
Configure VOS Device Alarms

 For supported software information, click [here](#).

Versa Operating System™ (VOS™) device alarms provide real-time status about services and activities that require attention. The severity level associated with an alarm provides an indication of the gravity of the situation.

By default, alarms are sent to Versa Analytics and are then streamed to Versa Director. You can configure alarms to stream them to any third-party collector. Versa Analytics stores alarms in its database for diagnostics and internal usage purposes only. By default, this data is purged automatically after seven days. You can modify the purge timer settings.

Supported Alarm Types

The following table lists the alarm types supported by VOS devices and the default destination for the alarm types. Note that the Netconf destination has been deprecated.

Alarm Type	Description	Default Destination	Severity
adc-server-down	Backend server did not respond to application delivery controller (ADC) monitors within the configured time. After server is marked down, it is not considered for load balancing.	Analytics, SNMP, syslog	Major
adc-vservice-down	All backend servers attached to a virtual service have been declared down because of a monitor health failure. No traffic is served by this virtual service (VIP).	Analytics, SNMP, syslog	Critical
adc-vpel-event	ADC VPEL event occurred.	Analytics, SNMP, syslog	Critical
app-stopped	An application went down.	Analytics, syslog	Indeterminate

Alarm Type	Description	Default Destination	Severity
address-group-file-compilation-failure	(For Releases 22.1.3 and later.) Address group file compilation failed.	Analytics, SNMP, syslog	Major
address-group-file-compilation-success	(For Releases 22.1.3 and later.) Address group file compilation succeeded.	None	Indeterminate
appliance-not-subjugated	Appliance was not subjugated to Versa Director.	Analytics	Indeterminate
application-monitor-down	(For Releases 22.1.1 and later.) Application monitor down (monitor failure).	Analytics	
app-stopped	An application went down.	Analytics, syslog	Indeterminate
bgp-nbr-max-prefix	Number of prefixes that a BGP instance can receive per session from its peer is nearing the maximum configured value.	Analytics, SNMP, syslog	Major
bgp-nbr-max-prefix-threshold	Number of prefixes that a BGP instance can receive per session from its peer has been exceeded.	Analytics, SNMP, syslog	Major
bgp-nbr-state-change	BGP peer session went down or come back up. Note that the default soak time for this alarm is 0 seconds.	Analytics, SNMP, syslog	Critical
branch-in-maintenance-mode	Branch went down because of non-recoverable failure, and a fallback IPsec connection was created between the branch and the Controller.	Analytics, SNMP, syslog	Critical
branch-ready-for-staging	Branch is ready for staging.	Analytics, SNMP, syslog	Minor

Alarm Type	Description	Default Destination	Severity
ca-server-url-not-resolved	(For Releases 22.1.1 and later.) Failed to resolve the CA server URL.	Syslog	Major
certificate-about-to-expire	(For Releases 22.1.1 and later.) Certificate is about to expire.	Analytics, syslog	
cgnat-pool-utilization	CGNAT pool size exceeded the configured threshold value, or CGNAT pool is exhausted.	Analytics, SNMP, syslog	Major, Critical
config-change	The configuration changed.	Analytics, syslog	Major
copp-threshold	(For Releases 22.1.3 and later.) Control plane policing threshold exceeded.	Analytics, SNMP, syslog	Major, Critical
cpu-health	VOS device CPU crossed the configured threshold. This alarm is deprecated in Releases 22.1.2 and later.	Analytics, SNMP, syslog	Major, Critical
cpu-utilization	Data path CPU utilization exceeded the configured threshold value.	Analytics, SNMP, syslog	Major, Critical
ddos-threshold	DDoS traffic exceeded the configured aggregate or classified DDoS threshold.	Analytics, SNMP, syslog	Major, Critical
deprecated-appid-configured	A policy configuration includes a deprecated application ID.	Analytics, SNMP, syslog	Warning
device-cpu-high-temp	One or more CPU cores crossed the high temperature threshold (70°C).	Analytics, syslog	Critical

Alarm Type	Description	Default Destination	Severity
device-disk-errors	Bad blocks were detected on the disk.	Analytics	Critical
device-session-utilization	Current number of sessions for a device or an appliance exceeded the configured value.	None	Major, Critical
dhcp-ip-declined	Client declined the DHCP IP address.	Analytics, SNMP, syslog	Warning
dhcp-pool-utilization	DHCP addresses were exhausted, and no more addresses could be allocated from the DHCP address pool. To generate this alarm, you must enable Log Utilization on the Add Lease Profile window when you configure a DHCP lease profile for the DHCP server. For more information, see Configure a DHCP Lease Profile .	Analytics, SNMP, syslog	Major, Critical
director-ping	Director node initiated a ping request.	None	Major
disk-utilization	Disk utilization exceeded the configured threshold value.	None	Major, Critical
dnlink-bw-threshold	Current downlink bandwidth for an interfaces exceeded the configured value.	None	Major, Critical
duplicate-ip	(For Releases 22.1.1 and later.) Duplicate IP packet detected.	Analytics, SNMP, syslog	Warning
dynamic-provisioning	One of the following conditions occurred: <ul style="list-style-type: none"> • Tenant on a VOS 	Analytics, SNMP, syslog	Minor

Alarm Type	Description	Default Destination	Severity
	<p>device was provisioned or deprovisioned.</p> <ul style="list-style-type: none"> • New VOS device, such as a hub or spoke, was spawned in AWS or Azure. • VOS device created on AWS or Azure was destroyed dynamically because of low utilization 		
evpn-dup-mac-error	A duplicate MAC detection error occurred.	Analytics, SNMP, syslog	Major
evpn-sticky-mac-error	Layer 2 MAC address pinning error occurred.	Analytics, SNMP, syslog	Major
fexd-auth-server-token-failure	(For Releases 22.1.1 and later.) ATP cloud file export access token failed.	Analytics, SNMP, syslog	Critical
fexd-fss-connect-failure	(For Releases 22.1.1 and later.) ATP cloud file export file submit system connection failed.	Analytics, SNMP, syslog	Critical
fexd-fss-export-latency-failure	(For Releases 22.1.1 and later.) ATP cloud file export result notification service connection failed.	Analytics, SNMP, syslog	Critical
fexd-rns-connect-failure	(For Releases 22.1.1 and later.) ATP cloud file export result notification service connection failed.	Analytics, SNMP, syslog	Critical
flexvnf-restart	A VOS device restarted	Analytics, syslog	Major

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_VOS_...

Updated: Wed, 23 Oct 2024 08:23:26 GMT

Copyright © 2024, Versa Networks, Inc.

Alarm Type	Description	Default Destination	Severity
	and Versa services restarted. This can happen if you manually reboot a system using the CLI or if the system automatically restarts because of a service restart.		
flow-health	VOS device flows crossed the configured threshold.	Analytics, SNMP, syslog	Major, Critical
guest-vnf-down	Guest VNF on a uCPE device is down.	Analytics, SNMP, syslog	Critical
ha-peer-state-req	Interchassis HA peer VOS node standby device initiated health check of its peer as a measure to avoid split-brain state.	Analytics, SNMP, syslog	Major
ha-quorum-evaluation	HA quorum evaluation started to determine whether active node is present.	Analytics, SNMP, syslog	Major
ha-quorum-result	HA quorum evaluation result is available.	Analytics, SNMP, syslog	Major
ha-state-change	HA state changed from active to backup, or vice versa.	Analytics, SNMP, syslog	Indeterminate
ha-sync-state-change	HA synchronization state was paused or unpaused.	Analytics, SNMP, syslog	Critical
ha-sync-status	Configuration sync occurred between active and standby. The message "sync error" or "sync ok" is reported.	Analytics, SNMP, syslog	Indeterminate
interface-down	Interface or subinterface went down.	Analytics, SNMP, syslog	Major
interface-half-duplex	Interface was detected to be in half-duplex mode.	Analytics, SNMP, syslog	Indeterminate

Alarm Type	Description	Default Destination	Severity
ipguard-vsync-update-failure	Vsync update failed.	Analytics, SNMP, syslog	Warning
ipguard-vsync-update-success	Vsync updated succeeded.	None	Warning
iprep-engine-load-failure	IP reputation engine failed to load, and IP filtering might no longer work.	Analytics, SNMP, syslog	Warning
ipsec-ike-auth-failure	IKE authentication with a peer failed.	Analytics, SNMP, syslog	Major
ipsec-ike-down	IKE connection to a peer went down.	Analytics, SNMP, syslog	Major
ipsec-tunnel-down	IPsec tunnel to a peer went down.	Analytics, SNMP, syslog	Major
l2-lldp-nbr-change	LLDP neighbor on an interface changed.	Analytics, SNMP, syslog	Major
l2-lldp-nbr-native-vlan-mismatch	LLDP neighbor's native VLAN did not match local native VLAN.	Analytics, SNMP, syslog	Major
l2-mac-limit	Maximum number of MAC addresses that can be dynamically learned was reached or cleared.	Analytics, SNMP, syslog	Major
l2-mac-move-state-change	Switch updated its Layer 2 forwarding table because it received a packet whose MAC address matched an existing entry but arrived on a different port than in the existing forwarding table entry.	Analytics, SNMP, syslog	Major
l2-stp-role-change	Role of a Layer 2 STP interface changed.	Analytics, SNMP, syslog	Major
l2-stp-root-change	Layer 2 STP root interface changed.	Analytics, SNMP, syslog	Major
l2-stp-state-change	State of a Layer 2 STP interface changed.	Analytics, SNMP, syslog	Major

Alarm Type	Description	Default Destination	Severity
ldap-server-connection-status	(For Releases 22.1.1 and later.) Connection status of LDAP servers.	Analytics, SNMP, syslog	Critical
lef-collector-queue-utilization	Number of logs queued to be sent by a log collector exceeds the pending queue threshold. The default pending queue size limit is 2048 logs. To modify the limit, see Configure a Collector .	Analytics, SNMP, syslog	Major, Critical
mbuf-health	VOS device free buffers crossed the configured threshold.	Analytics, SNMP, syslog	Major, Critical
memory-health	VOS device memory crossed the configured threshold. This alarm is deprecated in Releases 22.1.2 and later.	Analytics, SNMP, syslog	Major, Critical
memory-utilization	Data path memory utilization exceeded the configured threshold value.	Analytics, SNMP, syslog	Major, Critical
monitor-down	IP destinations that are part of the monitor did not respond to the specified type of probe packets. After the monitor is marked down, dependent routes are withdrawn and redistribution policies are recomputed.	Analytics, SNMP, syslog	Major
monitor-group-down	A monitor member state changed, which resulted in the state change of the monitor group.	Analytics, SNMP, syslog	Indeterminate
multihost-netconf-connect	Both Director nodes in a DCA pair were in active state and both established	Analytics	Critical

Alarm Type	Description	Default Destination	Severity
	<p>a separate Netconf session to a CPE.</p> <p>To clear the alarm, set the active and passive roles separately for both Director nodes. Then, the Netconf session between the passive Director node and the CPE is automatically taken down.</p>		
netconf-commit-auto-rollback	When the IPsec connection between a branch and a Controller node is lost, the branch node automatically rolls back the last configuration change performed from the Versa Director.	syslog	Major
new-osspace-available	New OS SPack bundle for OS security patches is available to be downloaded.	Analytics	Indeterminate
nexthop-down	Next-hop gateway did not respond to monitors. After the next hop is marked down, routes are withdrawn.	Analytics, SNMP, syslog	Major
nexthop-sla-not-met	Next-hop gateway did not meet the configured SLA or once again met the configured SLA.	Analytics	Major
ocsp-cache-entry-timeout	Online Certificate Status Protocol cache entry expired.	Analytics, syslog	Major
ocsp-responder-down	OSCP responder is unavailable.	Analytics, syslog	Critical

Alarm Type	Description	Default Destination	Severity
ocsp-responder-url-not-resolved	(For Releases 22.1.1 and later.) Failed to resolve OCSP responder URL.	Syslog	Major
ocsp-unknown-response-received	VOS device received. an unknown response from a CA peer.	Analytics, syslog	Major
org-session-utilization	Current number of sessions for an organization (tenant) exceeded the configured value.	None	Major, Critical
ospf-nbr-state-change	OSPF adjacency went down or come back up.	Analytics, SNMP, syslog	Major
ospf-if-auth-failure	Authentication failed on an OSPF interface.	Analytics, SNMP, syslog	Major
ospf-if-cfg-failure	Configuration of an OSPF interface failed.	Analytics, SNMP, syslog	Major
ospf-if-state-change	OSPF interface went down or come back up.	Analytics, SNMP, syslog	Major
ospf-nssa-trans-change	OSPF NSSA interface went down or came back up.	Analytics, SNMP, syslog	Major
osspack-download-failure	New OS SPack download failed.	Analytics, SNMP, syslog	Indeterminate
osspack-download-success	New OS SPack was downloaded successfully.	Analytics, SNMP, syslog	Indeterminate
osspack-installation-failure	OS SPack installation on VOS device failed.	Analytics, SNMP, syslog	Indeterminate
osspack-installation-status	Installation of an OS SPack succeeded or failed.	Analytics	Indeterminate
osspack-installation-success	OS SPack installation on VOS device succeeded.	Analytics, SNMP, syslog	Indeterminate

Alarm Type	Description	Default Destination	Severity
package-fetch-failure	VOS software packet fetch (remote copy) failed.	Analytics, syslog	Major
package-fetch-success	VOS software packet fetched successfully.	Analytics, syslog	Major
pim-cbsr-state-change	PIM candidate bootstrap router state changed.	Analytics, SNMP, syslog	Major
pim-ebsr-state-change	PIM elected bootstrap router state changed.	Analytics, SNMP, syslog	Major
pim-if-state-change	PIM interface state changed.	Analytics, SNMP, syslog	Major
pim-nbr-state-change	PIM neighbor went down.	Analytics, SNMP, syslog	Major
port-scan-flood	Port scan from a source to a destination exceeded the configured zone protection profile value.	Analytics, SNMP, syslog	Major, Critical
power-supply-status	Power supply failed.	Analytics	Critical
scale-in	A scale-in occurred because of low CPU or low load on a Versa service node group.	Analytics, SNMP, syslog	Critical
scale-out	A scale-out occurred because of low CPU or low load on a Versa service node group.	Analytics, SNMP, syslog	Warning
scale-out-complete	A scale-out on a Versa service node group completed.	Analytics, SNMP, syslog	Major
sdwan-branch-connect	Branch connected to the Controller node.	Analytics, SNMP, syslog	Minor
sdwan-branch-disconnect	Branch disconnected from the Controller node.	Analytics, SNMP, syslog	Critical
sdwan-branch-info-update	Report status of branch connection to the	Analytics	Minor

Alarm Type	Description	Default Destination	Severity
	Controller node.		
sdwan-branch-lte-only-transport	VOS branch device is reachable only on LTE transport paths.	Director, through Netconf	Minor
sdwan-datapath-down	All paths between two branches went down.	Analytics (from Controller)	Critical
sdwan-datapath-sla-not-met	Path between two branches for a particular traffic class did not meet SLA.	Analytics, SNMP, syslog	Major
sdwan-duplicate-branch	(For Releases 22.1.3 and later.) Duplicate SD-WAN branch detected.	Analytics, SNMP, syslog	Critical
sdwan-duplicate-tunnel-ip	(For Releases 22.1.3 and later.) Duplicate SD-WAN tunnel IP detected.	Analytics, SNMP, syslog	Critical
sdwan-nbr-datapath-down	This alarm is deprecated..	Analytics, SNMP, syslog	
sdwan-wan-ip-change	(For Releases 22.1.3 and later.) A WAN IP address changed.	Analytics, SNMP, syslog	
snat-pool-utilization	SNAT pool size exceeded the configured threshold value, or SNAT pool is exhausted.	Analytics, SNMP, syslog	Major, Critical
sng-down	A monitor associated with a service node group when down.	Analytics, SNMP, syslog	Critical
software-key-about-to-expire	VOS device key expires soon. Contact Versa Support to replace with a	Analytics	Critical

Alarm Type	Description	Default Destination	Severity
	new key. For unrestricted usage, ensure that the VOS device is subjugated to the Versa Director and that there is connectivity between the VOS device and the Versa Director.		
software-rollback-failure	VOS software rollback failed when the rollback occurred because of an upgrade failure.	Analytics	Major
software-rollback-success	VOS software rollback succeeded when the rollback occurred because of an upgrade failure.	Analytics, syslog	Indeterminate
software-trial-error	VOS software trial key was tampered with.	Analytics	Critical
software-trial-expired	VOS software trial period expired.	Analytics	Major
software-upgrade-failure	VOS software upgrade failed.	Analytics	Major
software-upgrade-success	VOS software upgrade succeeded.	Analytics, syslog	Indeterminate
software-version-change	VOS software was upgraded.	Analytics, syslog	Indeterminate
spack-download-failure	SPack download to VOS device failed.	Analytics, SNMP, syslog	Indeterminate
spack-download-success	SPack download to VOS device succeeded.	Analytics, SNMP, syslog	Indeterminate
spack-installation-failure	SPack installation on VOS device failed.	Analytics, SNMP, syslog	Indeterminate
spack-installation-success	SPack installation on VOS device succeeded.	Analytics, SNMP, syslog	Indeterminate
spoof-device	(For Releases 22.1.3 and later.) Spoofed device	Analytics, SNMP, syslog	

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_VOS_...

Updated: Wed, 23 Oct 2024 08:23:26 GMT

Copyright © 2024, Versa Networks, Inc.

Alarm Type	Description	Default Destination	Severity
	detected.		
svc-load-health	VOS device service load crossed the configured threshold.	Analytics, SNMP, syslog	Major, Critical
twamp-session-event	Sender or reflector session was created or deleted	Analytics, SNMP, syslog	Major
uplink-bw-threshold	Current uplink bandwidth for an interface exceeded the configured value.	None	Major, Critical
urlf-async-update-failure	(For Releases 22.1.3 and later.) URL-filtering vsync update failed.	Analytics, SNMP, syslog	Critical
urlf-async-update-success	(For Releases 22.1.3 and later.) URL-filtering vsync update succeeded.	None	Minor
vms-download-failure	Virtual messaging server software download failed	Analytics, SNMP, syslog	Indeterminate
vms-download-success	VMS software download succeeded.	Analytics, SNMP, syslog	Indeterminate
vms-installation-failure	VMS software installation failed.	Analytics, SNMP, syslog	Indeterminate
vms-installation-success	VMS software installation succeeded.	Analytics, SNMP, syslog	Indeterminate
vrrp-v3-backup-not-available	VRRP backup went down.	Analytics, SNMP, syslog	Critical
vrrp-v3-new-backup	VRRP router transitioned to backup state.	Analytics, SNMP, syslog	Indeterminate
vrrp-v3-new-master	VRRP router transitioned to active state.	Analytics, SNMP, syslog	Indeterminate
vrrp-v3-protocol-error	VRRP router encountered a protocol error, such as a version mismatch,	Analytics, SNMP, syslog	Indeterminate

Alarm Type	Description	Default Destination	Severity
	checksum error, or VRRP group ID mismatch.		
vsn-state	Generated to notify the Versa service node state.	Analytics	Major
vsync-file-download-failure	(For Releases 22.1.3 and later.) Vsync file download failed.	Analytics, SNMP, syslog	Warning
vsync-file-download-success	(For Releases 22.1.3 and later.) Vsync file download succeeded.	Analytics	Indeterminate
vsync-file-validation-failure	(For Releases 22.1.3 and later.) Vsync file validation failed.	Analytics, SNMP, syslog	Major
vsync-invalid-incremental-patch	(For Releases 22.1.3 and later.) Invalid vsync patch for incremental update.	Analytics, SNMP, syslog	Major
zone-protection-flood	Flood traffic exceeded the configured zone protection threshold value.	Analytics, SNMP, syslog	Major, Critical

Alarm Severity Levels

VOS device alarms can one of the following severity levels:

- **Cleared**—One or more previously reported alarms have been cleared. More specifically, all alarms for the managed object with the same alarm type, cause, and specific problem have been cleared. 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.
- **Critical**—A service-affecting condition is present for which an immediate corrective action is required. For a critical alarm, the managed object is completely unable to provide its services.
- **Indeterminate**—The severity level cannot be determined.
- **Major**—A service-affecting condition is present for which an urgent corrective action is required. For a major alarm, the services of the managed object are severely degraded, but they are still being provided.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_VOS...

Updated: Wed, 23 Oct 2024 08:23:26 GMT

Copyright © 2024, Versa Networks, Inc.

- ## Alarm Destinations

The diagram illustrates the flow of log processing in a Versa network environment. It features several components and their interactions:

- Syslog Servers:** Two Syslog Servers are shown on the left. They receive logs from the VOS Device Branch (labeled with a green circle 3) and send them to the Versa Controller (labeled with a green circle 3).
- Versa Controller:** The central component that receives logs from the Syslog Servers and the VOS Device Branch. It sends logs to the Versa Director (labeled with a green circle 3) and the Versa Analytics (labeled with a green circle 3).
- Versa Director:** Receives logs from the Versa Controller and sends them to the Versa Analytics (labeled with a green circle 1).
- Versa Analytics:** Receives logs from the Versa Controller and the Versa Director. It sends logs to the External Collector (labeled with a yellow circle 5) and the Local log file (labeled with a yellow circle 5).
- VOS Device Branch:** Receives logs from the Syslog Servers and the Versa Controller (labeled with a green circle 4). It sends logs to the Versa Controller (labeled with a blue circle 1 IPFIX) and the Local log file (labeled with an orange circle 2).
- External Collector:** Receives logs from the Versa Analytics.
- Local log file:** Receives logs from the Versa Analytics and the VOS Device Branch.

The flow is summarized as follows:

- Syslog Servers send logs to the VOS Device Branch (green circle 3) and the Versa Controller (green circle 3).
- The VOS Device Branch sends logs to the Versa Controller (green circle 4) and the Local log file (orange circle 2).
- The Versa Controller sends logs to the Versa Director (green circle 3) and the Versa Analytics (green circle 3).
- The Versa Director sends logs to the Versa Analytics (green circle 1).
- The Versa Analytics sends logs to the External Collector (yellow circle 5) and the Local log file (yellow circle 5).
- The VOS Device Branch sends logs to the Versa Controller (blue circle 1 IPFIX).

ALARM DESTINATIONS	
1	Versa Analytics/Director
2	Local file logging
3	SNMP trap/syslog collector
4	To Versa Director via Netconf
5	Versa Analytics export to external syslog collector

The following table describes the Network Management protocols and ports that VOS device uses to communicate with external entities.

SNMP	Versa VOS device	eth0 (out-of-band)	SNMP trap receiver	UDP/TCP	162	SNMP traps for interfaces, applications, SLA, protocol alarms
SNMP	Versa VOS device	TVI (SD WAN in-band)	SNMP trap receiver	UDP/TCP	162	SNMP traps for interfaces, application, SLA, protocol alarms
IPFIX	Versa VOS device	Any	Analytics cluster	UDP/TCP	Custom	NetFlow data, SLA monitoring and alarms
Syslog	Versa VOS device	eth0 (out-of-band)	Syslog receiver	UDP/TCP	514	Linux and VOS device syslog messages and alarms
NetConf/SSH	Versa VOS device	TVI (SD WAN in-band)	Director monitoring	TCP	2022	All monitoring alarms and monitor command output
AMQP	Versa Director	Any	AMQP bus	TCP	5672	Director-related events, including URL assignment for ZTP
Syslog	Versa Director	Any	Syslog receiver	UDP/TCP	514/ Custom	Linux and Director syslog messages and alarms
Syslog	Versa Analytics	Any	Syslog receiver	UDP/TCP	514/ Custom	VOS device syslog messages and alarms
REST	External	Any northbound	Director	TCP	9182	Used by Director UI

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_VOS_...

Updated: Wed, 23 Oct 2024 08:23:26 GMT

Copyright © 2024, Versa Networks, Inc.

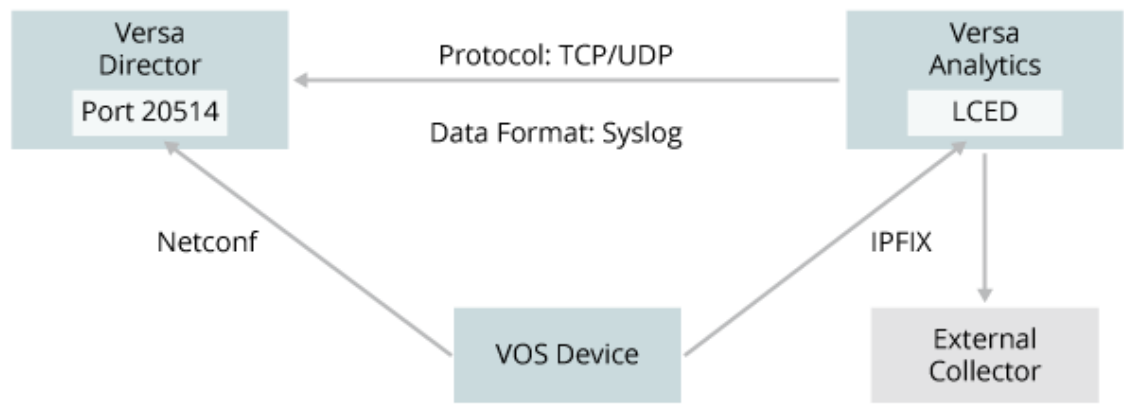
						and external systems to query monitoring
--	--	--	--	--	--	--

Alarm Flow

Alarm flow from a VOS device to a Director node can happen in one of the following ways:

- From a VOS device to Versa Director over Netconf.
- From a VOS device to the Analytics log collector export process (LCED) and then to Versa Director.

The following figure illustrates these alarm flows.



The Director node supports both UDP and TCP channels for alarms flows from LCED. Only one channel, either TCP or UDP, can be active at a time. The Director node supports the syslog data format.

By default, the Director node listens on a TCP channel. To use Netconf or UDP, edit the ALARM_DATA_FORMAT and ALARM_PROTOCOL entries in the vnms.properties file, as shown in the following table.

Channel	vnms.properties Entries
Netconf	ALARM_DATA_FORMAT=netconf
TCP	ALARM_DATA_FORMAT=syslog ALARM_PROTOCOL=tcp
UDP	ALARM_DATA_FORMAT=syslog ALARM_PROTOCOL=udp

Alarm Type Contexts

The following table describes the fields in alarm logs that uniquely identify the alarm context, tenant name, appliance name, alarm type, and alarm key.

Alarm Type	Alarm Context
adc-server-down	Server name
adc-vservice-down	Virtual service name
app-stopped	VSN ID
bgp-nbr-state-change	Instance ID and peer IP
branch-in-maintenance-mode	VSN ID
cgnat-pool-utilization	CGNAT pool name
cpu-utilization	VSN ID; in a typical setup, this value is 0
device-session-utilization	VSN ID
ddos-threshold	Rule name
dhcp-pool-utilization	DHCP service profile name
ha-state-change	VSN ID
ha-sync-status	VSN ID
interface-down	Interface name
interface-half-duplex	Interface name

Alarm Type	Alarm Context
ipsec-ike-down	Peer IP and tunnel ID
ipsec-tunneldown	Peer IP and tunnel ID
mem-utilization	VSN ID
monitor-down	Monitor context name
nexthop-down	IP and and VRF name
org-session-utilization	VSN ID
sdwan-branch-disconnect	Site name
sdwan-datapath-down	Local site name, local WAN link name, remote site name, remote WAN link name, and forwarding class
sdwan-datapath-sla-not-met	Rule name, local site name, local WAN link name, remote site name, remote WAN link name, and forwarding class
snat-pool-utilization	SNAT pool name
software-key-about-to-expire	VSN ID
software-version-change	VSN ID
vrrp-v3-new-backup	VRRP group ID and interface name
vrrp-v3-proto-error	VRRP group ID and interface name

Alarm Type	Alarm Context
vrrp-v3-new-master	VRRP group ID and interface name
VSN ID	VSN ID
zone-protection-flood	Zone profile name

HA Support

The Director node supports HA for Netconf, TCP, and UDP alarm flows. The fault module supports HA for TCP and UDP. For a TCP channel, only the active Director node accepts the connection, and you must configure a log collector group. For a UDP channel, a syslog flow is sent to both Director nodes, but only the active Director node processes the alarms. For a UDP channel, you must configure a remote collector for each Director node.

The data sync between the Director nodes is processed using the POSTGRES replication.

Sample Analytics LCED Configuration

To configure LCED for alarm flows, issue the following CLI commands:

- **set log-collector-exporter local collectors C1 address 192.168.53.2**
- **set log-collector-exporter local collectors C1 port 1234**
- **set log-collector-exporter local collectors C1 storage directory /var/tmp/log**
- **set log-collector-exporter local collectors C1 storage format syslog**
- **set log-collector-exporter local collectors C1 storage file-generation-interval 10**

Configure VOS Device Alarms

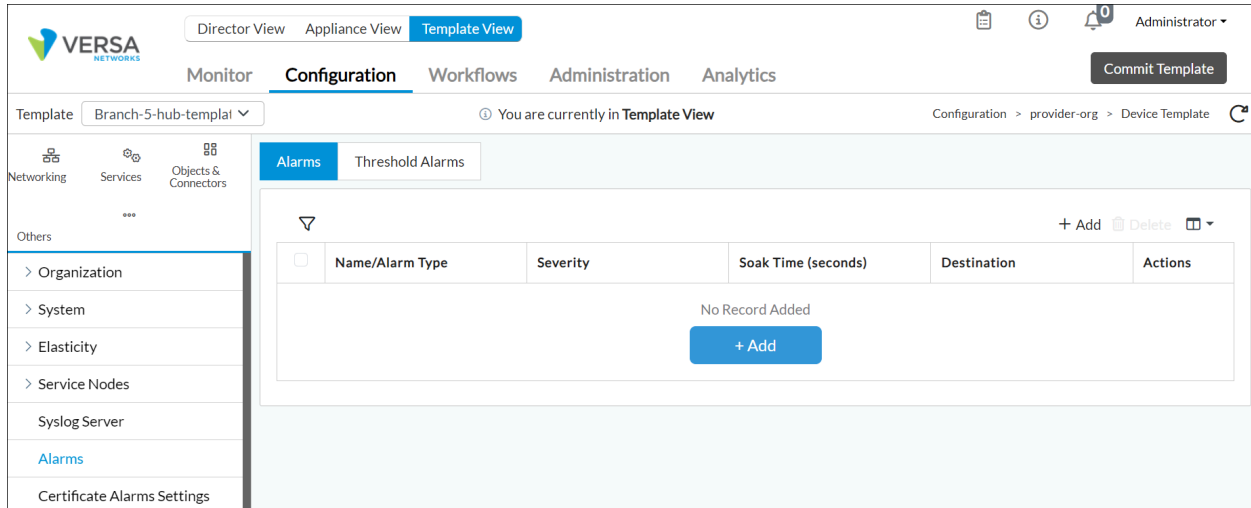
When you configure VOS device alarms, the alarms that the VOS device generates are streamed from the Controller node to the default destination.

Modify General Alarms

To modify the settings for VOS device alarms:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Templates > Templates in the horizontal menu bar.

- c. Select an organization in the left menu bar.
- d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Others > Alarms in the left menu bar.
4. Select the Alarms tab and click the + Add icon. The Add Alarm popup window displays.



5. To configure an alarm's owner and severity, enter information for the following fields

Add Alarm

Alarm Type *

Select Option

Severity

---Please Select---

Soak Time (seconds)

0...65535

Destination *


Select Option

OK

Cancel

Field	Description
Alarm Type (Required)	Select an alarm type from the list in Supported Alarm Types , above.
Severity	Select a severity for the alarm type: <ul style="list-style-type: none"> ◦ Cleared ◦ Indeterminate ◦ Major ◦ Minor ◦ Warning
Soak Time	Enter how long the VOS device waits to determine whether a condition is transient or whether the condition is persistent and an alarm needs to be raised. The soak time is a method for damping

Field	Description
	repetitive alarms. <i>Range:</i> 0 through 65535 seconds <i>Default:</i> 10 seconds; 0 seconds (for bgp-nbr-state-change alarm)
Destination (Required)	Select a destination for the alarm. Click the Add icon to add a destination to the list. You can configure multiple destinations.

6. Select the Threshold Alarms tab and click the  Add icon. The Add Threshold Alarm popup window displays.
7. To configure alarm threshold values, enter information for the following fields.

Add Threshold Alarm

×

Alarm Type *

Select Option

▼

Low Severity

---Please Select---

▼

High Severity

---Please Select---

▼

Low Threshold (%)

0...100

High Threshold (%)

0...100

Soak Time (seconds)

0...65535

▲▼

Destination *

Select Option

▼

OK

Cancel

Field	Description
Alarm Type (Required)	Select a utilization or threshold alarm type: <ul style="list-style-type: none"> ◦ CGNAT pool utilization (cgnat-pool-utilization) ◦ CPU utilization (cpu-utilization) ◦ DDoS threshold (ddos-threshold) ◦ Device session utilization (device-session-utilization) ◦ DHCP IP declined (dhcp-ip-declined) ◦ DHCP pool utilization (dhcp-pool-utilization) ◦ Disk utilization (disk-utilization)

Field	Description
	<ul style="list-style-type: none"> ◦ Downlink bandwidth threshold (dnlink-bw-threshold) ◦ LEF collector queue utilization (lef-collector-queue-utilization) ◦ Log disk utilization ◦ Memory utilization (memory-utilization) ◦ Port scan flood (port-scan-flood) ◦ SNAT pool utilization (snat-pool-utilization) ◦ Tenant session utilization (org-session-utilization) ◦ Uplink bandwidth threshold (uplink-bw-threshold) ◦ Zone protection flood (zone-protection-flood)
Low Severity	<p>Select a severity to assign to the the low end of the alarm threshold:</p> <ul style="list-style-type: none"> ◦ Cleared ◦ Critical ◦ Indeterminate ◦ Major ◦ Minor ◦ Warning
High Severity	<p>Select a severity to assign to the high end of the alarm threshold:</p> <ul style="list-style-type: none"> ◦ Cleared ◦ Critical ◦ Indeterminate ◦ Major ◦ Minor ◦ Warning
Low Threshold	<p>Enter a percentage value for the low threshold.</p> <p><i>Range:</i> 0 through 100 percent</p> <p><i>Default:</i> 75 percent</p>
High Threshold	<p>Enter a percentage value for the high threshold.</p>

Field	Description
	<p><i>Range:</i> 0 through 100 percent</p> <p><i>Default:</i> 95 percent</p>
Soak Time	<p>Enter how long the VOS device waits to determine whether a condition is transient or whether the condition is persistent and an alarm needs to be raised. The soak time is a method for damping repetitive alarms.</p> <p><i>Range:</i> 0 through 65535 seconds</p> <p><i>Default:</i> 10 seconds; 0 seconds (for bgp-nbr-state-change alarm)</p>
Destination (Required)	<p>Select a destination for the alarm. Click the Add icon to add a destination to the list. You can configure multiple destinations.</p>

8. Click OK.

Note that when you change the low-threshold or high-threshold settings for the CPU utilization, but the CPU load itself does not change, no alarm is generated if a violation of the new threshold value occurs. However, as soon as the CPU load changes, an alarm is generated if the load value violates the new threshold value. This same behavior applies when you change the memory and session utilization on a VOS device.

Enable BGP Alarms

To enable BGP alarms on a virtual router:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Templates > Templates in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a post-staging template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Routers in the left menu bar.
4. Select a routing instance in the main pane. The Edit Provider-Control-VR popup window displays.
5. Select BGP and click the instance ID. The Edit BGP Instance popup window displays.

Edit BGP Instance

×

General

Prefix List

SLA Profile

Peer/Group Policy

Peer Group

Route Aggregation

Damping Policy

Versa Private TLV

Advanced

Description

Instance ID

3000

Disable

--Select--

Router ID

169.254.0.1

Local AS

64513

Peer AS

1 to 4294967295 Or <0..65535>.<0..6

Local Address

IP Address Or Interface

Hold Time (seconds)

Allowed Range is 3 - 65535

TTL

Allowed Range is 1 - 255

Password

Local Network Name

--Select--

IBGP Preference

Allowed Range is 1 - 255

EBGP Preference

Allowed Range is 1 - 255

Local AS Mode

--Select--

AS Origination Interval

Allowed Range is 1 - 65535

SLA Community

☐ Suppress Peer AS
☐ Relax First AS Check
☐ Community 4 byte

☐ Passive
☐ Remove All Private AS#
☐ Route Reflector Client
☒ Enable Alarms

☐ Site Of Origin
☐ Soft Reconfiguration
☐ Next Hop UnChanged

Prefix Limit

Maximum

Threshold

Restart Interval

Action

Allowed Range is 1 - 2147483647

Allowed Range is 1 - 100

Allowed Range is 30 - 86400

--Select--

Family

Debug

Family	Loop Count	Prefix Limit		Restart Interval	Action	Soft Reconfiguration	Next Ho
		Maximum	Threshold				
--Select--	Allowed Range is 1 - 2	Allowed Range is 1 - 2	Allowed Range is 1 - 1	Allowed Range is 30 -	--Select--	<input type="checkbox"/> Soft Reconfiguration	<input type="checkbox"/> Next

No Records to Display

OK

Cancel

- Click Enable Alarms to enable the alarms for the instance.
- Click OK.
- Repeat Steps 5 through 7 to enable alarms for other BGP routing instances.

Enable Monitor Alarms

VOS devices monitor the reachability of IP addresses by sending ICMP probe packets, and they update static routes based on the reachability. These probe packet states generate monitor alarms.


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

- In Director view:

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_VOS_...

Updated: Wed, 23 Oct 2024 08:23:26 GMT

Copyright © 2024, Versa Networks, Inc.

- a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a Controller in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
 3. Select Networking > IP-SLA > Monitor in the left menu bar.
 4. In the main pane, click the  Add icon. In the Add IP-SLA Monitors popup window, enter information for the following fields.

Add IP-SLA Monitor

Name *

☒ Interval

☐ Interval (msec)

3

3000

Threshold

Monitor Type *

Domain Name *

Destination Port *

5

DNS

53

Forwarding Class

Nexthop

Monitor Subtype

--Select--

Nexthop

No Subtype

Source Interface

Routing Instance

Networks

--Select--

--Select--

--Select--

☒ IP Address

☐ FQDN

IP Address *

+

IP Address Not Configured

FQDN List


+


FQDN List Not Configured


OK

Cancel

Field	Description
Name (Required)	Enter a name for the IP SLA monitor object.
Interval	<p>Click, and enter the frequency, in seconds, at which to send ICMP packets to the IP address.</p> <p><i>Range:</i> 1 through 60 seconds</p> <p><i>Default:</i> 3 seconds</p>
Interval Milliseconds	<p>Click, and enter the frequency, in milliseconds, at which to send ICMP packets to the IP address.</p> <p><i>Range:</i> 100 through 60000 milliseconds</p> <p><i>Default:</i> 3000 milliseconds</p>
Threshold	<p>Enter the maximum number of ICMP packets to send to the IP address. If the IP address does not respond after this number of packets, the monitor object, and hence the IP address, is marked as down.</p> <p><i>Range:</i> 1 through 60</p> <p><i>Default:</i> 5</p>
Monitor Type (Required)	<p>Select the type of packets to send to the IP address:</p> <ul style="list-style-type: none"> ◦ DNS ◦ (For Releases 22.1.1 and later.) HTTP ◦ (For Releases 22.1.1 and later.) HTTP Raw ◦ ICMP ◦ TCP
Domain Name (Required)	For DNS monitors and if you configure an FQDN, enter the domain name for the IP SLA monitor.
Destination Port (Required)	For DNS, HTTP, raw HTTP, and TCP monitor types, enter the destination port for the IP SLA monitor.
HTTP Response Code	(For Releases 22.1.1 and later.) For HTTP and raw HTTP monitors, enter a numeric range of status codes

	to indicate that an HTTP request has been received from the remote endpoint.
◦ HTTP Response Code Low (Required)	Enter the lowest value of the status code.
◦ HTTP Response Code High (Required)	Enter the highest value of the status code range.
HTTP Raw Request (Required)	(For Releases 22.1.1 and later.) For HTTP raw monitors, enter the HTTP request string to send generic HTTP requests to the remote endpoint. For example, if you issue the HTTP request GET/get HTTP/1.1\r\n, the monitor sends a GET request to retrieve information from the remote endpoint.
Monitor Subtype	<p>Select the monitor subtype:</p> <ul style="list-style-type: none"> ◦ HA probe type—Select to avoid interchassis HA split brain. For more information, see Configure Interchassis HA. ◦ Layer 2 loopback type—Select to monitor an external service node configured as a Layer 2 loopback (virtual wire). ◦ No subtype—Do not use a monitor subtype. This is the default. <p><i>Default:</i> No subtype</p>
Source Interface (Required)	Select the source interface on which to send the probe packets. This interface determines the routing instance through which to send the probe packets. This routing instance is the target routing instance for the probe packets.
Routing Instance	Select the routing instance for the monitor object to use to reach the target IP addresses and FQDNs.
Networks	
IP Address	Click to configure one or more IP addresses to monitor. You must configure either IP addresses or FQDNs.
◦ IP Address (Required)	Click the  Add icon, and then select the IP address to monitor. If you select more than one IP address, all the IP addresses must be reachable for the IP monitor to be applied (this is an AND condition).
FQDN	(For Releases 22.1.1 and later.) Click to configure one

	or more FQDNs to monitor. You must configure either IP addresses or FQDNs.
◦ FQDN List (Required)	Click the  Add icon, and then enter the FQDN to monitor. If you select more than one FQDN, all the FQDNs must be reachable for the IP monitor to be applied (that is; it is an AND condition). When you configure FQDNs, you must also configure the system DNS server to use for the name resolution.
Forwarding Class	(For Releases 21.1.1 and later.) Select a forwarding class for the IP SLA monitor to override the default forwarding class.
Next Hop	Select the device to use as the next hop.

5. Click OK.
6. Repeats Steps 4 and 5 to configure addition IP-SLA monitor profiles.
7. Select Virtual Routers in the left menu bar.
8. Select a device in the main pane.
9. In the Edit Virtual Router popup window, select the Static Routing tab.
10. Click an existing route, or click the  Add icon to add a new static route. The Edit IPv4/v6 Unicast/Add IPv4/v6 Unicast popup window displays.

Director View

Appliance View

Template View

Monitor

Configuration

Workflows

Administration

Analytics

Commit Template

Organization

provider-org

You are currently in Director View

Summary

Devices

Cloud Workload

Asset Summary

VIEW DETAILS

CATEGORY	UP	DOWN	TOTAL
SDWAN Branches	5	0	5
SDWAN Controllers	2	0	2
Hub Controllers	0	0	0
Router Firewalls	0	0	0
SDWAN Hubs	0	0	0
uCPEs	0	0	0
Sub Organizations	-	-	13
Directors ^①	-	-	1
Analytics Cluster ^①	-	-	1

Recent Events

VIEW DETAILS

CRITICAL

0

MAJOR

2

MINOR

0

INDETERMINATE

0

WARNING

0

☐ Refresh every 5 minutes

Provider Health

CATEGORY	UP	DOWN	DISABLED
Config Sync Status	7	0	0
Reachability Status	7	0	0
Service Status	7	0	0
Interfaces	67	0	0
BGP Adjacencies	246	0	0
IKE Status	202	-	0
Paths	2K	20	0

System Summary

Hardware Information	1
Software Version	1
Hardware Model	1
Security Packages	1
OS Security Packages	1
App ID Protocol Bundle Version	1

Services

SDWAN	74
NGFW	4
TDF	1
CGNAT	12
ADC	5
SFW	2

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

Asset Summary

VIEW DETAILS

CATEGORY	UP	DOWN	TOTAL
SDWAN Branches	5	0	5
SDWAN Controllers	2	0	2
Hub Controllers	0	0	0
Router Firewalls	0	0	0
SDWAN Hubs	0	0	0
uCPEs	0	0	0
Sub Organizations	-	-	13
Directors ^①	-	-	1
Analytics Cluster ^①	-	-	1

Recent Events

VIEW DETAILS

CRITICAL

0

MAJOR

2

MINOR

0

INDETERMINATE

0

WARNING

0

☐ Refresh every 5 minutes

Provider Health

CATEGORY	UP	DOWN	DISABLED
Config Sync Status	7	0	0
Reachability Status	7	0	0
Service Status	7	0	0
Interfaces	67	0	0
BGP Adjacencies	246	0	0
IKE Status	202	-	0
Paths	2K	20	0

3. The event-related details are displayed.

Director View

Appliance View

Template View

Monitor

Configuration

Workflows

Administration

Analytics

Commit Template

Organization

provider-org

You are currently in Director View

Export All Records

Export

Recent Events

Search

Back

Clear Selected Alarm

Export

Handle/Assign

Alarms Filter

Device Name	Organization Name	Alarm Type	Handling State	Severity	Status Change Time	Alarm Text
<input type="checkbox"/> SDWAN-Controller1	provider-org	config-change		Major	Wed, Jan 03 2024, 11:21:53	Configuration changed : username (admin), context (...)
<input type="checkbox"/> SDWAN-Branch1	provider-org	config-change		Major	Tue, Dec 19 2023, 14:29:32	Configuration changed : username (admin), context (...)

Rows per page

25

Showing 1 - 2 of 2

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Releases 22.1.1 adds additional alarm types.
- Releases 22.1.3 adds additional alarms types.

Additional Information

[Configure Notifications for Alarms](#)

[Configure Webhook Notifications for Alarms](#)

[Configure Log Collectors and Log Exporter Rules](#)

[Configure Log Export Functionality](#)

[High Availability Alarms](#)

[Interface Alarms](#)

[Routing Alarms](#)

[SD-WAN Alarms](#)

[Service Alarms](#)

[Session Alarms](#)

[Software Alarms](#)

[System Alarms](#)

[Use the Versa Director Monitor Dashboard](#)