Service Alarms

For supported software information, click here.

The following Versa Operating System^{TM} (VOS^{TM}) services generate alarms:

- ADC
- CGNAT
- DHCP
- IPsec
- Security

ADC Alarms

adc-server-down

Description	Backend server connected to a virtual service went down. VOS devices periodically monitor backend server attached to a virtual service (VIP) and declares them as down if monitoring fails. Down servers do not take part in load balancing.
Cause	• Default ICMP monitor failure • Custom monitor (TCP, UDP) failure
Action	• Check the connectivity between the VOS device and backend servers • Check the server (application VM) and ensure it's up and running

Related Commands

- Run the **show orgs org-services Versa adc server summary** CLI command to view the ADC summary.

```
admin@Scale-Controller-1-cli> show orgs org-services Versa adc server summary
```

```
                                          ADMIN    OPER
NAME               TYPE  ADDRESS    PORT  ROUTING INSTANCE  STATE    STATE
------------------------------------------------------------------------------
Cluster1-Analytics1  any   10.202.1.4  1234  Versa-Control-VR  enabled  DOWN
Cluster1-Analytics2  any   10.202.1.5  1234  Versa-Control-VR  enabled  DOWN
```

- Run the **show orgs org-services Versa adc server detail** CLI command to view the ADC server details.

```
admin@Scale-Controller-1-cli> show orgs org-services Versa adc server detail
Server         : Cluster1-Analytics1
  Address      : 10.202.1.4
  Port         : 1234
  Type         : any
  Routing inst : Versa-Control-VR
  Admin state  : enabled
  Oper  state  : DOWN
                        ALIAS      ALIAS
  MONITOR          TYPE      ADDRESS     PORT  HEALTH
  ----------------------------------------------------------------------------
  icmp-default     icmp      n/a         n/a    DOWN
  ----------------------------------------------------------------------------
Server         : Cluster1-Analytics2
  Address      : 10.202.1.5
  Port         : 1234
  Type         : any
  Routing inst : Versa-Control-VR
  Admin state  : enabled
  Oper  state  : DOWN
                      ALIAS     ALIAS
  MONITOR        TYPE      ADDRESS    PORT  HEALTH
  ----------------------------------------------------------------------------
  icmp-default  icmp      n/a        n/a   DOWN
  ----------------------------------------------------------------------------
```

adc-vservice-down

Description	ADC virtual service (VIP) went down.
Cause	• All the servers attached to the virtual service went down, including servers in both default and backup pool.
Action	Check the reason for monitoring failure of all servers causing virtual service to go down.

Related Commands

- Run the **show orgs org-services Versa adc virtual-service summary** CLI command to view the ADC virtual service summary details.

```
admin@Scale-Controller-1-cli> show orgs org-services Versa adc virtual-service summary

VSERVICE                                  ADMIN  OPER
NAME      TYPE  ADDRESS     PORT  ROUTING INSTANCE  STATE  STATE
-------------------------------------------------------------------
VAN-VIP   any   10.200.1.10  1234  Versa-Control-VR  enabled  DOWN
```

- Run the **show orgs org-services Versa adc virtual-service detail** CLI command to view the adc virtual service details.

```
admin@Scale-Controller-1-cli> show orgs org-services Versa adc virtual-service detail

Virtual Service  : VAN-VIP
  Type          : any
  Address       : 10.200.1.10
  Port          : 1234
  Routing inst  : Versa-Control-VR
  Admin state   : enabled
  Oper state    : DOWN

  SERVER             TYPE  ADDRESS     PORT  STATE
  ---------------------------------------------------
  Cluster1-Analytics1 any   10.202.1.4  1234  DOWN
  Cluster1-Analytics2 any   10.202.1.5  1234  DOWN
  Cluster1-Search1    any   10.202.1.2  1234  DOWN
  Cluster1-Search2    any   10.202.1.3  1234  DOWN
```

CGNAT Alarms

cgnat-pool-utilization

Description	Bindings allocated from the CGNAT pool crossed a lower or higher threshold value. The default lower threshold is set to 75% and high threshold is set to 95% of the total bindings.
Cause	• Bug in the software and if the bindings are leaked. • Number of NAT flows is actually closer to 0.2 to 0.4M sessions.
Action	Check whether you can increase the number of public IP addressess used for NAT

Related Commands

- Run the **show orgs org** *customer-name* **sessions summary** CLI command to view the customer's session summary.

```
admin@Site1Branch1-cli> show orgs org Customer1 sessions summary

                 NAT      NAT                          SESSION
VSN  SESSION  SESSION  SESSION  SESSION  SESSION  SESSION  SESSION  COUNT
ID   COUNT    CREATED  CLOSED   COUNT    CREATED  CLOSED   FAILED   MAX
-----------------------------------------------------------------------
0    39       362768   362729   39       342598   342559   240987   1000000
```

- Run the **show orgs org-services** *customer-name* **cgnat pools** CLI command to view the customers CGNAT pool statistics.

```
admin@Site1Branch1-cli> show orgs org-services Customer1 cgnat pools

cgnat pools DIA-Pool-ISPA-Network
 statistics
  tcp-bindings-allocd 210988
  tcp-bindings-freed  210928
  tcp-alloc-failures  0
  tcp-free-failures   0
  udp-bindings-allocd 132322
  udp-bindings-freed  132303
  udp-alloc-failures  0
  udp-free-failures   0
  any-bindings-allocd 0
  any-bindings-freed  0
  any-alloc-failures  0
  any-free-failures   0
  pool-usage          0.0175
```

DHCP Alarms

dhcp-pool-utilization

Description	DHCP pool utilization crossed the configured low threshold. If the utilization increasee and crossed the high threshold value, the alarm changes to pool near exhaustion. After the utilization falls below the low threshold, the alarm changes to pool utilization normal.
Cause	• Pool utilization crossed low threshold. • Pool utilization crossed high threshold.

	- Pool utilization reached below low threshold.
Action	- Run the **show orgs org-services** *customer-name* **dhcp active-leases** CLI command to check the number of IP addresses issued. - Expand the pool range or add a new pool.

Related Commands

- Run the **show orgs org-services** *customer-name* **dhcp active-leases** CLI command to view the providers active lease details.

```
admin@Site1Branch1-cli> show orgs org-services Customer2 dhcp active-leases
dhcp active-leases 6
 ip-address      172.18.102.50
 hw-address      52:54:a1:db:0a:f4
 client-id       <none>
 valid-lifetime  86400
 expires         "2017/10/19 21:57:53"
 subnet-id       2
 interface       vni-0/4.102
 dynamic-pool    1
 service-profile 1
 fqdn-forward    0
 fqdn-reverse    0
 hostname        <none>
 discover        0
 from-server     1
 from-hint       0
 from-pool       0
 trans-id        2414643512
```

IPsec Alarms

ipsec-ike-down

Description	IPsec IKE went down. When the control plane goes down, the IPsec tunnel goes down. This affects all data traffic passing through the IPsec tunnels created as part of this IKE.
Cause	- IKE peer is not reachable.

	• Authentication with the peer failed. • Encryption parameters of the peer changed.
Action	Execute commands to check the following: • Whether SA was deleted • History • Ping reachability between the IKE endpoints

Related Commands

- Run the **show orgs org-services Provider ipsec vpn-profile branch ike security-associations brief** CLI command to display the current status of the IKE SAs.

```
admin@14-vm5-cli> show orgs org-services Provider ipsec vpn-profile branch ike security-associations
brief

Flags:
 P - PSK  C - Certificate  N - NAT-T   R - Responder  I - Initiator
Tunnel Ver  Local       Remote      VPN        Local              Remote            Flags
ID         Gateway      Gateway     Type       SPI                SPI
------ ---  ------------ -----------  ----------  -----------------   ------------------  -----------
5      v2   31.31.31.5   31.31.31.1   SDWAN-B-PS  0xea9b00eb0db20002  0xf30cdd50b0260002  P,I
```

- Run the **show orgs org-services Provider ipsec vpn-profile branch ike history** CLI command to display the history of different events related to this SA.

```
admin@14-vm5-cli> show orgs org-services Provider ipsec vpn-profile branch ike history

Local Gateway: 31.31.31.5      Remote Gateway: 31.31.31.1
 Last Known State     : Active
 Last State Timestamp : 2017-08-31T20:10:46.481047-08:00
 Event History:
  0. Event     : IKE Done
  Timestamp    : 2017-08-31T20:10:46.481049-08:00
  Role         : initiator
  Inbound SPI  : 0xea9b00eb0db20002
  Outbound SPI : 0xf30cdd50b0260002
  1. Event     : IKE Failed
  Timestamp    : 2017-08-31T20:10:41.310722-08:00
  Role         : initiator
  Inbound SPI  : 0x63a438d92b670002
  Outbound SPI : None
  Error        : Timed out
  2. Event     : IKE Rekey
  Timestamp    : 2017-08-31T20:08:07.621681-08:00
  Role         : responder
```

ipsec-tunnel-down

Description	IPsec tunnel went down. When an IPsec tunnel goes down, data traffic is affected, because the security associations (SAs) to encrypt outgoing data or decrypt incoming data is not available.
Action	Execute commands to check the following: • Current status • Reason for deletion of SA • IKE control path

Related Commands

- Run the **show orgs org-services Provider ipsec vpn-profile branch security-associations brief** CLI command to check the current status of the IPsec SAs.

```
admin@14-vm5-cli> show orgs org-services Provider ipsec vpn-profile branch security-associations brief

Remote Gateway   Transform  Inbound SPI  Bytes/sec  Outbound SPI  Bytes/sec  Up Time   Next Rekey Time
---------------  ---------  -----------  ---------  ------------  ---------  --------  ---------------
31.31.31.1       aes-cbc    0x20037bf    0          0x20052b6     0          1d00h53m  00:01:59
```

- Run the **show orgs org-services Provider ipsec vpn-profile branch ipsec history** CLI command to check the SA event history.

```
admin@14-vm5-cli> show orgs org-services Provider ipsec vpn-profile branch ipsec history

Local Gateway: 31.31.31.5      Remote Gateway: 31.31.31.1
 Last Known State     : Active
 Last State Timestamp : 2017-08-31T20:10:46.481489-08:00
 Event History:
  0. Event     : IPsec Done
  Timestamp    : 2017-08-31T20:10:46.48149-08:00
  Inbound SPI  : 0x2005272
  Outbound SPI : 0x2006e19
  1. Event     : IPsec Rekey
  Timestamp    : 2017-08-31T20:08:42.491321-08:00
  Inbound SPI  : 0x2002a3e
  Outbound SPI : 0x20079bd
```

Security Alarms

Zone-based protection profiles protect VOS devices against DoS attacks. These profiles apply an extensive denial-of-service (DoS) template to untrusted zones in the firewall to protect the network from high-volume DoS attacks and to provide the first security barrier against DoS attacks.

Zone-based protection policies prevent attacks such as floods, sweeps, and malformed IP packets. These policies raise alarms when threshols are exceeded to alert the administrator about DoS attacks.

Zone-based protection calculates the thresholds to account for the access interface speed (for example, 1 Gbps and 10 Gbps). Zone protection protects against a flood of traffic. Generally the attacker uses random source or destination IP addresses or port numbers for such attacks. zone Protection is applied only for the first packet of a new session, thus allowing 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 a DoS attack exceeds the previously configured threshold, alarms are raised. The following alarms are raised depending on the attack type:

- DDoS threshold—A DoS protection profile configured by the administrator for flood detection with an alarm threshold has been crossed.
- Flood threshold—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.

ddos-threshold

Description	This alarm is raised when a DoS protection profile configured for flood detection with an alarm threshold is exceeded.
Cause	The VOS instance receives the flood traffic (new sessions) at a rate greater 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 profiles is that a zone protection profile is evaluated before the creation of a flow, and a DoS protection profile is evaluated after the creation of the flow.
Action	Review the DoS profile configuration, adjust the alarm, and activate thresholds.

port-scan-flood alarm: port-scan-flood

Description	A zone protection profile configured with scan parameters detected sufficient traffic activity and exceeded the configured alarm rate.
Cause	The VOS instance receives the flood traffic (new sessions) at a rate greater 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 configuration, adjust the alarm, and activate thresholds.

zone-protection-flood

Description	A zone protection profile configured with flood parameters detected sufficient traffic activity and exceeded the configured alarm rate.
Cause	The VOS instance receives flood traffic (new sessions) at a rate greater 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 configuration, adjust the alarm, and activate thresholds.

Related Commands

- Run the **show orgs org-services** *tenant-name* **security profiles zone-protection zone-protection-statistics** CLI command to view zone protection statistics.
- Run the **show orgs org-services** *tenant-name* **security dos-policies rules** CLI command to view DoS Protection statistics.

SLA Violation Alarms

nexthop-sla-not-met

Description	This alarm is generated on a node using SD-WAN policies for traffic steering over one or more configured next hops when the node is determining the SLA compliance of these next hops. This alarm does not associate with site-to-site path selection.
Cause	Packet loss or high latency experienced by the application monitors configured locally or towards a remote branch.
Action	Not applicable.

Related Commands

- Run the following command to check the metrics for each next hop associated with the SD-WAN rule. For a next hop associated with a local application monitor, the metrics directly come from the application monitor. For a next hop associated with a remote application monitor, the metrics are a combination of those imported from the remote monitor and the site-to-site SLA metrics towards the remote appliance on which the monitor is running.

```
admin@sk-br1-cli(config)% run show orgs org-services Customer1 sd-wan policies default_policy
rules nexthop application-monitor detail
                                          APPLICATION  APPLICATION  APPLICATION  APPLICATION
        NEXTHOP   NEXTHOP  NEXTHOP  NEXTHOP  HIT    MONITOR     MONITOR     MONITOR
MONITOR     APPLICATION
NAME      PRIORITY  NAME     STATUS   ACTIVE   COUNT  NAME       TYPE       LATENCY
LOSS       MONITOR VLS
------------------------------------------------------------------------------------------------------------------
r1       1       p1      up      yes     9     appmon_1    icmp       2.26       0.0        3421
         2       p2      up      no      0     appmon_1    icmp       2.09       0.0        3414
         3       p3      up      no      0     appmon_1    icmp       2.07       0.0        3413
o365_rule  1       p1      up      yes     0     -         -         -         -         -
wan-r1
wan-r2
```

- If one of the configured next hops is an SD-WAN next hop, the metrics associated with the next hop are a combination of site-to-site SLA metrics. Run the following commands to check the SLA towards a remote branch.

```
admin@sk-br1-cli(config)% run show orgs org Customer1 sd-wan sla-monitor metrics last
                                  LOCAL  REMOTE
                      LOCAL  REMOTE  WAN    WAN    TWO    FWD    REV    PDU    FWD
REV
          PATH    FWD    WAN    WAN    LINK   LINK   WAY    DELAY  DELAY  LOSS   LOSS   LOSS
FWD   REV   PDU   PDU
SITE NAME    HANDLE   CLASS  LINK   LINK   ID     ID     DELAY  VAR    VAR    RATIO  RATIO  RATIO
LOSS  LOSS  SENT  RCVD
-----------------------------------------------------------------------------------------------------------------------
Branch2     6689028  fc_ef  b1-w1  b2-w1   1     1      0     1     2     0.0    0.0    0.0    0     0     1     1
          6693380  fc_ef  b1-w2  b2-w2   2     2      1     1     1     0.0    0.0    0.0    0     0     1     1
controller1  1052932  fc_ef  b1-w1  c1-w1   1     1      1     0     1     0.0    0.0    0.0    0     0     1     1
          1057284  fc_ef  b1-w2  c1-w2   2     2      1     1     0     0.0    0.0    0.0    0     0     1     1
```

```
admin@sk-br1-cli(config)% run show orgs org-services Customer1 sd-wan path path-metrics Branch2
                    TWO    FWD    REV
REMOTE   LOCAL    REMOTE   WAY    DELAY  DELAY  FWD LOSS    REV LOSS    PDU
LOSS                    VOICE  AUDIO  VIDEO
BRANCH   CIRCUIT  CIRCUIT  DELAY  VAR    VAR    PERCENTAGE  PERCENTAGE  PERCENTAGE
RX BYTES    TX BYTES    MOS    MOS    MOS
-------------------------------------------------------------------------------------------------------------------------
Branch2  b1-w1    b2-w1    0      0      0      0.00        0.00        0.00        75550598   75578696   0.00   0.00
0.00
       b1-w2    b2-w2    1      0      0      0.00        0.00        0.00        132704992  132704510  0.00   0.00   0.
00
```

```
admin@sk-br1-cli(config)% run show application-monitor remote brief

APPLICATION
MONITOR      ORGANIZATION  REMOTE        LOSS       LATENCY
```

```
NAME        NAME         SITE     TYPE  PERCENTAGE  MILLISEC
--------------------------------------------------------------
appmon_1    Customer1    Branch2  icmp  0.0         2.07
```

- Run the **show application-monitor local detail** command to check the application monitor locally.

```
admin@sk-br1-cli(config)% run show application-monitor local detail

APPLICATION
MONITOR     ROUTING          LOSS        LATENCY   LOCAL          EXPORT
NAME        INSTANCE   TYPE  PERCENTAGE  MILLISEC  ORGANIZATION   ORGANIZATION
------------------------------------------------------------------------------
appmon_1    wan-vrf-1  icmp  0.0         2.16      Customer1
            wan-vrf-2  icmp  0.0         2.2       Customer1
```

Supported Software Information

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

- Releases 21.2.1 and later support SLA violation alarm.

Additional Information

Configure VOS Device Alarms