High Availability Alarms

For supported software information, click here.

With high availability (HA), Versa Operating System™ (VOS™) devices have two types of roles, active and standby. The VOS device role is determined by configuration parameters. VOS devices generate HA alarms when the HA role type changes.

The VOS software active-standby HA design allows you to configure redundant services between two VOS devices. Configuring redundant services can maximize service uptime, protect against hardware and software failures, and protect against local network connectivity issues, such as link and physical failures on switches and routers.

You can enable stateful protocols such as BFD and LACP on VOS device interfaces to improve resiliency and to detect protocol-level failures in connected devices. Using such stateful protocols helps to expedite recovery actions when they detect a failure.

The switchover trigger policy that you configure determines the HA triggerType. The triggers are based on the interfaces and routing peers that the policy tracks. When the low values for interface count, routing peer count, and VRRP group count in the policy rule match condition are met, the VOS device takes the action defined in the trigger policy. If the action is specified as switchover, and if the standby VOS device has a greater number of tracked routing peers, active interfaces, and active VRRP groups, the system switches over, changing the role of the standby node to be the active node.

The triggerType alarm indicates the reason for the failover. A switchover can occur when the standby VOS device has more available interfaces, such as when an LACP down or interface down event occurs. A switchover can also occur because of IP connectivity failures between the active and standby VOS devices, which can be caused by such events as control or data plane process failure on the active VOS device and a BFD failure over the control plane connection. A switchover trigger can be manual, for example, if you issue the **request redundancy interchassis appliance-master-switch** CLI command.

quorum-evaluate and quorum-result

Description	If the standby VOS device can no longer communicate with its peer active VOS device, it begins a quorum evaluation process to assess the presence of the active

	peer, and it triggers the quorum-evaluate alarm. This alarm specifies the reason why the quorum evaluation process started. The quorum-result alarm specifies the outcome of the evaluation.
Cause	• Failure of the BFD session from the standby toward the active VOS device. • Control connection failure (TCP) toward the active VOS device. • Active VOS device did not receive any HA monitor probes for the configured number of seconds.
Action	• Verify that both VOS devices are reachable and that all processes are running. • Verify the control and physical links between the two VOS devices, and check whether the BFD session between them is up and running. • View the reason for quorum evaluation in the alarm log to determine the initial cause of the communication failure. • Verify the system uptime for both VOS devices. If the uptime is not as expected, check for crashed processes and for any core dump files. If you find core dump files, contact Versa Networks support (support@versa-networks.com) for further diagnostics.

ha-sync-status and ha-state-change

Description	If the active VOS device fails, the mastership changes, and the standby notifies the administrator with an alarm indicating the role change. The haTriggerType alarm specifies the reason for the HA role type change.
Cause	• Change in state of the active VOS device, the standby VOS device, or control protocols. • Link failure detected by LACP.

	• Loss of physical link, or timeout of BFD session between the active and standby VOS devices.
Action	• Verify that both VOS devices are reachable and that all processes are running. • Verify the control and physical links between the two VOS devices, and check whether the BFD session between them is up and running. • View the HA and BFD events in the alarm log to determine the initial cause of the failover. • Verify the system uptime for both VOS devices. If the uptime is not as expected, check for crashed processes and for any core dump files. If you find core dump files, contact Versa Networks support (support@versa-networks.com) for further diagnostics.

Related Commands

- Issue the **show redundancy inter-chassis control nodes** CLI command to view HA control status.

```
admin@Branch5-Hub-cli> show redundancy inter-chassis control nodes
APPLIANCE  VCN       VCN
INSTANCE   INSTANCE  SLOT   RED ROLE            IP
-------------------------------------------------------------------------------
Local      VCN0      0      *Active (ENABLED)     10.10.115.2
Remote     VCN0      0       Standalone(DOWN)     10.10.116.2
```

- Issue the **show redundancy inter-chassis service nodes** CLI command to view HA service status.

```
admin@Branch5-Hub-cli> show redundancy inter-chassis service nodes
                       RED
APPLIANCE  SNG              GROUP  VSN
INSTANCE   ID   SNG  NAME    ID    ID   VID  RED ROLE
-------------------------------------------------------------------
Local      0    default-sng  1     0    2    Active(IN-SYNC)
Remote     0    default-sng  1     0    18   Standby(UP)
```

- Issue the **show bfd session brief** CLI command to view BFD session status.

```
admin@Branch5-Hub-cli> show bfd session brief
Instance            Address        State  RxPkts     TxPkts
Provider_VR         10.10.116.2    up     63         67
Provider_VR         10.10.110.2    down   0          59
```

- Issue the **show alarms | match BFD** CLI command to view BFD alarms.

```
admin@Branch5-Hub-cli> show alarms | match BFD
```

```
routing bfdNbrStateChange 2017.09.19T10:20:14-0 routing-instance Provider_VR: BFD neighbor 10.10.116.2
changed from Down state to Up state
routing bfdNbrStateChange 2017.09.19T10:25:35-0 routing-instance Provider_VR: BFD neighbor 10.10.116.2
changed from Up state to Down state
routing bfdNbrStateChange 2017.09.19T10:26:55-0 routing-instance Provider_VR: BFD neighbor 10.10.116.2
changed from Down state to Up state
routing bfdNbrStateChange 2017.09.19T10:29:34-0 routing-instance Provider_VR:  BFD neighbor  10.10.116.2
changed from Up state to Down state
routing bfdNbrStateChange 2017.09.19T10:30:25-0 routing-instance Provider_VR: BFD neighbor 10.10.116.2
changed from. Down state to Up state
```

- Issue the **show alarms | match HA** CLI command to view HA alarms.

```
admin@Branch5-Hub-cli> show alarms | match HA
ha  haSyncStatus  2017-09-12T14:58:29-0 (null): HA-Active Intra-Chassis Resource Controller sync status OK
ha haSyncStatus   2017-09-16T17:05:54-0 provider-org: HA-Active Intra-Chassis Resource Controller sync
status OK
ha haStateChnage  2017-09-16T17:05:54-0 provider-org: In Inter-Chassis mode, changing role to HA-Active
during bootup
ha haSyncStatus   2017-09-19T10:13:34-0 (null): HA-Active Intra-Chassis Resource Controller sync status OK
ha haSyncStatus   2017-09-19T10:12:02-0 provider-org: HA-Active Intra-Chassis Resource Controller sync
status OK
ha haStateChange  2017-09-19T10:12:02-0 provider-org: In Inter-Chassis mode, changing role to HA-Active
during bootup
```

- Issue the **show coredumps** CLI command to view core files.

```
admin@vcpe102-cli> show coredumps
total 732K
-rw-rw-r-x  1  root  root 634K Jul  5   18:25  core.versa-vsmd.1536.versa-flexvn..1499304350.gz
-rw-rw-r-x  1  root  root 24K  Aug  30  12:27  core.iperf3.6645.vcpe102.1504121275.gz
-rw-rn-r-x  1  root  root 22K  Aug  30  12:28  core.iperf3.6708.vcpel02.1504121302.gz
-rm-rm-r-x  1  root  root 22K  Aug  30  12:28  core.iperf3.6762.vcpe102.1504121321.gz
-rw-rm-r-x  1  root  root 22K  Aug  30  12:29  core.iperf3.6814.vcpe102.1504121378.gz
```

Summary Statistics of Alarms on VOS Devices

The **show device alarm** CLI command provides a quick view of all the alarms statistics that a device has generated. Analyze these alarms to detect any discrepancies.

Related Commands

- Issue the **show device alarms** CLI command to view device alarm details.

```
admin@vCPE101-cli> show device alarm
                                NUM     NUM       NUM      NUM      NUM     NUM      NUM
ALARM                           NEW     CHANGED   CLEARED  NETCONF  SNMP    SYSLOG   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	bgp-nbr-max-prefix	0	0	0	0	0	0	0
25	bgp-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
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
```

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

Configure VOS Device Alarms
Configure Interchassis HA