay Peer (TPS of relay messages)
	Clear	{{ $labels.remote_peer}} Relay Link TPS in control.	
RELAY_LINK _STATUS	Critical	{{ $labels.remote_peer }} Relay Link is Down.	Relay Link is Down (Relay link status is monitored)
	Clear	{{ $labels.remote_peer}} Relay Link is UP.	
NO_RELAY_PEER _TPS_EXCEEDED	Critical	{{ $labels.remote_peer}} Relay Peer TPS exceeded, current value is {{ $value }}.	TPS Rate of Relay Peer Failure
	Clear	{{ $labels.remote_peer}} Relay Peer TPS in control.	

Alert Rules

Alert Rules Configuration

The following commands are used to configure alert rules:

```
scheduler#config
scheduler(config)# alert rule <rule_name>
```

where, <*rule_name*> is the name of the alert rule. For example, test

```
Value for 'expression' (<string>): <expression based on the stats>
```

where, <*expression based on the stats*> is the expression. For example, test>1

```
Value for 'message' (<string>): <message string to be sent in the alarm message>
```

where, <*message string to be sent in the alarm message*> is the message to be sent in the alarm. For example, testing

```
Value for 'snmp-clear-message' (<string>): <message string for clear alarm>
```

where, <*message string for clear alarm*> is the string for the clear message. For example. test clear

```
scheduler(config-rule-test)#
scheduler(config-rule-test)# snmp-facility
Possible completions:
  application  hardware  networking  os  proc  virtualization

scheduler(config-rule-test)# snmp-facility <SNMP facility to be provided for this alert>
```

where, <*SNMP facility to be provided for this alert*> is the facility to be provided for this alert. For example, application

```
scheduler(config-rule-test)# event-host-label <provide the node details>
```

where, <*provide the node details*> is used to provide node details. For example, instance

```
scheduler(config-rule-test)# snmp-severity
Possible completions:
  alert  critical  debug  emergency  error  info  none  notice  warning

scheduler(config-rule-test)# snmp-severity <SNMP severity to be send for this alert>
```

where, <*SNMP severity to be send for this alert*> is the severity level to be used for alert rule. For example, critical

```
scheduler(config-rule-test)# duration <time>
```

where, <*time*> causes Prometheus to wait for a certain duration between first encountering a new expression output vector element (like, an instance with a high HTTP error rate) and counting an alert as firing for this element. Elements that are active, but not firing yet, are in pending state.

```
scheduler(config-rule-test)# commit
Commit complete.
scheduler(config-rule-test)# end
```

Sample Configuration

The alert rules configuration are for reference only. Here is the configuration with sample values:

You can configure your alert rules based on your requirements.

```
scheduler#config
scheduler(config)# alert rule test
Value for 'expression' (<string>): test>1
Value for 'message' (<string>): testing
Value for 'snmp-clear-message' (<string>): test clear
scheduler(config-rule-test)#
scheduler(config-rule-test)# snmp-facility
Possible completions:
  application  hardware  networking  os  proc  virtualization
scheduler(config-rule-test)# snmp-facility application
scheduler(config-rule-test)# event-host-label instance
scheduler(config-rule-test)# snmp-severity
Possible completions:
  alert  critical  debug  emergency  error  info  none  notice  warning
scheduler(config-rule-test)# snmp-severity critical
scheduler(config-rule-test)# duration 30s
scheduler(config-rule-test)# commit
Commit complete.
```

```
scheduler(config-rule-test)# end
```

To display all the configured alert rules use the following command:

```
scheduler# show running-config alert | tab
                           EVENT
                           HOST                SNMP          SNMP       SNMP CLEAR
NAME  EXPRESSION  DURATION  LABEL     MESSAGE   FACILITY      SEVERITY   MESSAGE
-------------------------------------------------------------------------------------
test  test > 1    -         instance  testing   application   critical   testing clear
```

Sample Alert Rules

You can configure alert rules based on your requirements. For sample configuration, refer to Sample Alert Rule Configuration.

Note *event-host-label* value is used as a key in the alarm map. So, configure the correct value based on your requirements while configuring alert rules.

Note Grafana can be used to see all the statistics generated by the system and based on these statistics alerting rules can be configured.

Note Alert SNMP command includes an optional parameter named add-vm-info that you can use to specify whether or not the VM name is prepended in the SNMP alarm in broadhopComponentName. For example, broadhopComponentName: VMName/containerName. By default, the parameter is set to true. If set to false, broadhopComponentName does not prepend VM name. For example, broadhopComponentName: containerName. The following table includes sample alert rules when add-vm-info is set to false. For more information about this parameter and the command, see the *vDRA Operations Guide*.

Table 7: Sample Alert Rules

Alarm Name	Configuration
DiskFull	broadhopComponentName: Linux host name broadhopComponentNotificationName: DISK_FULL broadhopNotificationFacility: hardware Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: Disk Filesystem/usage is more than 90% Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: Disk filesystem/usage is greater than 10% **Expression:** node_filesystem_free{job='node_exporter',filesystem!~\"^/(/|$)\"} /node_filesystem_size{job='node_exporter'} < 0.10
HighLoad	broadhopComponentName: Linux host name broadhopComponentNotificationName: HIGH_LOAD broadhopNotificationFacility: hardware Alert broadhopNotificationSeverity: major Alert broadhopComponentAdditionalInfo: load average value for 5 minutes is greater than 3 current value is {{ $value }} Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: load average value for 5 minutes is lower than 3 **Expression:** node_load5 > 3
LowMemoryAlert	broadhopComponentName: Linux host name broadhopComponentNotificationName: LOW_MEMORY broadhopNotificationFacility: hardware Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: Available RAM is less than 80% current value is {{ $value }} Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: Available RAM is more than 80% **Expression:** round((node_memory_MemFree +node_memory_Buffers+node_memory_Cached)/node_memory_MemTotal *100) < 80

Alarm Name	Configuration
High CPU Usage Alert	broadhopComponentName: Linux host name broadhopComponentNotificationName: HIGH_CPU_USAGE broadhopNotificationFacility: hardware Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: CPU usage in last 10 sec is more than 30% current value {{ $value }} Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: CPU usage in last 10 sec is lower than 30% **Expression:** rate(node_cpu{mode="system"} [10s])*100 > 30
Link down Alert	broadhopComponentName: Linux host name broadhopComponentNotificationName: LINK_STATE broadhopNotificationFacility: networking Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: {{ $labels.interface }} is down on {{ $labels.instance }} Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: {{ $labels.interface }} is up on {{ $labels.instance }} **Expression:** link_state == 0
Process down Alert	Container Name: Linux host name broadhopComponentNotificationName: PROCESS_STATE broadhopNotificationFacility: application Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: {{ $labels.service_name }} instance {{ $labels.module_instance }}of module {{ $labels.module }} is in Aborted state. Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: {{ $labels.service_name }} instance {{ $labels.module_instance }}of module {{ $labels.module }} is moved from Aborted state **Expression:** docker_service_up==3

Alarm Name	Configuration
VM/Node Down Alert	broadhopComponentName: IP Address broadhopComponentNotificationName: IP_NOT_REACHABLE broadhopNotificationFacility: networking Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: VM/VIP IP {{$labels.instance }} is not reachable Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: VM/VIP IP {{$labels.instance }} is reachable **Expression:** probe_icmp_target==0
DiameterPeer Status	broadhopComponentName: Peer FQDN broadhopComponentNotificationName: DIAMETER_PEER_DOWN broadhopNotificationFacility: application Alert broadhopNotificationSeverity: error Alert broadhopComponentAdditionalInfo: Diameter peer is down Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: Diameter peer is up. **Expression:** peer_status==0
DRA Process Down (healthy) Alert	broadhopComponentName: Container Name broadhopComponentNotificationName: DRA_PROCESS_UNHEALTHY broadhopNotificationFacility: application Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: {{ $labels.service_name }} instance {{ $labels.module_instance }} of module {{ $labels.module }} is not healthy Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: {{ $labels.service_name }} instance {{ $labels.module_instance }} of module {{ $labels.module }} is healthy **Expression:** docker_service_up!=2

Alarm Name	Configuration
All DB Member of Replica Set Down Alert	broadhopComponentName: Shard Name broadhopComponentNotificationName: DB_SHARD_DOWN broadhopNotificationFacility: application Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: All DB Members of replica set {{ $labels.shard_name }} are down Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: Some DB Members of replica set {{ $labels.shard_name }} are up **Expression:** absent(mongodb_mongod_replset_member_state{shard_name="shard-1"})==1
No primary DB Member found Alert	broadhopComponentName: Shard Name broadhopComponentNotificationName: NO_PRIMARY_DB broadhopNotificationFacility: application Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: Primary DB member not found for replica set {{ $labels.shard_name }} Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: Primary DB member found for replica set {{ $labels.shard_name }} **Expression:** absent(mongodb_mongod_replset_member_health {shard_name="shard-1",state="PRIMARY"})==1
Secondary DB Member Down Alert	broadhopComponentName: Shard Name broadhopComponentNotificationName: SECONDARY_DB_DOWN broadhopNotificationFacility: application Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: Secondary Member {{ $labels.name }} of replica set {{ $labels.shard_name }} is down Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: Secondary Member {{ $labels.name }} of replica set {{ $labels.shard_name }} is down **Expression:** (mongodb_mongod_replset_member_state != 2) and ((mongodb_mongod_replset_member_state==8) or (mongodb_mongod_replset_member_state==6))

Alarm Name	Configuration
DRA message processing failure TPS exceeded	broadhopComponentName: System broadhopComponentNotificationName: DRA_MESSAGE_PROCESSING_FAILURE_TPS_EXCEEDED broadhopNotificationFacility: application Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: Message Processing Failure TPS exceeded. Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo Message Processing Failure TPS in control. Expression: rate(rejected_messages_total[5m]) > 5
Keepalive RAR routing failure - TPS exceeded	broadhopComponentName: System broadhopComponentNotificationName: KEEP_ALIVE_RAR_ROUTING_FAILURE_TPS_EXCEEDED broadhopNotificationFacility: application Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: Keep Alive RAR TPS exceeded. Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: Keep Alive RAR TPS in control. Expression: rate(keep_alive_rar_failure[5m]) > 5
Egress rate limited session error response TPS exceeded	broadhopComponentName: Peer FQDN broadhopComponentNotificationName: EGRESS_RATE_LIMITED_SESSION_ERR_RESP_TPS_EXCEEDED broadhopNotificationFacility: application Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: Egress rate limited messages with error response TPS exceeded. Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: Egress rate limited messages with error response TPS in control. Expression: rate(diameter_peer_egress_rate_limited_with_err_response[5m]) > 5

Alarm Name	Configuration
Egress rate limited session reject TPS exceeded	broadhopComponentName: Peer FQDN broadhopComponentNotificationName: EGRESS_RATE_LIMITED_SESSION_REJECT_TPS_EXCEEDED broadhopNotificationFacility: application Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: Egress rate limited messages dropped without error TPS exceeded. Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: Egress rate limited messages dropped without error TPS in control. Expression: rate(diameter_peer_egress_rate_limited_without_err_response[5m]) > 5
Ingress rate limited session error response TPS exceeded	broadhopComponentName: Peer FQDN broadhopComponentNotificationName: INGRESS_RATE_LIMITED_SESSION_ERR_RESP_TPS_EXCEEDED broadhopNotificationFacility: application Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: Ingress rate limited messages with error response TPS exceeded. Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: Ingress rate limited messages with error response TPS in control. Expression: rate(diameter_peer_ingress_rate_limited_with_err_response[5m]) > 5
Ingress rate limited session reject TPS exceeded	broadhopComponentName: Peer FQDN broadhopComponentNotificationName: INGRESS_RATE_LIMITED_SESSION_REJECT_TPS_EXCEEDED broadhopNotificationFacility: application Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: Ingress rate limited messages dropped without error response TPS exceeded. Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: Ingress rate limited messages dropped without error response TPS in control. Expression: rate(diameter_peer_ingress_rate_limited_without_err_response[5m]) > 5

Alarm Name	Configuration
Binding key not found in AAR TPS exceeded	broadhopComponentName: System broadhopComponentNotificationName: BINDING_KEY_NOT_FOUND_IN_AAR_TPS_EXCEEDED broadhopNotificationFacility: application Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: Binding Key not found in AAR TPS exceeded. Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: Binding Key not found in AAR TPS in control. Expression: rate(aar_bind_key_not_found_total[5m]) > 5
Binding key not found in CCR-I TPS exceeded	broadhopComponentName: System broadhopComponentNotificationName: BINDING_KEY_NOT_FOUND_IN_CCR_I_TPS_EXCEEDED broadhopNotificationFacility: application Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: Binding Key not found in CCR(I) TPS exceeded. Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: Binding Key not found in CCR(I) TPS in control. Expression: rate(ccri_bind_key_not_found_total[5m]) > 5
Peer response time exceeded	broadhopComponentName: Peer FQDN broadhopComponentNotificationName: PEER_RESPONSE_TIME_EXCEEDED broadhopNotificationFacility: application Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: Peer response time exceeded. Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: Peer response time in control. Expression: rate(message_duration_seconds{type=~\"peer_.*\"}[5m]) > 5

Alarm Name	Configuration
No peer group member available	broadhopComponentName: Container Name broadhopComponentNotificationName: NO_PEER_GROUP_MEMBER_AVAILABLE broadhopNotificationFacility: application Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: Peer group not available. Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: Peer group available. Expression: no_active_peer_in_peer_group ==1
Forwarding loop found TPS exceeded	broadhopComponentName: System broadhopComponentNotificationName: FORWARDING_LOOP_FOUND_TPS_EXCEEDED broadhopNotificationFacility: application Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: Loop Detected TPS exceeded. Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: Loop Detected TPS in control. Expression: rate(diameter_loop_detected [5m]) > 5
No relay peer TPS exceeded	broadhopComponentName: Container Name broadhopComponentNotificationName: NO_RELAY_PEER_TPS_EXCEEDED broadhopNotificationFacility: application Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: Relay Peer TPS exceeded. Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: Relay Peer TPS in control. Expression: rate(relay_send_nopeer[5m]) > 5

Alarm Name	Configuration
Relay link status	broadhopComponentName: Peer FQDN broadhopComponentNotificationName: RELAY_LINK_STATUS broadhopNotificationFacility: application Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: Relay Link is down. Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: Relay Link is up Expression: relay_peer_status == 0
Binding not found TPS exceeded	broadhopComponentName: System broadhopComponentNotificationName: BINDING_NOT_FOUND_TPS_EXCEEDED broadhopNotificationFacility: application Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: Binding not found TPS exceeded. Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: Binding not found TPS in control Expression: rate(binding_not_found_total[5m]) > 5
Relay link TPS GT 0	broadhopComponentName: Peer FQDN broadhopComponentNotificationName: RELAY_LINK_TPS_GT_0 broadhopNotificationFacility: application Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: Relay started. Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: Relay not started. Expression: rate(relay_peer_messages_total[5m]) > 0
Relay link TPS exceeded	broadhopComponentName: Peer FQDN broadhopComponentNotificationName: RELAY_LINK_TPS_EXCEEDED broadhopNotificationFacility: application Alert broadhopNotificationSeverity: critical Alert broadhopComponentAdditionalInfo: Relay Link TPS exceeded. Clear broadhopNotificationSeverity: clear Clear broadhopComponentAdditionalInfo: Relay Link TPS in control. Expression: rate(relay_peer_messages_total[5m]) > 5

Health Status of Service

On getting the Qns Java Process State alert, the user has to access the system and check the diagnostics logs of the service to get the exact issue with the service. To access the system and check the diagnostics log, run the following command:

```
show system diagnostics | include <service_name>
```

For example:

```
scheduler# show system diagnostics | include diameter-endpoint-s1
system diagnostics diameter-endpoint-s1 serfHealth 1
system diagnostics diameter-endpoint-s1 service:cisco-policy-app 1
system diagnostics diameter-endpoint-s1 service:cisco-policy-app 2
system diagnostics diameter-endpoint-s1 service:cisco-policy-app 3
system diagnostics diameter-endpoint-s1 service:cisco-policy-app 4
 message "CLEARED: InterfaceID=diameter-endpoint-s1.weave.local;msg=\"Memcached server is
operational\""
system diagnostics diameter-endpoint-s1 service:cisco-policy-app 5
 message "CLEARED: InterfaceID=com.broadhop.server:diameter-endpoint-s1.weave.local;msg=\"
 before Feature com.broadhop.server is Running\""
system diagnostics diameter-endpoint-s1 service:cisco-policy-app 6
 message "CLEARED:
InterfaceID=com.broadhop.dra.service:diameter-endpoint-s1.weave.local;msg=\" before Feature
 com.broadhop.dra.service is Running\""
system diagnostics diameter-endpoint-s1 service:cisco-policy-app 7
 message "CLEARED:
InterfaceID=com.broadhop.common.service:diameter-endpoint-s1.weave.local;msg=\" before
Feature com.broadhop.common.service is Running\""
system diagnostics diameter-endpoint-s1 service:cisco-policy-app 8
 message "CLEARED:
InterfaceID=com.broadhop.resourcemonitor:diameter-endpoint-s1.weave.local;msg=\" before
Feature com.broadhop.resourcemonitor is Running\""
system diagnostics diameter-endpoint-s1 service:cisco-policy-app 9
 message "CLEARED:
InterfaceID=com.broadhop.microservices.control:diameter-endpoint-s1.weave.local;msg=\"
before Feature com.broadhop.microservices.control is Running\""
system diagnostics diameter-endpoint-s1 service:cisco-policy-app 10
 message "CLEARED:
InterfaceID=com.broadhop.custrefdata.service:diameter-endpoint-s1.weave.local;msg=\" before
 Feature com.broadhop.custrefdata.service is Running\""
system diagnostics diameter-endpoint-s1 service:cisco-policy-app 11
system diagnostics diameter-endpoint-s1 service:cisco-policy-jmx 1
scheduler#
```

Delete Alert Rules

The following section describes the procedure to delete an alert rule and are for reference only:

```
scheduler# config
Entering configuration mode terminal
scheduler(config)# no alert rule node_down
scheduler(config)# commit
Commit complete.
scheduler(config)# end
scheduler#
```

Alert Status

Use the following command to display the current alerts status:

```
show alert status
```

For example:

```
scheduler# show alert status
NAME                  EVENT HOST      STATUS    MESSAGE
                        UPDATE TIME
-------------------------------------------------------------------------------------------------------
high_cpu_alert        system          firing    CPU usage is more than 30% current_value
is 37.05555555555597     2017-05-22T10:59:37.945+00:00
high_cpu_alert_1      control-0       resolved  CPU usage is more than 30% current_value
is 33.62500000000637     2017-05-22T17:17:38.184+00:00
high_cpu_alert_1      control-1       resolved  CPU usage is more than 30% current_value
is 35.666666666667076    2017-05-22T11:29:37.899+00:00
high_cpu_usage_alert  localhost:9090  resolved  CPU Usage for last 1 min is more than
configured threshold        2017-05-22T09:55:37.902+00:00
2017-05-22T15:39:37.811+00:00

scheduler#
```

NMS Destination Configuration

The following configuration is for reference only:

You can configure the NMS destination based on your requirements.

Example: SNMPv2

```
scheduler#config
scheduler(config)# alert snmp-v2-destination "10.1.1.1"
Value for 'community' (<string>): "cisco"
scheduler(config-snmp-v2-destination-10.1.1.1)# commit
Commit complete.
scheduler(config-snmp-v2-destination-10.1.1.1)# end
```

where, "10.1.1.1" is the SNMPv2 NMS destination address.

Example: SNMPv3

```
scheduler# config
scheduler(config)# alert snmp-v3-destination <nms_ip> e.g. 10.1.1.2
Value for 'user' (<string>): <username> e.g. cis_user
Value for 'auth-password' (<string>): <password string > e.g. cisco-123
Value for 'privacy-password' (<string>): <password string> e.g. cisco-123
scheduler(config-snmp-v3-destination-10.1.1.2)# auth-proto
[MD5,SHA] (SHA): SHA
scheduler(config-snmp-v3-destination-10.1.1.2)# privacy-p
Possible completions:
  privacy-password  privacy-protocol
scheduler(config-snmp-v3-destination-10.1.1.2)# privacy-protocol
[AES,DES] (AES): AES
scheduler(config-snmp-v3-destination-10.1.1.2)# engine-id
(<string>) (0x0102030405060708): 0x0102030405060708
scheduler(config-snmp-v3-destination-10.1.1.2)# commit
Commit complete.
scheduler(config-snmp-v3-destination-10.1.1.2)# end
scheduler#
```

where, "10.1.1.2" is the SNMPv3 NMS destination address.

All the configured NMS destinations in the system can be displayed using the following command:

```
scheduler# show running-config alert | tab
NMS
ADDRESS   COMMUNITY
---------------------
10.1.1.1  cisco

alert snmp-v3-destination 10.142.148.160
 engine-id        0x0102030405060708
 user             cis_user
 auth-proto       SHA
 auth-password    cisco-123
 privacy-protocol AES
 privacy-password cisco-123
!
```