

# Lumen<sup>®</sup> SD-WAN Alarms Guide

v16.1R2

LUMEN<sup>®</sup>

---

## General Disclaimer

Although Lumen has attempted to provide accurate information in this guide, Lumen does not warrant or guarantee the accuracy of the information provided herein. Lumen may change the programs or products mentioned at any time without prior notice. Mention of non-Lumen products or services is for information purposes only and constitutes neither an endorsement nor a recommendation of such products or services or of any company that develops or sells such products or services.

ALL INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED "AS IS," WITH ALL FAULTS, AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED OR STATUTORY. LUMEN AND ITS SUPPLIERS HEREBY DISCLAIM ALL WARRANTIES RELATED TO THIS GUIDE AND THE INFORMATION CONTAINED HEREIN, WHETHER EXPRESSED OR IMPLIED OR STATUTORY INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT, OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

LUMEN AND ITS SUPPLIERS SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR REVENUES, COSTS OF REPLACEMENT GOODS OR SERVICES, LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OF THE GUIDE OR ANY LUMEN PRODUCT OR SERVICE, OR DAMAGES RESULTING FROM USE OF OR RELIANCE ON THE INFORMATION PROVIDED IN THIS GUIDE, EVEN IF LUMEN OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and other information used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Many of the Lumen products and services identified in this guide are provided with, and subject to, written software licenses and limited warranties. Those licenses and warranties provide the purchasers of those products with certain rights. Nothing in this guide shall be deemed to expand, alter, or modify any warranty or license or any other agreement provided by Lumen with any Lumen product, or to create any new or additional warranties or licenses.

---

## Contents

Preface .....	6
Lumen Proactive Alarm Monitoring .....	8
Alarm Types and Destinations .....	10
Alarm Configuration.....	14
Interface Alarms .....	22
System Alarms .....	25
Session Alarms .....	28
Services Alarms .....	30
Routing Alarms.....	34
SD-WAN Alarms.....	36
Software Alarms .....	38
High Availability Alarms.....	42

## Preface




### Introduction

This document describes configuring and analyzing Alarms in Versa FlexVNF. This guide also explains the usage of alarms in troubleshooting problems.

### Audience

This document is for experienced network and system administrators who are responsible for troubleshooting, configuring and managing public and private cloud infrastructure. It is presumed that admins are aware of firewall, virtualization concepts, syslog servers and configuration of network devices.

### Document Conventions

Convention	Description
<b>Bold</b>	Represents UI elements.
<i>Italics</i>	Values to enter in the text fields or values in drop down menus.
Monospace	CLI or system code.
\$	Command beginning with \$ denotes a shell command, which is run on bash.
>	Command beginning with > denotes a operational mode CLI command.
%	Command beginning with % denotes a config mode CLI command.
	Notes contain incidental information about the subject and call attention to exceptions.
	Caution indicates actions that can cause loss of data.
	Tips provide great shortcuts, hints, and recommended settings/configurable values.

### Glossary

Term	Description/Full Form
Address Pool	Address pool is the IP address list from which IP addresses are dynamically allocated by the DHCP server to clients requesting an IP address.
Aggregate interface	An aggregate interface is a bundle of Ethernet interfaces.
ARP	Address Resolution Protocol.

CFM	CFM (Connectivity Fault Management) is a protocol to monitor the health of network links. Depending on network events (blocked port, blocked interface), an action is configured. This is done in an action profile.
DHCP	Dynamic Host Configuration Pool.
Dot IP Address	A dot IP address (also known as a dotted quad address) refers to the notation to write four-byte IP address as a sequence of four decimal numbers separated by dots.
DSCP	Differentiated Services Code Point (DSCP) refers to the value or cost of the policy.
LEF	Log Export Functionality (LEF) is used to generate logs on an external device.
MPLS	Multiprotocol Label Switching.
MTU	Maximum transmission unit. The size in bytes of largest protocol data unit that the port can receive or transmit.
RED	Random Early Detection.
Router	A router is a device that forwards data packets along networks. A router is connected to at least two networks and is located at gateways, the places where two or more networks connect.
Service Node Group	A service node group is a logical grouping of network services, which include individual network services (for example, NAT, DHCP, and NTP). Additionally, various policies and quotas can be applied for the service node group (for example, elastic policy, traffic policing and
TTL	Time to Live (TTL) Condition is the number of hops that a packet can travel before being discarded by a router. It indicates the lifespan of a data packet.
VNI	Virtual Network Interface.
Versa Director	VNF Manager for all controllers, SD-WAN hubs, and branch nodes. Versa Director is provisioned at one or more data centers with connectivity to management and control networks for the SD-WAN.
Versa Analytics	The Versa Analytics node provides a pre-integrated solution to a full operational visibility into the SD-WAN topology. The Analytics node gathers IPFIX data from the controller, hub, and branch sites and archives and displays this data in readily accessible formats.
RRRP	Virtual Router Redundancy Protocol.

## Lumen Proactive Alarm Monitoring

Lumen SD-WAN service includes proactive alarm monitoring and ticketing for SD-WAN service instances. Customers can define the contacts and contact methods for notification via their Lumen service portal. Lumen SD-WAN support may also reach out to customers directly via phone or e-mail in the process of troubleshooting an alarm.

Lumen polls appliances/circuits every four minutes to check health. The following alarms may occur and actions will be taken, as per the table below:

Alarm Type	Definition	Alarm Severity	Lumen Action Taken
Daemon Down	Detects when the SD-WAN software service goes down	Urgent	An automatic ticket is generated immediately if SD-WAN
Interface Down	Detects when an interface is down	Business – High	Ticket is auto-generated if interface remains down for 12 minutes.
Branch Disconnect	Detects when branch device is not connected to either controller	Business – High	Ticket is auto-generated if branch device remains down
High CPU	Detects when CTL-Provided CPE exceeds defined thresholds	Business - Medium	Ticket is auto-generated if CPE remains above 80% for 20 minutes.
High Memory	Detects when memory exceeds defined thresholds	Business – Medium	Ticket is auto-generated if CPE remains above 80% for
BGP Neighbor Down	Detects when a BGP neighbor is not in an established state	Business – Medium	Ticket is auto-generated if BGP neighbor remains down for 12 minutes
Circuit Down	Detects when a SD-WAN overlay tunnel to both SD-WAN controllers is down across any transport path	Business – Medium	Ticket is auto-generated if both SD-WAN controllers are down for 20 minutes. Upon alarm, Lumen calls customer's site contact to check power, reboot modem, and escalate to carrier (if appropriate).
CPE Interface Bouncing	Detects when interface on CTL provided CPE is bouncing	Business – Medium	Ticket is auto-generated if interface bounces 5 or more times in a 25 minute window
CPE VRRP Switchover	Reports on failover between two appliances configured	Business – Medium	Ticket is auto-generated if alarm active for 12 minutes

	in HA utilizing VRRP protection scheme		
OSPF Neighbor State Change	Detects a change in OSPF neighbor state (when applicable) Normally representative of a "flapping" condition	Business – Medium	Ticket is auto-generated if OSPF state is NOT 'Full" for 12 minutes

## Alarm Types and Destinations

### Supported Alarm Types

Versa FlexVNF supports multiple alarm types with different severity level to provide live status of any service or device activity that needs attention.

**NOTE:** By default, the alarms are sent to Versa Analytics and then streamed to Versa Director. Based on the configuration, you can stream them to any 3rd party collector.

Versa Analytics stores alarms in the database for diagnostics and internal usage purpose only. By default, this data is purged automatically after 7 days. You can modify the purge timer settings.

You can use the Versa FlexVNF alarms configuration for:

- Enabling alarms to stream directly from Versa FlexVNF to external sources.
- Modify the default behavior.

**Table 1** provides information on supported alarm types, threshold values, and the default destination to which the alarms are exported.

Table 1: Supported Alarm Types and Default Destination

Alarm Type	Description	Default Destination
cpu-utilization	Generated when datapath CPU utilization exceeds configured threshold value.	snmp, syslog, analytics
mem-utilization	Generated when datapath memory utilization exceeds configured threshold value.	snmp, syslog, analytics
disk-utilization	Generated when disk utilization exceeds configured threshold value.	snmp, syslog, analytics
org-session-utilization	Generated when number of sessions of an org exceed configured number of sessions.	snmp, syslog, analytics
device-session-utilization	Generated when number of sessions exceeds configured number of sessions for a device/appliance.	snmp, syslog, analytics
Interface-down	Generated when an interface (or sub-interface) goes down.	snmp, syslog, analytics
uplink-bw-threshold	Generated when current uplink bandwidth exceeds configured uplink bandwidth of an interface.	snmp, syslog, analytics
dnlink-bw-threshold	Generated when current downlink bandwidth exceeds configured uplink bandwidth of an interface.	snmp, syslog, analytics



adc-server-down	Generated when backend server does not respond to ADC monitor(s) for a specified amount of time. Once server is marked down, it will not be considered for load balancing.	snmp, syslog, analytics
adc-vservice-down	Generated when all backend server(s) attached to virtual service are declared down because of monitor health failure. No traffic will be served by this virtual service (VIP).	snmp, syslog, analytics
cgnat-pool-utilization	Generated when CGNAT pool exceeds configured threshold value or when pool is exhausted.	snmp, syslog, analytics
snat-pool-utilization	Generated when SNAT pool exceeds configured threshold value or when pool is exhausted.	snmp, syslog, analytics
ipsec-tunneldown	Generated when IPSEC tunnel with a peer goes down.	snmp, syslog, analytics
ipsec-ike-down	Generated when IKE connection established with a peer goes down.	snmp, syslog, analytics
bgp-nbr-state-change	Generated when BGP between peers goes down or comes back up.	snmp, syslog, analytics
vrrp-v3-new-master	Generated when VRRP router transitions to MASTER state.	snmp, syslog, analytics
vrrp-v3-new-backup	Generated when VRRP router transitions to BACKUP state.	snmp, syslog, analytics
vrrp-v3-proto-error	This notification indicates that the VRRP router has encountered protocol error like version mismatch, checksum error, or VRRP	snmp, syslog, analytics
ddos-threshold	Generated when DDOS traffic exceeds configured aggregate/classified DDOS threshold.	snmp, syslog, analytics
zone-protection-flood	Generated when flood traffic exceeds configured zone protection threshold value.	snmp, syslog, analytics
port-scan-flood	Generated when PORT-SCAN from a source to destination exceeds configured zone protection profile value.	snmp, syslog, analytics
sdwan-branch-disconnect	Generated a branch gets disconnected from Controller.	snmp, syslog, analytics
sdwan-datapath-down	Generated when all paths between two branches goes down.	analytics (From Controller)

sdwan-datapath-sla-not-met	Generated when the path between two branches for a particular traffic class does not meet SLA.	None (From Controller)
branch-in-maintenance-mode	Generated branch goes down because of non-recoverable failure. Fallback IPSEC connection is created between branch and	syslog
dhcp-pool-utilization	Generated when DHCP addresses are exhausted and no more addresses can be allocated from DHCP address pools.	snmp, syslog, analytics
device-disk-errors	Bad blocks detected on disk.	snmp, syslog
appliance-not-subjugated	Appliance not subjugated to Versa Director.	snmp, syslog
app-stopped	Appliance not subjugated to Versa Director	syslog
software-version-change	Generated after Versa FlexVNF is upgraded.	syslog
software-upgrade-success	Versa FlexVNF software upgrade succeeded.	syslog
software-upgrade-failure	Versa FlexVNF software upgrade failed.	syslog
software-rollback-success	Versa FlexVNF software rollback succeeded (rollback due to upgrade failure).	syslog
software-rollback-failure	Versa FlexVNF software rollback failed (upgrade failed, and rollback too).	syslog
software-trial-expired	Versa appliance trial period expired.	snmp, syslog, analytics
software-trial-error	Versa appliance trial key tampered.	snmp, syslog, analytics
interface-half-duplex	Generated when an interface is detected to be in Half Duplex mode.	snmp, syslog, analytics
nexthop-down	Generated when nexthop gateway does not respond to monitor(s) for a specified amount of time. Once nexthop is marked down,	snmp, syslog, analytics
monitor-down	Generated when an IP destination(s) that are part of the monitor does not respond to the given type of probe packets for a specified	snmp, syslog, analytics

software-key-about-to-expire	Versa FlexVNF key expires soon. Contact Versa Support to replace with a new key. For unrestricted usage, ensure Versa FlexVNF is	snmp, syslog, analytics
ha-state-change	Generated when HA state changes from master to slave or vice versa.	snmp, syslog, analytics
ha-sync-status	Generated after configuration sync happens between active and standby. Either sync error (or) sync ok will be reported.	snmp, syslog, analytics

## Alarm Destinations

By default Versa FlexVNF alarms are configured and saved on the local file system and sent to the default destination (Analytics, Syslog & SNMP) as specified in [Table 1: Supported Alarm Types and Default Destination](#). You can update the default behavior by configuring additional destination or change the default behavior based on requirements. You can configure these changes in the Versa Director GUI Portal.

Lumen sets up a default profile for all customers to configure alarms to flow to Versa Analytics. Protocols listed below would be additional destinations that are optional for alarm forwarding.

Versa FlexVNF uses these Network Management protocols and ports to communicate with external entity:

Table 2: Network Management Protocols and Ports

Protocol	Source	Interface	Destination	Transport	Port	Content
SNMP	Versa FlexVNF	eth0 - out-of-band	SNMP Trap Receiver	UDP/TCP	162	SNMP Traps for Interface, Application, SLA, Protocol alarms
SNMP	Versa FlexVNF	TVI - SD WAN in-band	SNMP Trap Receiver	UDP/TCP	162	SNMP Traps for Interface, Application, SLA, Protocol alarms
Syslog (for Alarms)	Versa FlexVNF	eth0 - out-of-band	Syslog receiver	UDP/TCP	514	Linux and FlexVNF syslog messages and alarms

## Alarm Configuration


### Configuring Alarms on Versa FlexVNF

Use the Versa Director GUI or CLI to configure the Versa FlexVNF alarms.


The Versa FlexVNF generated alarms are streamed from the Controller to the default destination.

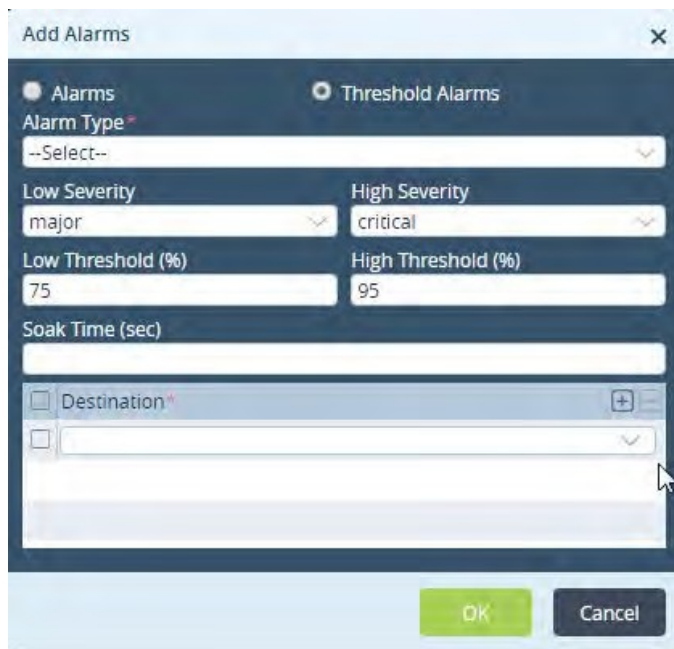
**NOTE:** Versa recommends configuring alarms using the Versa Director GUI config template mode. Follow these steps to configure alarms using Versa Director GUI config template:

1. Login to Versa Director.
2. Navigate to Director Context > Config Templates.
3. Select the appropriate template.
4. Navigate to Others > System > Options > Alarms.

5. Click  to add a new alarm profile. This opens the Add Alarms window.
6. Select Alarms and enter these details:


Use this field...	To ...
Alarm Type	Select a type of alarm from the drop-down box. This is a mandatory field.

Severity	Select a severity for the selected alarm type. These are the options: <ul style="list-style-type: none"> <li>• critical</li> <li>• cleared</li> <li>• indeterminate</li> <li>• major</li> <li>• minor</li> </ul>
Soak Time (sec)	Select a threshold to send ICMP probe. Default value: 5
Destination	Click  to add a destination for the alarm. Multiple destinations are allowed.



7. Select Threshold Alarms and enter these details:

Use this field...	To ...
Alarm Type	Select a type of alarm from the drop-down box.
Low Severity	Select a low severity for the selected alarm type. These are the options: <ul style="list-style-type: none"> <li>• critical</li> <li>• cleared</li> <li>• indeterminate</li> <li>• major</li> <li>• minor</li> </ul>

High Severity	Select a high severity for the selected alarm type. These are the options: <ul style="list-style-type: none"> <li>• critical</li> <li>• cleared</li> <li>• indeterminate</li> <li>• major</li> <li>• minor</li> </ul>
Low Threshold (%)	Select a low threshold for the selected alarm.
High Threshold (%)	Select a high threshold for the selected alarm.
Soak Time (sec)	Select a threshold to send ICMP probe. Default value: 5
Destination	Click  to add a destination for the alarm. Multiple destinations are allowed.

8. Click OK to configure a new alarm.

## Alarm Severities

These are the severities defined for an alarm:

- Cleared—This severity level indicates the clearing of one or more previously reported alarms.

This alarm clears all alarms for the managed object with the same alarm type, cause, and specific problems (if given). The clearing of previously reported alarms need not be reported. Therefore, a managing system cannot assume that the absence of an alarm with the Cleared severity level means that the condition that caused the generation of previous alarms is still present. Managed object definers state the condition under which cleared severity level is used.

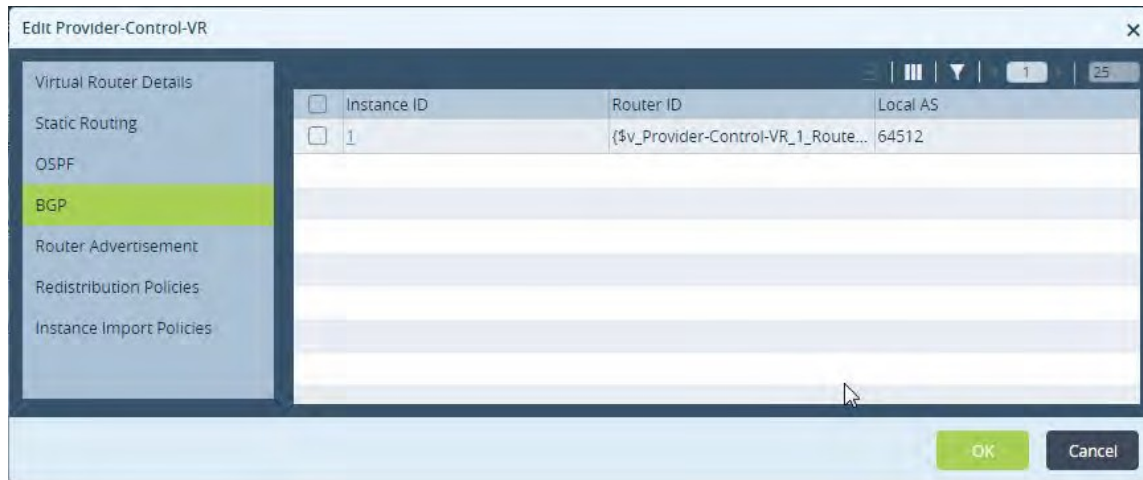
- Indeterminate—This level indicates that the severity level cannot be determined.
- Critical: This severity level indicates a presence of service affecting condition for which an immediate corrective action is required. Report this severity when a managed object is totally out of service and its capability must be restored.
- Major—This severity level indicates a service affecting condition and an urgent corrective action is required. Report this severity when there is a severe degradation in the capability of the managed object and its full capability must be restored.
- Minor—This severity level indicates the existence of a non-service affecting fault condition and a corrective action is required to prevent serious (for example, service affecting) fault. This severity needs to be reported when the detected alarm condition is not currently degrading the capacity of the managed object.
- Warning—This severity level indicates the detection of a potential or impending service affecting fault before any significant effects. You must take the required action to diagnose (if necessary) and correct the problem to prevent any serious service affecting fault.

## Enabling BGP Alarms

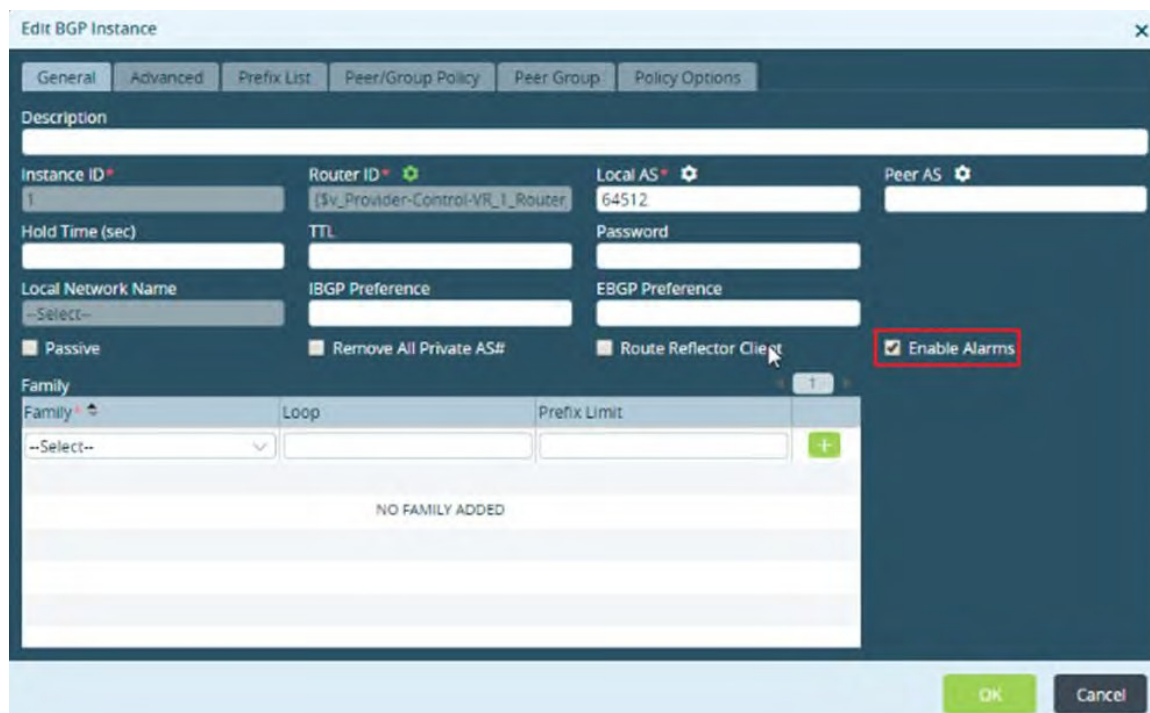
Enable alarms from Virtual router section to receive BGP alarms.

NOTE: This alarm was introduced in Release 16.1.R1S3. Follow these steps to receive BGP neighbor state change alarms:

1. Navigate to Director Context > Config Templates and select a template.



2. Navigate to Networking > Virtual Routers and select a routing instance. The Edit Provider-Control-VR window is displayed.
3. Select BGP and click the instance ID. This opens the Edit BGP Instance window.



4. Select Enable Alarms to enable the alarms for the Instance ID.

Follow the same procedure to enable alarms for other BGP routing instances.

## Enabling Monitor Alarms


Versa FlexVNF supports monitoring the IP address. It sends ICMP probe packets and based on the reachability the static routes are updated. These probe packet states generate alarms called Monitor Alarms.

To enable monitor alarms, first configure IP-SLA monitor profile, and then associate this profile to the routing instance.

**NOTE:** This alarms was introduced in Release 16.1.R1S3.


Follow these steps to enable monitor alarms:

1. Navigate to Director Context > Config Templates and select a template.

2. Navigate to Settings > IP-SLA Monitors and click  to open the Add IP-SLA Monitors window.
3. Enter these details in the Add IP-SLA Monitors window:

Use this field...	To ...
Name	Select a name for the IP-SLA monitor profile.
Interval	Select an interval, in seconds, for ICMP probe to be sent. Default value: 3 seconds
Threshold	Select a threshold to send ICMP probe. Default value: 5
Monitor Type	Select a monitor type.
Source Interface	Select a source interface for the probe.

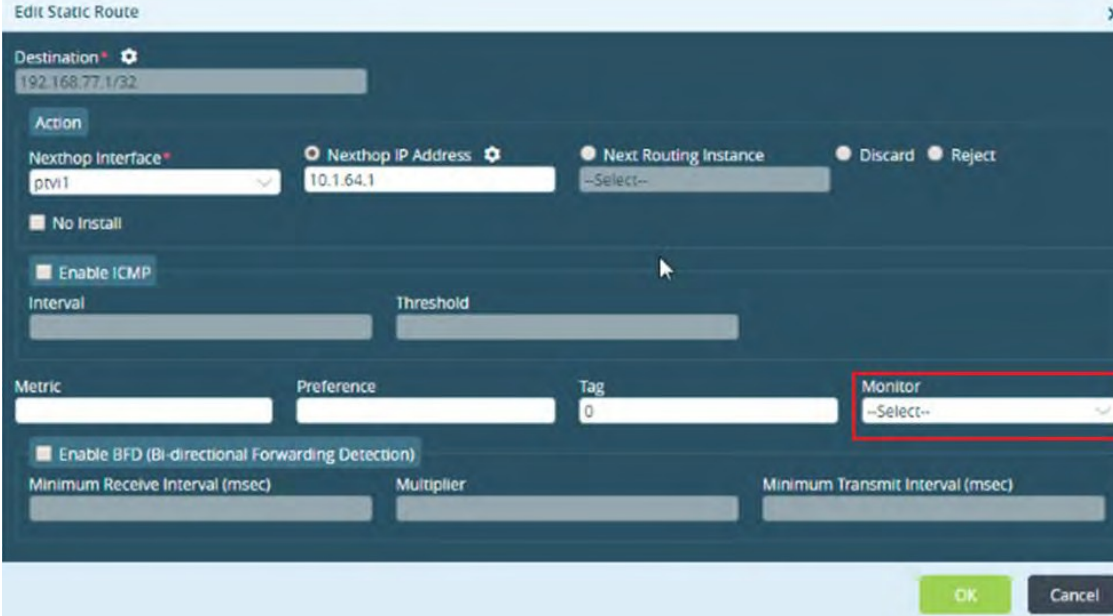


IP Address      Click  provide the destination IP address for the probe by clicking .


4. Click OK.

NOTE: You can configure multiple IP SLA monitor profiles.

5. Navigate to Virtual Routers > Routing Instance > Static Routing.



The screenshot shows the 'Edit Static Route' configuration window. The 'Destination' field is set to '192.168.77.1/32'. Under the 'Action' section, 'Next Hop Interface' is 'pvt1', 'Next Hop IP Address' is '10.1.64.1', and 'Next Routing Instance' is '--Select--'. There are radio buttons for 'Discard' and 'Reject'. Below this, there are checkboxes for 'No Install', 'Enable ICMP', and 'Enable BFD (Bi-directional Forwarding Detection)'. The 'Monitor' dropdown menu is highlighted with a red box. At the bottom, there are 'OK' and 'Cancel' buttons.

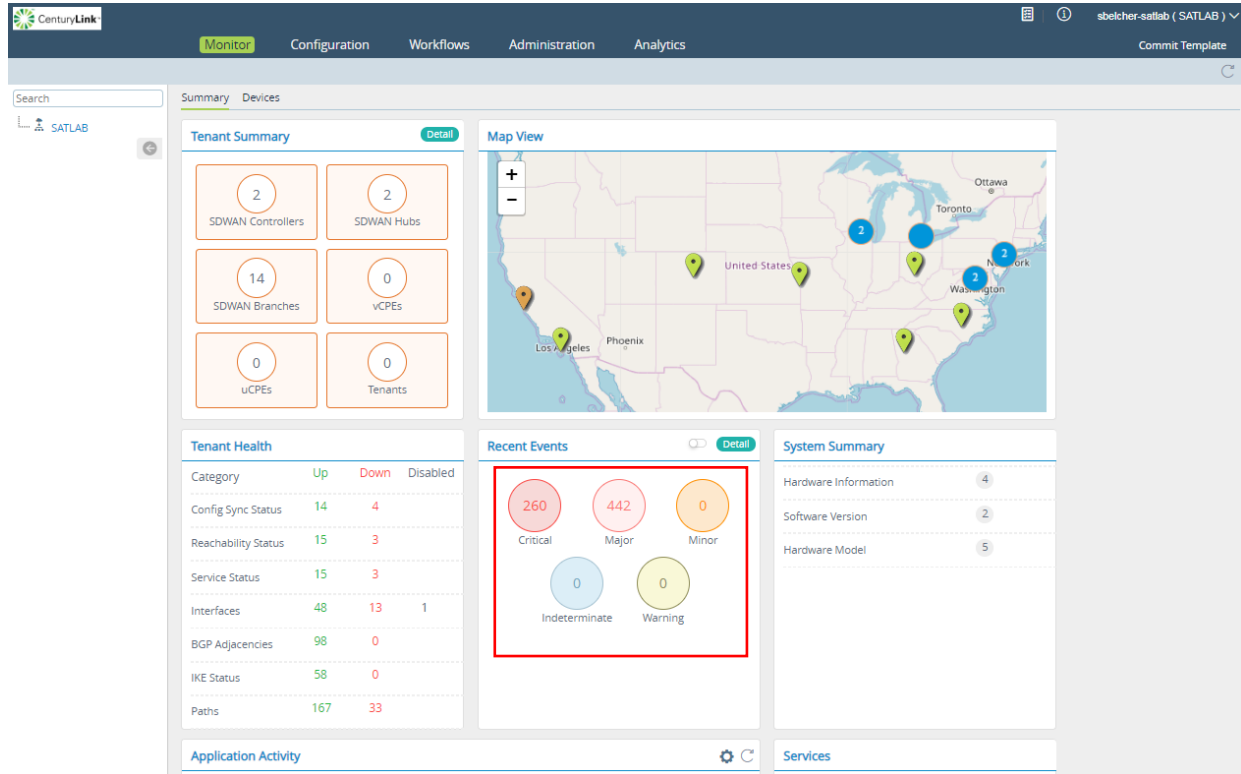
6. Click an existing route OR click  to add a new static route. This opens the Edit Static route/Add Static Route window.

7. From the Monitor drop-down box, select the IP-SLA profile to associate the IP-SLA profile with a static route.

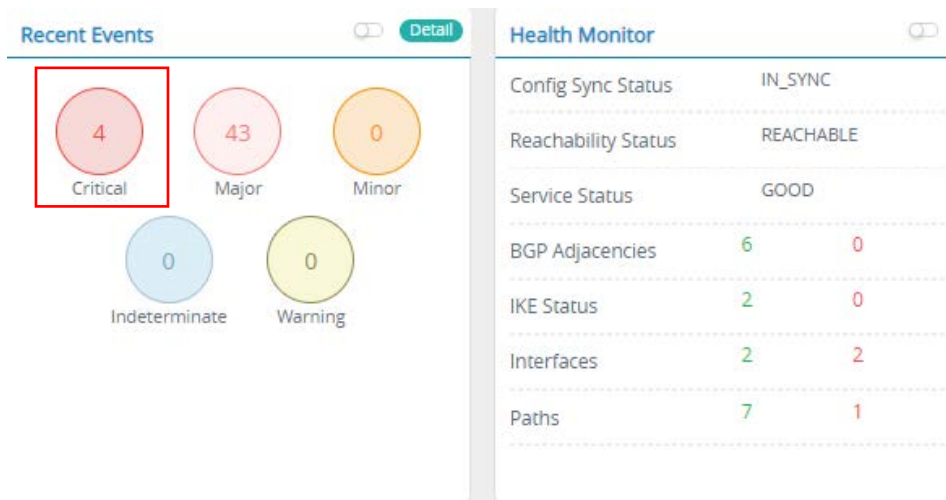
## Viewing Alarm Log in Versa Director

Follow these steps to view the alarm logs received in the Versa Director from the Versa Analytics:

1. Select the Monitor tab of the Versa Director GUI and select the device on which the syslog data you want to analyze.



- Select the appropriate events from the Recent Events section to view the details of the alarms for the device.



This displays the event related details.

The screenshot shows the CenturyLink Monitor interface. The top navigation bar includes 'Monitor', 'Configuration', and 'Administration'. Below this, there are tabs for 'Home' and 'SATLAB-bgrubbs'. A search bar is present, and a table of alarms is displayed. The table has columns for Device Name, Organization Name, Alarm Type, Handling, Severity, Status Change Time, and Alarm Text. There are four rows of data, all showing 'interface-down' alarms for device 'SATLAB-bgrubbs' with a severity of 'critical'.

<input type="checkbox"/>	Device Name	Organization Name	Alarm Type	Handling ...	Severity	Status Change Time	Alarm Text
<input type="checkbox"/>	<a href="#">SATLAB-bgrubbs</a>	SATLAB	interface-down		critical	Mon, Feb 04 2019, 21:...	Interface vni-0/4.0 is down (n/a)
<input type="checkbox"/>	<a href="#">SATLAB-bgrubbs</a>	SATLAB	interface-down		critical	Mon, Feb 04 2019, 21:...	Interface vni-0/4 is down (n/a)
<input type="checkbox"/>	<a href="#">SATLAB-bgrubbs</a>	SATLAB	interface-down		critical	Thu, Jan 17 2019, 12:53	Interface vni-0/3.0 is down (n/a)
<input type="checkbox"/>	<a href="#">SATLAB-bgrubbs</a>	SATLAB	interface-down		critical	Thu, Jan 17 2019, 12:53	Interface vni-0/3 is down (n/a)

## Interface Alarms

### Overview

Interface alarms are configured to generate an alert whenever an interface goes down. The Versa FlexVNF sends these interface alarms to the Versa Director:

- interface-down alarm
- interface-half-duplex alarm

**NOTE:** This alarm was introduced in Release earlier to 16.1.R1S3.

### Interface-down Alarm

The Versa FlexVNF represents physical interfaces as VNI interfaces. When these interfaces go down, the interface-down alarm is raised. This alarm is cleared after the recovery of the link.

Description	<p>Versa FlexVNF Virtual Network Interfaces (VNI) raise interface down alarm when the operational state changes. This is a critical alarm , because VNI interfaces need to be operationally and administratively up for normal working of the interfaces.</p> <p><u>During upgrade of an image, the interface state will not change.</u></p>
Cause	<ul style="list-style-type: none"> <li>• When the Versa FlexVNF is running on a physical machine (BM server or a Lanner/Advantech device), the physical link state change triggers interface down alarms.</li> <li>• When the Versa FlexVNF is running on a virtual machine, the interface down alarms gets triggered only if operator disables the interface in the configuration.</li> </ul>
Action	<ul style="list-style-type: none"> <li>• Verify the physical connectivity for the vni port that raised the alarm.</li> <li>• Check the LED status to determine if the link is UP.</li> <li>• Check the configuration to see if the interface was disabled.</li> <li>• Check the alarm log.</li> </ul> <p>If several linkup and linkDown alarms are received in a short time span for a LACP enabled interface, then it could be a faulty physical connection or LACP issue on the adjacent switch. The alarm log contains timestamps of the link events to correlate with adjacent attached devices, such as physical L2 switches or physical routers.</p>

### Interface-half-duplex Alarm

When the Versa FlexVNF's VNI interface is connected to a switch or remote end configured with a duplex mismatch settings, the interface-half-duplex alarm is raised.

Description	If the VNI interface has a mismatch of half-duplex, either locally or remoter end, the interface changes to down state and raises the interface-half-duplex alarm.
Cause	Mismatch of interface duplex configuration, either locally or remotely.
Action	Configure both end of the link with the same duplex settings.

## VRRP-v3-new-master Alarm

This table explains vrrp-v3-new-master alarm details.

Description	This alarm is generated when a VRRP group is changed to master state.
Cause	<ul style="list-style-type: none"> <li>• masterNoResponse—When master is down, VRRP group is transitioned from Backup to Master state. This is due to communication failure between the VNFs. If VNF1 is up but the group state shows INIT, then there is issue with interface or system process on VNF1.</li> <li>• If VNF1 is up and shows master state, and VNF2 shows the not incrementing highlighted counters, then there is communication failure between VNF1 and VNF2.</li> <li>• Priorit—When a VRRP group with higher priority (designated Master) comes back online, it takes over master role from other VNF.</li> <li>• Preempted—When a VRRP group with priority 255 is started, or comes back online, it takes over master role. This is because the virtual IP is same as its own interface IP.</li> </ul>

## VRRP-v3-new-backup Alarm

This table explains vrrp-v3-new-backup alarm details.

Description	This alarm is generated when a VRRP group state is changed to Backup state.
Cause	<ul style="list-style-type: none"> <li>• Startup—The VRRP group is initialized and transitioned from INIT to Backup state. This is because of any of the these: <ul style="list-style-type: none"> <li>○ VNF is powered on or services are restarted.</li> <li>○ Interface on which VRRP group is configured is disabled/enabled (reset).</li> <li>○ VRRP protocol (global) config has changed (changing protocols vrrp</li> </ul> </li> </ul>

	<p>mac-address-mode).</p> <ul style="list-style-type: none"> <li>• Priority—Another VNF comes online with higher priority. After receiving higher priority packet, the group is transitioned from Master to Backup. The <code>show vrrp group summary</code> command shows the priority and state of group on other VNF.</li> <li>• Larger IP—Another group with same priority but larger interface IP address comes online. When two VNFs are configured with same priority, then the VNF with larger interface IP address takes the Master role. The <code>show vrrp group summary</code> command shows interface IP of the groups.</li> </ul>
--	--

## VRRP-v3-proto-error Alarm

This table explains vrrp-v3-proto-error alarm details.

Description	This alarm is generated when a VRRP group encounters protocol error while receiving packets.
Cause	<ul style="list-style-type: none"> <li>• vrlIdError—Another VNF has a group, configured on the same LAN, with a group id that is not configured in the VNF generating the alarm. The <code>show vrrp group summary</code> command lists the groups configured on other VNF.</li> </ul> <p>To resolve this configuration error vrlIdError messages, either remove the group on other VNF, or create a group with same group-id in the VNF generating the alarm.</p> <ul style="list-style-type: none"> <li>• versionError— Two VRRP VNFs turn into Master if both are configured with different version (VRRPv2 and VRRPv3) -&gt; Configuration error.</li> <li>• ipTtlError— VRRP packet received does not have IP TTL set to 255.</li> <li>• checksumError—Packet received has incorrect VRRP checksum, due to malicious entity trying to peer with Versa or during interop.</li> </ul>

## System Alarms

### Overview

Versa FlexVNF sends the system alarms to alert users about CPU and memory utilization issues.

Versa FlexVNF uses CPU and memory from the guest VM or baremetal server it is installed on. Exceeding the utilization of CPU or memory raises alarms. The Versa FlexVNF uses many CPU cores and memory and is adequately sized for the intended network services. A minimum of 4 CPU cores and 4GB of RAM is recommended for proper operation of Versa FlexVNF functions. When the Versa FlexVNF CPU utilization exceeds 75%, the *cpuUtilizationHigh* alarm is raised. And at 95%, the *cpuUtilizationExceeded* alarm is raised. The default value for Versa FlexVNF memory high utilization threshold is 70% and the memory exceed threshold is 90%.

These are the system alarms sent by Versa FlexVNF:

- *cpuUtilizationExceeded*
- *cpuUtilizationHigh*
- *memUtilizationExceeded*
- *memUtilizationHigh*

**NOTE:** This alarm was introduced in Release earlier to 16.1.R1S3.

### CPU-utilization

The CPU utilization alarm is raised when the Versa FlexVNF CPU utilization exceeds the default/configured value.

Description	<p>These alarms are raised when the Versa FlexVNF CPU utilization exceeds the default/configured value:</p> <ul style="list-style-type: none"> <li>• <i>cpuUtilizationExceeded</i>—The Versa FlexVNF CPU utilization has exceeded a hard limit of 95%, and the system becomes unusable.</li> <li>• <i>cpuUtilizationHigh</i>—The Versa FlexVNF CPU utilization has exceeded a soft limit system of 75%, and the system may become unstable, unless measures are taken to reduce the utilization.</li> </ul>
Cause	A disrupting process is consuming CPU resources.

Action	<ul style="list-style-type: none"> <li>• If there are multiple CPU utilization alarms, monitor the system carefully.</li> <li>• If it is a Virtual FlexVNF platform, add more CPU from the host.</li> <li>• Check for processes that are utilizing CPU cycles or memory by executing the related show commands in the Versa CLI, and the <code>top -H</code> Ubuntu Host VM shell command.</li> <li>• If a process such as <code>vsmd</code> is using all the CPU cycles, contact Versa support for troubleshooting.</li> <li>• If the Ubuntu <code>top -H</code> command shows a worker or poller thread using all of the CPU cycles, contact Versa Networks support (<a href="mailto:support@versa-networks.com">support@versa-networks.com</a>) for further troubleshooting.</li> </ul>
--------	--

## Memory-utilization

The memory utilization alarm is raised when the Versa FlexVNF memory utilization exceeds the default/configured value.

Description	<p>These alarms are raised when the Versa FlexVNF memory utilization exceeds the default/configured value.</p> <ul style="list-style-type: none"> <li>• <code>memUtilizationExceeded</code>—The Versa FlexVNF memory utilization has exceeded a hard limit of 90%, and the system becomes unusable.</li> <li>• <code>memUtilizationHigh</code>—The Versa FlexVNF Memory utilization has crossed a soft limit of 70%, and the system becomes unstable, unless countermeasures are</li> </ul>
Action	<ul style="list-style-type: none"> <li>• If there are multiple memory utilization alarms, monitor the system carefully.</li> <li>• If it is a Virtual FlexVNF platform add more memory from the host.</li> </ul>

## Disk Utilization

The disk utilization alarm is raised when the Versa FlexVNF disk utilization exceeds the default/configured value.

Description	<p>These alarms are raised when the Versa FlexVNF disk utilization exceeds the default/configured value.</p> <ul style="list-style-type: none"> <li>• <code>diskUtilizationExceeded</code>—The Versa FlexVNF disk utilization has exceeded a hard limit of 90%, and the system becomes unusable.</li> <li>• <code>diskUtilizationHigh</code>—The Versa FlexVNF disk utilization has crossed a soft limit of 70%, and the system becomes unstable, unless countermeasures are taken</li> </ul>
Action	<p>Monitor the system carefully if there are multiple disk utilization alarms.</p>

## Device Disk error

This table explains the details of device-disk-error alarm:



---

Description	This alarm is raised when there are bad-blocks detected on the disk.
Cause	<ul style="list-style-type: none"><li>• Disk usage</li><li>• Hardware issues</li></ul>
Action	<ul style="list-style-type: none"><li>• Check the disk for software errors, using tools like fsck.</li><li>• Replace the disk if there are physical damages.</li></ul>

## Session Alarms

### Overview

Versa FlexVNF sends session utilization alarms to alert users about active session related issues. These alarms help to overcome connectivity issues and stopping of applications by facilitating optimal running of Versa FlexVNF.

**NOTE:** This alarm was introduced in Release earlier to 16.1.R1S3.

### Org-session-utilization

Versa FlexVNF uses a multi-tenant design that allows configuration of several orgs or tenants, with a maximum amount of sessions like Stateful and NextGen firewall, CGNAT etc., to enforce equality of resource sharing in the system among multiple tenants. Versa FlexVNF provides configuration to limit the number of sessions per tenant/org (default 1M). It also provides configuration knob to increase/decrease the number of sessions an appliance can support (default 1M, maximum 5M). If the tenant/org resources are appropriately sized, the session exceeded alarm is not raised. The alarms are only raised when a compromised host on that tenant's network is invalidly generating numerous sessions and traffic that appears legitimate (not DDoS traffic).

Description	<p>Consider a tenant entitled to 10,000 sessions, and that a has a default time-out of 300 seconds after no activity. If the session table reaches the capacity of 10,000 entries, no new sessions will be created until older sessions age out, or the administrator increases the maximum session count to greater than 10,000. An alarm is generated indicating that the tenant has exceeded the maximum configured session count, and additional traffic that requires a new session to be instantiated is attempting to traverse the Versa FlexVNF.</p> <p>Default value is 1 million, and maximum value is 5 million.</p> <p>The device-session-threshold alarm is similar to the org-session-threshold alarm, at a device level.</p> <p>This is a critical alarm because it indicates a halt in new session creation for an org. It also indicates that Versa FlexVNF is not running optimally. This also leads to connectivity</p>
Cause	<p>When many users access the system simultaneously, or when there is a denial of service attack where the users are trying to scan IP address of different destinations.</p>

---

Action	<p>The Org Sessions threshold exceeds when the tenant (customer) generates numerous sessions per second that do not deteriorate on time to allow creation of new sessions. This indicates that the customer needs additional session capacity and potentially higher bandwidth connection.</p> <ul style="list-style-type: none"><li>• Verify that the traffic flows generated at the time of the alarm is legitimate. For this, you must verify the source and destination IP addresses in the IPFIX records in the Versa Analytics database.</li><li>• If this traffic is legitimate, increase the org limits for total amount of sessions, to</li></ul>
--------	--

---

## Services Alarms

### Services Alarms

These are the services alarms sent by Versa FlexVNF:

- Security alarms
- IPSEC alarms
- ADC alarms
- CGNAT alarms
- DHCP alarms

**NOTE:** This alarm was introduced in Release earlier to 16.1.R1S3.

### Security Alarms

Versa FlexVNF uses zone-based protection profiles to protect against DoS attacks. This protection method implements an extensive Denial of Service (DoS) template commonly applied to the untrusted zone of the firewall. This protects the network from high volume DoS attacks and acts like the first security barrier against DoS attacks.

The zone-based protection policies prevents attacks such as floods, sweeps, malformed IP packets etc. The zone-based DDoS policies raise alarms, associated with exceeded thresholds, to alert the administrator of a DDoS attack.

Calculate the thresholds to account for the access interface speed (ie 1Gbps, 10Gbps etc). Zone Protection protects against a 'flood' of traffic. Generally the attacker uses random source or destination IP and/or port information for such attacks. Zone Protection is applied for only the first packet of a new session and this enables you to control the rate of creation of new sessions. DoS protection is similar to Zone Protection however DoS protection is either classified or aggregate and provides a fine grained control to set thresholds on a per source or per source-destination pairs.

If there is a DoS attack that exceeds the previously configured threshold then alarms are raised according to the attack type; Zone Protection flood, Zone Protection port scan, and DoS Policy threshold.

These are the alarms raised according to the attack type:

- FloodThreshold—A Zone Protection policy configured by the administrator for flood detection with an alarm threshold has been crossed.
- PscanThreshold—A Zone Protection policy configured by the administrator with port scan parameters has detected activity and the alarm threshold has been crossed.
- DDoSThreshold—A DoS Protection profile configured by the administrator for flood detection with an alarm threshold has been crossed.

## zone-protection-flood

This table explains the details of zone-protection-flood alarm:

Description	This alarm is raised when a zone protection profile configured with flood parameters detects sufficient traffic activity and exceeds the configured alarm date.
Cause	The Versa FlexVNF instance receives flood traffic (new sessions) at a rate more than the configured flood limit threshold and the traffic is destined to a range of ports of a single destination address.
Action	Review the zone profile config, adjust the alarm, and activate thresholds.

## port-scan-flood

This table explains the details of port-scan-flood alarm:

Description	This alarm is raised when a zone protection profile configured with scan parameters detects sufficient traffic activity, and exceeds the configured alarm date.
Cause	The Versa FlexVNF instance receives the flood traffic (new sessions) at a rate more than the configured scan limit threshold, and the traffic is destined to range of ports of a single destination address.
Action	Review the zone profile config, adjust the alarm, and activate thresholds.

## ddos-threshold

This table explains the details of ddos-threshold alarm:

Description	This alarm is raised when a DoS protection profile configured for flood detection with an alarm threshold is exceeded.
Cause	The Versa FlexVNF instance receives the flood traffic (new sessions) more than the configured alarm rate. All new sessions are marked as dropped after the maximal rate is reached. The main difference between Zone and DoS Protection is that Zone Protection profile is evaluated before the creation of a flow, and Dos Protection is evaluated after the creation of the flow.
Action	Review the DoS profile config, adjust the alarm, and activate thresholds.

## IPSEC Alarms

This section provides information on these IPsec alarms generated by Versa FlexVNF:

### ipsec-tunnel-down

This table explains the details of ipsec-tunnel-down alarm:

Description	This alarm is generated when the ipsec-tunnel goes down.  When an ipsec-tunnel goes down the data traffic gets affected, because the security associations to encrypt outgoing data or decrypt incoming data is not available.
-------------	--

Action	Execute related commands to check these: <ul style="list-style-type: none"> <li>• current status</li> <li>• reason for deletion of security-association</li> <li>• IKE control path</li> </ul>
--------	--

## ipsec-ike-down

This table explains the details of ipsec-ike-down alarm.

Description	This alarm is generated when the ipsec ike goes down. When the control plane goes down, ipsec-tunnel goes down. Therefore, all data traffic passing through the ipsec-tunnels created as part of this IKE tunnel will be affected.
Cause	<ul style="list-style-type: none"> <li>• If the IKE-peer is not reachable.</li> <li>• If authentication with the peer fails.</li> <li>• If encryption parameters of the peer changes.</li> </ul>
Action	Execute related commands to check these: <ul style="list-style-type: none"> <li>• if security-association is deleted</li> <li>• history</li> <li>• ping reachability between the IKE end-points</li> </ul>

## ADC Alarms

This section provides the details of these alarms raised by Versa FlexVNF:

### adc-server-down

This table explains the details of adc-server-down alarm:

Description	This alarm is generated when a backend server connected to a virtual service goes down. Versa FlexVNF periodically monitors backend server attached to a virtual service (VIP) and declares them as down if monitoring fails. Down servers do not take part in load
Cause	<ul style="list-style-type: none"> <li>• Default ICMP monitor failure</li> <li>• Custom monitor (TCP, UDP) failure</li> </ul>
Action	<ul style="list-style-type: none"> <li>• Check the connectivity between Versa FlexVNF and backend servers</li> <li>• Check the server (application VM) and ensure it's up and running</li> </ul>

### adc-vservice-down

This table explains the details of adc-vservice-down alarm:

Description	This alarm is generated when ADC virtual service (VIP) goes down.
-------------	---

Cause	When all the servers attached to VIP go down. This includes servers in both default and backup pool.
Action	Check the reason for monitoring failure of all servers causing VIP to go down.

## CGNAT Alarms

This section provides the details of the CGNAT alarms raised by Versa FlexVNF.

### cgnat-pool-utilization

This table explains the details of cgnat-pool-utilization alarm:

Description	This threshold alarm generated when the bindings allocated from the CGNAT pool cross lower/higher threshold value. The default lower threshold is set to 75% and high threshold is set to 95% of the total bindings.
Cause	This alarm is generated: <ul style="list-style-type: none"> <li>• If there is a bug in the software and if the bindings are leaked.</li> <li>• Genuine case where the number of NAT flows is actually closer to 0.2 to 0.4M sessions.</li> </ul>
Action	Check if you can increase the number of public IPs used for NAT

## DHCP Alarm

This section provides the details of the DHCP alarms raised by Versa FlexVNF.

### dhcp-pool-utilization

This table explains the details of dhcp-pool-utilization alarm.

Description	This alarm is generated when the DHCP pool utilization crosses the configured low threshold.  If the utilization increases and crosses the high threshold value then the alarm is changed to pool near exhaustion.  After the utilization falls below the low threshold, the alarm is changed to pool utilization
Cause	<ul style="list-style-type: none"> <li>• When the pool utilization crosses low threshold.</li> <li>• When the pool utilization crosses high threshold.</li> </ul>
Action	<ul style="list-style-type: none"> <li>• Run the <code>show orgs org-services Provider dhcp active-leases</code> CLI command to check the number of IP addresses issued.</li> <li>• Expand the pool range and add a new pool.</li> </ul>

## Routing Alarms

### Overview

Routing alarms are configured to get advanced notification that allows monitoring of large-scale networks. These are the routing alarms sent by Versa FlexVNF:

- nexthop-down
- monitor-down
- bgp-nbr-state-change

NOTE: This alarm was introduced in Release earlier to 16.1.R1S3.

### Nexthop-down

This table explains the details of nexthop-down alarm:

Description	This alarm gets generated when an unnamed monitor transitions to DOWN state. This impacts the service, as the next hop is not reachable.
Cause	<ul style="list-style-type: none"> <li>• The reachability to next hop may be down</li> <li>• Interface may be in down state</li> </ul>
Action	Check the datapath connectivity.

### Monitor-down

This table explains the details of monitor-down alarm:

Description	This alarm is generated when a named monitor transitions to DOWN state. This impacts the service, as the next hop is not reachable.
Cause	<ul style="list-style-type: none"> <li>• Datapath to the reachability of the monitored Nexthop has issues.</li> <li>• Network link issues.</li> <li>• Dropped packets</li> </ul>
Action	Check the data path connectivity.

### BGP-nbr-state-change

This table explains the details of bgp-nbr-state-change alarm:

Description	This alarm is raised when there is a change in BGP neighbor connection state. This impacts the service, as BGP session to the neighbor goes down.
-------------	---



---

Cause	<ul style="list-style-type: none"><li>• Interface on which the BGP neighbor ship formed goes down.</li><li>• Changes in remote end BGP configuration.</li><li>• Reset of BGP neighbor on remote end.</li></ul>
Action	<ul style="list-style-type: none"><li>• Ping the BGP neighbor address to check the reason for BGP session going down. This is either due to controller going down or datapath connectivity issue.</li><li>• If the controller is UP and ping is not working, find the state of IPSEC session to the controller, and debug datapath connectivity.</li></ul>

## SD-WAN Alarms

### Overview

SD-WAN alarms are used to trigger alerts about issues in the SD-WAN environment. These are the SD-WAN alarms sent by Versa FlexVNF:

- sdwan-branch-disconnect
- sdwan-datapath-down
- sdwan-datapath-sla-not-met

**NOTE:** This alarm was introduced in Release earlier to 16.1.R1S3.

### SDwan-branch-disconnect

This table explains the details of sdwan-branch-disconnect alarm:

Description	This alarm is generated on a controller when it loses connectivity on all the overlay paths.
Cause	<ul style="list-style-type: none"> <li>• If a branch reboots.</li> <li>• If there is a software crash.</li> <li>• If the system reboots or is switched off.</li> <li>• If WAN interface is flapped.</li> <li>• If path goes down due to intermediate router issue, then icmp monitoring to nexthop gateway detects the failure.</li> </ul>

### SDwan-datapath-down

This table explains the details of sdwan-datapath-down alarm:

Description	This alarm is generated on a branch/hub or controller, when a branch/controller drops connectivity on an overlay path for a specific traffic class.
Cause	<ul style="list-style-type: none"> <li>• If local WAN link or remote WAN link is down.</li> <li>• If there is an intermediate router issue.</li> <li>• If there is a percentage PDU loss or actual traffic loss on the path.</li> </ul>

Action	<ul style="list-style-type: none"> <li>• Verify the interface state or check for interface alarms .</li> <li>• If the WAN link is down, then the path gets removed and is not displayed on the SLA monitor status command.</li> <li>• If the SLAs are flapping due to congestion issue on the local or remote site, then the forwarding class drops. Run the <code>show orgs org-services Customer1 class-of-service interfaces brief</code> or <code>detail</code> command to check if there are any drops in the transmit director.</li> <li>• Use SLA metrics show command to display percentage PDU loss or actual traffic loss.</li> </ul>
--------	---

## SDwan-datapath-sla-not-met

This table explains the details of sdwan-datapath-sla-not-met alarm:

Description	This alarm is generated on the branch/hub per SD-WAN rule when the SLA metrics does not comply with configured value for the rule.
Cause	If the class of service is enabled and if there are drops for the forwarding class.
Action	<ul style="list-style-type: none"> <li>• Check the path state command to display the status and the reason for the violation using the related show commands.</li> <li>• Check current SLA metrics by running SLA metrics show command.</li> </ul>

## Software Alarms

### Overview

Software alarms are configured to trigger alerts about issues in Versa FlexVNF software. These are the software alarms:

- software-version-change
- software-upgrade-success
- software-upgrade-failure
- software-rollback-failure
- software-key-about-to-expire
- software-trial-expired
- software-trial-error
- appliance-not-subjugated
- app-stopped

**NOTE:** This alarm was introduced in Release earlier to 16.1.R1S3.

### Software-version-change

This table explains the details of software-version-change alarm:

Description	This alarm is raised when the Versa FlexVNF package version changes.
Cause	Software upgrade or rollback.
Action	No specific action is required.

### Software-upgrade-success

This table explains the details of software-upgrade-success alarm:

Description	This alarm is raised when a Versa FlexVNF package upgrade is successful.
Cause	This alarm is generated after initiating the Versa FlexVNF software upgrade either through the Versa Director GUI/Versa FlexVNF CLI. This alarm indicates successful software upgrade.
Action	No specific action is required. This is an informational alarm for a user to know software upgrade result.

### Software-upgrade-failure

This table explains the details of software-upgrade-failure alarm:

Description	This alarm is raised when a Versa FlexVNF package upgrade fails.
Cause	This alarm is generated after administrator initiates Versa FlexVNF software upgrade, either through the Versa Director GUI/Versa FlexVNF CLI. This alarm indicates software upgrade failure.
Action	An error message is shown on the console when upgraded from CLI, or in the task menu when upgraded using GUI. The details are available in the debug logs (/var/log/versa/upgrade.log). Run an upgrade after rectifying the issue.

## Software-rollback-failure

This table explains the details of software-rollback-failure alarm:

Description	This alarm is raised when a Versa FlexVNF package upgrade fails, followed by a rollback failure.
Cause	When a Versa FlexVNF package upgrade fails, the system attempts an automatic rollback to the previous package. and if rollback fails, this alarm is raised.
Action	The system is in unstable state. Contact Versa support to help restore the host.

## Software-key-about-to-expire

This table explains the details of software-key-about-to-expire alarm:

Description	A Versa FlexVNF software comes with pre-installed key that is valid for 45 days. When there are 7 days for the key to expire, this alarm is raised every day as a reminder to either extend the evaluation period, or check for connectivity issues.
Cause	<ul style="list-style-type: none"> <li>• Evaluation period of 45 days is about to expire.</li> <li>• Connection to Versa Director is not up. By default, Versa FlexVNF waits for 7 days for NETCONF connection to establish, before starting eval period again.</li> </ul>
Action	<ul style="list-style-type: none"> <li>• If you are running evaluation copy of Versa FlexVNF software, contact Versa Support to either purchase license/extend evaluation period.</li> <li>• Check the reason for connectivity issues.</li> </ul>

## Software-trial-expired

This table explains the details of software-trial-expired alarm:

Description	Versa FlexVNF software comes with a pre-installed key with 45 days validity. This key, or a new key that was later installed, has expired.
Cause	Versa FlexVNF has lost connection to the Versa Director or the Versa FlexVNF is not subjugated to Versa Director. Refer to <a href="#">appliance-not-subjugated</a> .

Action	<ul style="list-style-type: none"> <li>• Contact Versa Support to either purchase license/extend evaluation period, if you are running evaluation copy of the Versa FlexVNF software.</li> <li>• Check the reason for connectivity issues.</li> </ul>
--------	---

## Software-trial-error

This table explains the details of software-trial-error alarm:

Description	This alarm is raised when a Versa FlexVNF software is tampered to alter the evaluation period tracking.
Cause	<ul style="list-style-type: none"> <li>• An accidental change/tampering of the Versa FlexVNF files.</li> <li>• A file system error, or disk being full.</li> </ul>
Action	Contact Versa Support.

## Appliance-not-subjugated

This table explains the details of appliance-not-subjugated alarm:

Description	Versa FlexVNF device is marked as subjugated on connecting to the Versa Director for the first time. If the device is not marked as subjugated, this alarm is raised every time a Versa FlexVNF service is restarted.
Cause	Connectivity to Versa Director is irregular or not up.
Action	Contact Versa Support.

## App-stopped

An application alarm is raised when there is an application failure. This table explains the details of app-stopped alarm:

Description	<p>The Versa FlexVNF uses applications/daemons to perform various system and network services tasks. When the Versa FlexVNF is in good health, all application processes are in running state.</p> <p>When an application fails, Versa FlexVNF raises an alarm, with the application name and status reported in the alarm text.</p>
Cause	<ul style="list-style-type: none"> <li>• When an application goes down due to an administrative command to shut down the application, or due to a crash that causes the application to stop running.</li> <li>• When an application is up to running state due to an administrative restart, or due to automatic restart after an application crash.</li> </ul>

---

Action	<ul style="list-style-type: none"><li>• If any of the Versa FlexVNF application processes stops or restarts, debug the error.</li><li>• The Versa FlexVNF keeps extensive logs for each of the key application processes in the <code>/var/log/versa</code> directory. Each application process is identified by its name and has a suffix of <code>.log</code>.<ul style="list-style-type: none"><li>• View clear text logs using the the Linux command <code>tail -f &lt;versa-application-name.log&gt;</code>.</li><li>• View historical information using <code>cat</code> or <code>more</code> Linux commands in conjunction with the specific application log name.</li><li>• Check the <code>/var/tmp/versa-cores</code> or run the <code>show coredumps</code> CLI command to see if there is a core file with the name of the application that stopped/restarted. If a core file exists, contact Versa Networks support (<a href="mailto:support@versa-networks.com">support@versa-networks.com</a>)</li></ul></li></ul>
--------	---

---

## High Availability Alarms

### Overview

High Availability (HA) alarms are generated when there is a change in the HA role type

The Versa FlexVNF uses an advanced active/standby HA design, that allows configuration of redundant services. Configuration of redundant services across two VNFs helps in:

- Maximizing service uptime.
- Protection against hardware and software failures.
- Protection against local network connectivity issues such as link or physical switch/router failures.

Enabling protocols like BFD and LACP on the Versa FlexVNF interfaces help in resiliency and detecting protocol level failures in connected devices. This helps to expedite actions when a failure is detected by these state machine protocols.

The HA triggerType is determined by a switchover trigger policy definition, based on the interfaces and the routing-peers to be tracked. Low watermarks defined by interface-count, routing-peer-count, and vrrp-group-count in the rule match condition specifies the trigger action. All the configuration conditions have to be met before the Versa FlexVNF takes action based on the trigger policy. If the action is specified as switchover, and if the standby VNF has a greater number of tracked routing-peers, active interfaces, and active VRRP groups, then the system will switchover to make the standby node as the active node.

The triggerType alarm indicates the reason for the failover. Greater number of available interfaces due to an LACP down event or interface down event on the former active VNF are the reasons for failover. The switchover trigger can also be due to manual switchover using request redundancy interchassis appliance-master-switch CLI command.

Additionally, if the Versa FlexVNF control plane or data plane process fails on the active VNF, or if there is a BFD failure over the control plane data connection, this information is populated in the trigger type alarm. These events occur due to IP connectivity failure between the active and standby VNF.

These are the HA alarms sent by Versa FlexVNF:

- ha-sync-status
- ha-state-change

NOTE: This alarm was introduced in Release earlier to 16.1.R1S3.

### Ha-sync-status & ha-state-change

This table explains the details of HA alarms:



Description	There are two HA role types; master (active) and standby. The configuration parameters determine the Versa FlexVNF HA role type. In case of active Versa FlexVNF failure, there is a mastership change, and the standby notifies the administrator with an alarm indicating a role change. The <i>haTriggerType</i> alarm specifies the reason for the HA role type change.
Cause	<ul style="list-style-type: none"> <li>• Change in state of active VNF, standby VNF, or control protocols.</li> <li>• Link failure detected by LACP.</li> <li>• Loss of physical link, or time-out of BFD session between the active and standby VNF.</li> <li>• IP connectivity failure between the active and standby VNF.</li> </ul>
Action	<ul style="list-style-type: none"> <li>• Verify both Versa FlexVNFs are reachable and that all processes are running.</li> <li>• Verify the control link/physical link between the two Versa FlexVNFs, and check if the BFD session is UP running, using the related show commands.</li> <li>• View the HA and BFD events in the alarm log to find the initial cause of the failover.</li> <li>• Verify the uptime of the system for both Versa FlexVNFs. If the uptime is not as expected, check if for crashed processes, and check for any core dump files.</li> </ul>

## Summary Statistics of Alarms on Versa FlexVNF

admin@vCPE101-cli> show device alarm

ALARM		NUM NEW	NUM CHANGED	NUM CLEARED	NUM NETCONF	NUM SNMP	NUM SYSLOG	NUM ANALYTICS
ID	ALARM NAME	ALARMS	ALARMS	ALARMS	ALARMS	ALARMS	ALARMS	ALARMS
0	cpu-utilization	0	0	0	0	0	0	0
1	memory-utilization	0	0	0	0	0	0	0
2	disk-utilization	0	0	0	0	0	0	0
3	log-disk-utilization	0	0	0	0	0	0	0
4	org-session-utilization	0	0	0	0	0	0	0
5	device-session-utilization	0	0	0	0	0	0	0
6	interface-down	0	0	2	0	0	2	0
7	uplink-bw-threshold	0	0	0	0	0	0	0
8	dnlink-bw-threshold	0	0	0	0	0	0	0
9	ha-state-change	0	0	0	0	0	0	0

10	ha-sync-status	1	0	0	0	0	1	1
11	scale-in	0	0	0	0	0	0	0
12	scale-out	0	0	0	0	0	0	0
13	scale-out-complete	0	0	0	0	0	0	0
14	vsn-down	0	0	0	0	0	0	0
15	vsn-state	0	0	0	0	0	0	0
16	adc-vpel-event	0	0	0	0	0	0	0
17	adc-server-down	0	0	0	0	0	0	0
18	adc-vservice-down	0	0	0	0	0	0	0
19	cgnat-pool-utilization	0	0	0	0	0	0	0
20	snat-pool-utilization	0	0	0	0	0	0	0
21	ipsec-tunnel-down	0	0	0	0	0	0	0
22	ipsec-ike-down	0	0	0	0	0	0	0
23	bgp-nbr-state-change	0	0	0	0	0	0	0
24	hnp-nbr-max-prefix	0	0	0	0	0	0	0

The `show device alarm` CLI command provides a quick view of all the alarms stats that are generated by the device based on the output, for analysis. The alarm stats are viewed to detect discrepancies.

## Related Commands

Run the `show device alarms` CLI command to view the device alarm details.

25	bop-nbr-max-prefix-threshold	0	0	0	0	0	0	0
26	ospf-nbr-state-change	0	0	0	0	0	0	0
27	ospf-if-state-change	0	0	0	0	0	0	0
28	ospf-nssa-trans-change	0	0	0	0	0	0	0
29	ospf-if-auth-failure	0	0	0	0	0	0	0
30	vrrp-v3-new-master	0	0	0	0	0	0	0
31	vrrp-v3-new-backup	0	0	0	0	0	0	0
32	vrrp-v3-proto-error	0	0	0	0	0	0	0
33	ddos-threshold	0	0	0	0	0	0	0
34	zone-protection-flood	0	0	0	0	0	0	0
35	port-scan-flood	0	0	0	0	0	0	0
36	sdwan-branch-connect	0	0	0	0	0	0	0
37	sdwan-branch-disconnect	0	0	0	0	0	0	0
38	sdwan-branch-info-update	0	0	0	0	0	0	0
39	sdwan-datapath-dow	0	0	0	0	0	0	0
40	sdwan-nbr-datapath-down	0	0	0	0	0	0	0
41	sdwan-datapath-sla-not-met	0	0	0	0	0	0	0
42	branch-in-maintenance-mode	0	0	0	0	0	0	0

---

43	dhcp-pool-utilization	0	0	0	0	0	0	0
44	device-disk-errors	0	0	0	0	0	0	0
45	device-mem-errors	0	0	0	0	0	0	0
46	appliance-not-subjugated	1	0	0	0	0	0	0
47	app-stopped	1	0	12	0	0	13	13
48	software-version-change	0	0	0	0	0	0	0
49	software-upgrade-success	0	0	0	0	0	0	0
50	software-upgrade-failure	0	0	0	0	0	0	0
51	software-rollback-success	0	0	0	0	0	0	0
52	software-rollback-failure	0	0	0	0	0	0	0
53	package-fetch-success	0	0	0	0	0	0	0
54	package-fetch-failure	0	0	0	0	0	0	0
55	software-trial-expired	0	0	0	0	0	0	0
56	software-trial-error	0	0	0	0	0	0	0
57	interface-half-duplex	0	0	0	0	0	0	0
58	ospf-if-cfg-failure	0	0	0	0	0	0	0
59	nexthop-down	0	0	1	0	0	1	1
60	monitor-down	0	0	0	0	0	0	0
61	software-key-about-to-expire	0	0	0	0	0	0	0