Troubleshoot SD-WAN Branches

For supported software information, click here.

This article describes how to troubleshoot issues with SD-WAN Versa Operating System™ (VOS™) branches.

Check Branch Staging and Lifecycle

This section explains the factory default configuration and staging configuration of branch devices,

Required Controller Configuration

The following are the minimum configuration elements on a Controller node for branch staging:

- Configure the service provider's tenant organization in the **system sd-wan site provider-org** *organization-name* command. For the provider organization, configure the routing instance that is used for branch management purposes in the **orgs org** *organization-name* **sd-wan site management-routing-instance** *instance-name* command.
- Mark the management routing instance use by SD-WAN-management with the **routing-instances** *instance-name* **usage-type SD-WAN-management** command.
- The **provider-org system sd-wan site provider-org** *organization-name* command configures the value of the global tenant ID in the **orgs org** *organization-name* **sd-wan site global-tenant-id** *tenant-id command*. The global tenant ID must match that in the factory-default configuration on the branch device.

Note: You should configure MP-BGP in the provider organization for SD-WAN deployments so that notifications for all relevant branch events are delivered to the Versa Director node

Check the IPsec Connection between the Controller and Branch Nodes

After a branch device successfully establishes an IPsec connection to the Controller node, the Controller nodes sends a notification to the Director node. To display the details of this notification, issue the **show alarms** CLI command. For example:

```
admin@SD-WAN-Controller1-cli> show alarms | match branchd | match br101
branchd SD-WAN-branch-connect    2016-03-30T15:01:53   chassis-id LR201510017703, branch-id 64,  branch br101
branchd SD-WAN-branch-connect    2016-03-30T15:06:57   chassis-id LR201510017703, branch-id 65,  branch br101
branchd SD-WAN-branch-connect    2016-03-30T15:09:48   chassis-id LR201510017703, branch-id 101, branch
```

> br101, wan-ip 11.11.12.102, wan-ip 11.11.11.103
> branchd SD-WAN-branch-disconnect 2016-03-30T15:55:06 chassis-id LR201510017703, branch-id 101, branch br101, wan-ip 11.11.11.103

Branch Lifecycle Notifications

Notifications are sent at various stages in the branch lifecycle:

- Branch with site name br101 is connected using the factory-default configuration.

  > branchd SD-WAN-branch-connect 2016-03-30T15:01:53 chassis-id LR201510017703, branch-id 64, branch br101

  If this connection notification does not display, debug either the data path or IPsec connectivity from the branch to the Controller node. See Stage 3 Debugging on Branch, below.

  In response to the branch connection notification, the Director node pushes the staging configuration to the branch device and requests a reboot of the branch device.

- After rebooting with the staging configuration, the branch is connected to the Controller node. The following is the notification indication that a branch has been staged:

  > branchd SD-WAN-branch-connect 2016-03-30T15:06:57 chassis-id LR201510017703, branch-id 65, branch br101

  If this connect notification is not seen, either data path or IPsec connectivity from branch to controller needs to be debugged. See Stage 3 Debugging on Branch, below.

- After rebooting with configuration, the branch is connected to the Controller noce. The following is the notification indicating that a branch has been staged:

  > branchd SD-WAN-branch-connect 2016-03-30T15:09:48 chassis-id LR201510017703, branch-id 101, branch br101, wan-ip 11.11.12.102, wan-ip 11.11.11.103

  If this notification does not display, the branch is not able to connect to the Controller node after staging. See Stage 3 Debugging on Branch below

  A branch operating with a configuration after the completion of staging is referred as a Stage 3 branch. The stage numbering corresponds to steps involved in the staging process.

- Branch is disconnected from the Controller node. This occurs only after the staging completes.

  > branchd SD-WAN-branch-disconnect 2016-03-30T15:55:06 chassis-id LR201510017703, branch-id 101, branch br101, wan-ip 11.11.11.103

Stage 3 Debugging on an SD-WAN VOS Device

The SD-WAN VOS device is designed for multitenancy and for branch site devices. All SD-WAN **show** commands are

at the tenant level. The provider tenant is the starting point for most of the debugging, because the branch lifecycle is managed in the context of the provider tenant.

The debug commands and workflow described in this section apply for all tenants. Several elements of configuration and runtime state are common for SD-WAN Controller, branch and hub devices.

The following CLI commands provide visibility into common state:

- To display information about the WAN interfaces used for SD-WAN uplink connectivity, issue the **show orgs org sd-wan wan-interfaces** CLI command. For example:

```
admin@Controller1-cli> show orgs org My-Org sd-wan wan-interfaces | tab
                                                                         MIN
        CIRCUIT  CIRCUIT  LINK            NAT               PUBLIC  DATAPATH  DATAPATH  LINK
SHAPING  SHAPING
INTF NAME  FAMILY   NAME     ID    ENDPT IP     STATUS   PUBLIC IP     PORT    IP       PORT
ENCRYPTION  RATE     RATE
------------------------------------------------------------------------------------------------------------------------
vni-0/1.0  ipv4    INET     1     192.168.10.5  unknown  192.168.10.5  4790    -        -       optional    0       0
vni-0/2.0  ipv4    MPLS     2     192.168.20.5  unknown  192.168.20.5  4790    -        -       optional    0       0
```

- To display statistics for the WAN interfaces used for SD-WAN uplink connectivity, issue the **show orgs org sd-wan statistics vni** CLI command. For example:

```
admin@Controller1-cli> show orgs org My-Org sd-wan statistics vni
                                              TX    RX
VNI NAME   RX PKTS    RX BYTES     TX PKTS    TX BYTES     BPS   BPS
-------------------------------------------------------------------
vni-0/1.0  202722652  69281435315  354181937  66354451846  2432  2192
vni-0/2.0  0          0            7841215    1442780128   240   0
```

- To clear WAN interface statistics, issue the **request clear statistics sd-wan vni all** CLI command.

Low-Level vty Commands

You can use low-level commands for in-depth debugging from the infmgr shell. To access the infmgr shell, issue the **vsh connect infmgr** CLI command from the Linux shell prompt.

The following are the low-level commands:

- To use the low-level commands, issue the following version of the **show p2mp nbrs detail all** CLI command:

```
infmgr> show p2mp nbrs detail My-Org all
network-id 1, site-id 0x0a00, rtt-index 14, branch-id 10, site-name East-Coast-Controller-1, flags: SELF
 site-type = SD-WAN, chassis-id East-Coast-Controller-1
 tunnel: (local: 10.10.110.2, remote: 10.10.110.2) [[ encap-outer 5, encap-inner 3, nbrtun_cfgidx 0 ]]
 tunnel: (local: 10.10.10.2, remote: 10.10.10.2) [[ encap-outer 5, encap-inner 1, nbrtun_cfgidx 0 ]]
 transport-ips:
(local-ip 192.168.211.2, routing-instance TransportVRF, link-id 1, port 4790, seq 0, ckt-name Braodband1,
tunnels encrypted/plaintext, nat_status:unknown transport-domain-ids [ 2  ]
(local-ip 192.168.212.2, routing-instance TransportVRF, link-id 2, port 4790, seq 0, ckt-name Broadband2,
```

```
tunnels encrypted/plaintext, nat_status:unknown transport-domain-ids [ 2  ]
 dynamic-endpt-info:
(link-id 1, public-ip 0.0.0.0, public-port 4790, seq 0, shaping_rate 0, shaping_rate_min 0
(link-id 2, public-ip 0.0.0.0, public-port 4790, seq 0, shaping_rate 0, shaping_rate_min 0
  mgmt_ip: 10.10.110.2
   cookie: 0x91037d0c
   local_conf: tenant_id 4
 ifname vni-0/0.0: (ifindex 1050, ip 192.168.211.2, link-id 1, circuit-name Braodband1, shaping_rate 0,
shaping_rate_min 0, tunnels:encrypt,plaintext, IKE-link)
 SLA-cfg (fc, sla-interval, sla-log-interval, no-encrypt): (0, 0, 0, 0) (1, 0, 0, 0), (2, 0, 0, 0), (3, 0, 0, 0), (4, 3,
300, 0), (5, 0, 0, 0), (6, 0, 0, 0), (7, 0, 0, 0),
 (8, 0, 0, 0), (9, 0, 0, 0), (10, 0, 0, 0), (11, 0, 0, 0), (12, 0, 0, 0), (13, 0, 0, 0), (14, 0, 0, 0), (15, 0, 0, 0),
 ifname vni-0/1.0: (ifindex 1052, ip 192.168.212.2, link-id 2, circuit-name Broadband2, shaping_rate 0,
shaping_rate_min 0, tunnels:encrypt,plaintext, IKE-link)
 SLA-cfg (fc, sla-interval, sla-log-interval, no-encrypt): (0, 0, 0, 0) (1, 0, 0, 0), (2, 0, 0, 0), (3, 0, 0, 0), (4, 0, 0,
0), (5, 0, 0, 0), (6, 0, 0, 0), (7, 0, 0, 0),
(8, 3, 300, 0), (9, 0, 0, 0), (10, 0, 0, 0), (11, 0, 0, 0), (12, 0, 0, 0), (13, 0, 0, 0), (14, 0, 0, 0), (15, 0, 0, 0),
 ctrlr_info: branch-vnf-mgr 192.168.75.2/24 ]
 [[ source: config; state: , ipc:  ]]
network-id 1, site-id 0x411f, rtt-index 14, branch-id 8001, site-name Branch1-SanFrancisco, flags:
 site-type = SD-WAN, chassis-id 001branch1
 tunnel: (local: 10.10.10.2, remote: 10.10.11.2) [[ encap-outer 5, encap-inner 1, nbrtun_cfgidx 42 ]]
 tunnel: (local: 10.10.110.2, remote: 10.10.111.2) [[ encap-outer 5, encap-inner 3, nbrtun_cfgidx 52 ]]
 transport-ips:
 (local-ip 101.101.101.1, routing-instance TransportVRF, link-id 1, port 12983, seq 1, ckt-name , tunnels /,
nat_status:unknown    transport-domain-ids [ 1  ]
 dynamic-endpt-info:
 (link-id 1, public-ip 101.101.101.1, public-port 12983, seq 1, shaping_rate 0, shaping_rate_min 0
 mgmt_ip: 10.10.111.2
 cookie: 0xc289b9a9
 [[ source: vsmd; state: ike_complete, , ipc: add_tun, remote_obj ]]
```

- To display information about a specific node, issue the following version of the **show p2mp nbrs detail** CLI command:

```
infmgr> show p2mp nbrs detail My-Org Branch1-SanFrancisco
```

Stage 3 Debugging on a Controller Node

An SD-WAN Controller node manages multiple branch and hub sites for one or more customer tenants. The typical debug workflow involves obtaining a high-level view of all the sites for a particular tenant and then drilling down into a specific site.

High-Level Summary Commands

- Display a summary of the number of sites in connected, disconnected, and error state:

```
admin@Controller1-cli> show orgs org My-Org sd-wan summary
Sites in connected state     :  2
Sites in disconnected state  :  1
```

```
Sites in erroneous state     :   1
```

- Display brief information about all SD-WAN sites managed by the Controller node, including the connectivity event history and status of the sites:

```
admin@Controller1-cli> show orgs org My-Org sd-wan brief
            SITE  MANAGEMENT                      CONNECTIVITY  IS
SITE NAME   ID    IP          TYPE    UP TIME       STATUS       CTRLR
-------------------------------------------------------------------------------
BRANCH1      65    10.255.0.129  remote  -             -            no
Branch-01    101   10.255.0.8    remote  3d:2h:29m:41s   Connected    no
Branch-02    102   10.255.0.10   remote  55d:9h:52m:29s  Connected    no
Controller-1  1     10.255.0.0    local   320d:3h:54m:3s  -            yes

Branch History:
   Branch-id          : 65
   Branch-name          : BRANCH1
   current-status       : ERRONEOUS
   Logs               :
    Record :
     Event-message     : Poststaging done
     Time-stamp        : 2024-02-22T12:38:03;

Branch History:
   Branch-id          : 101
   Branch-name          : Branch-01
   current-status       : UP
   Logs               :
    Record :
     Event-message     : IKE completed
     Time-stamp        : 2024-03-28T19:59:30;
    Record :
     Event-message     : IKE completed
     Time-stamp        : 2024-03-28T19:59:38;
```

Branch-Specific Commands

- Display information about a specific SD-WAN site. For example, for the site BRANCH1:

```
admin@Controller1-cli> show orgs org My-Org sd-wan detail BRANCH1
Site Id          -   65
State            -   -
Uptime           -   -
Site Name        -   BRANCH1
Site Type        -   branch
Chassis Id       -   Branch-03
Global Tenant Id   -   1
Management IP      -   10.255.0.129

Secure Tunnel Info
  Local Endpoint  -
  Remote Endpoint -
```

```
Plain Text Tunnel Info
  Local Endpoint  -
  Remote Endpoint -

LINK  LINK    ACCESS   LOCAL         LINK       SHAPING  MIN SHAPING
ID    FAMILY  CIRCUIT  IP            ENCRYPTION  RATE     RATE        TRANSPORT-DOMAINS
-------------------------------------------------------------------------------------------
  1   ipv4    BBAND    192.168.50.13  optional   0        0

NAT Status:

LINK  LINK    ACCESS   NAT      PUBLIC         PUBLIC  DataPath      DataPath
ID    FAMILY  CIRCUIT  STATUS   IP             PORT    IP            PORT
-----------------------------------------------------------------------------
  1   ipv4    BBAND    unknown  192.168.50.13  0       192.168.50.13  0
```

- Display information about connectivity events for a specific SD-WAN site. These events are displayed chronologically, in ascending order, so in the case of connectivity failures, the last event can provide useful information. For example, if the last event is an IKE attempt and the timestamp is more than several seconds ago, it is likely that an IKE attempt from branch is failing. This information provides a clue to for next step in debugging connectivity issue: either check IPsec or data path connectivity. For example, for the site 101:

```
admin@Controller1-cli> show orgs org My-Org sd-wan history 101
Branch History:
   Branch-id          : 101
   Branch-name        : Branch-03
   current-status     : DOWN
   Logs               :
    Record :
     Event-message    : IKE completed
     Time-stamp       : 2024-02-26T09:40:55;
    Record :
     Event-message    : Branch connected
     Time-stamp       : 2024-02-26T09:40:58;
    Record :
     Event-message    : IKE disconnected
     Time-stamp       : 2024-03-12T11:39:48;
    Record :
     Event-message    : IKE attempted
     Time-stamp       : 2024-03-12T11:42:59;
    Record :
     Event-message    : IKE attempted
     Time-stamp       : 2024-03-12T11:43:03;
    Record :
     Event-message    : IKE completed
     Time-stamp       : 2024-03-12T11:43:05;
    Record :
     Event-message    : IKE completed
     Time-stamp       : 2024-03-12T11:43:09;
    Record :
     Event-message    : IKE disconnected
     Time-stamp       : 2024-03-13T16:27:29;
```

- Display detailed information about connectivity events for a specific SD-WAN site.

```
admin@Branch-02-cli> show orgs org Chicago sd-wan detail Branch-01

Site Id          -  101
State            -  Connected
Uptime           -  18d:13h:30m:49s
Site Name        -  Branch-01
Site Type        -  branch
Chassis Id       -  Branch-01
Global Tenant Id -  1
Management IP    -  10.255.0.8
SA Available     -  yes

Secure Tunnel Info
  Local Endpoint  -  10.255.0.10
  Remote Endpoint -  10.255.0.8
Plain Text Tunnel Info
  Local Endpoint  -  10.255.0.11
  Remote Endpoint -  10.255.0.9

LINK  LINK    ACCESS   LOCAL        LINK       SHAPING  MIN SHAPING
ID    FAMILY  CIRCUIT  IP           ENCRYPTION  RATE     RATE       TRANSPORT-DOMAINS
-------------------------------------------------------------------------------------
  1  ipv4    INET     192.168.50.11   optional   0       0          Internet
  2  ipv4    MPLS     192.168.60.11   optional   0       0          MPLS

NAT Status:

LINK  LINK    ACCESS   NAT     PUBLIC       PUBLIC  DataPath     DataPath
ID    FAMILY  CIRCUIT  STATUS  IP           PORT    IP           PORT
-----------------------------------------------------------------------
  1  ipv4    INET     true    10.43.75.158  41600   10.43.75.158  41600
  2  ipv4    MPLS     true    10.43.75.159  46223   10.43.75.159  46223
```

- Display the traffic statistics for network path to a specific SD-WAN site:

```
admin@Branch-02-cli> show orgs org Chicago sd-wan statistics aggregate Branch-01
         PTVI   ENCAP      RX    RX      TX    TX
SITE NAME  INDEX  TYPE      PKTS  BYTES   PKTS  BYTES
-----------------------------------------------------------
Branch-01  1120   plaintext  0     0       0     0
         1121   encrypted  862   162056  864   162704
```

- Clear traffic statistics for network paths to a specific SD-WAN site:

```
admin@Controller1-cli> request clear statistics sd-wan ackt all
```

Debug NAT Connectivity Issues

The SD-WAN Controller node acts as a STUN server for branch devices to resolve their NAT bindings.

To debug NAT connectivity issues, issue the following CLI commands:

- To display details about the number of NAT binding resolution requests received from each SD-WAN VOS device and for each WAN interface, issue the **show orgs org sd-wan statistics vbp branch** CLI command. For example:

```
admin@Controller1-cli> show orgs org My-Org sd-wan statistics vbp branch
BRANCH                    LINK              PUBLIC  TX    TX     RX    RX
ID    SITE NAME           ID    PUBLIC IP     PORT    PKTS  BYTES  PKTS  BYTES
-------------------------------------------------------------------------------
10    East-Coast-Controller  1
8001  Branch1-SanFrancisco   1    101.101.101.1  12983   798   12768  798  9576
                    2    192.168.12.2   4790    798   12768  798  9576
8002  Branch2-Phoneix        1    102.102.101.1  4134    800   12800  800  9600
                    2    192.168.22.2   4790    800   12800  800  9600
8003  Hub-SaltLakeCity       1    192.168.31.2   4790    592   9472   592  7104
                    2    192.168.32.2   4790    592   9472   592  7104
8004  Branch4-Detroit        1    104.104.101.1  14851   794   12704  794  9528
                    2    192.168.42.2   4790    794   12704  794  9528
8005  Branch5-Tampa          1    105.105.101.1  52559   795   12720  795  9540
                    2    192.168.52.2   4790    795   12720  795  9540
8006  Hub-Denver             1    192.168.61.2   4790    793   12688  793  9516
                    2    192.168.62.2   4790    793   12688  793  9516
```

- To clear the statistics, issue the **request clear statistics sd-wan vbp all** CLI command.
- To determine whether a branch device has attempted to resolve a NAT binding, issue the **show orgs org sd-wan statistics vbp branch** CLI command. If a NAT resolution request fails to reach the Controller node, either there is a basic connectivity issue between the branch and the Controller node or a data path issue is causing VBP packets to drop.

Stage 3 Debugging on a Branch

This section describes additional ways to debug SD-WAN connectivity from a branch node.

- Configure the branch device to establish secure connectivity to controller nodes and possibly to hubs. The branch devices continuously tries to establish connectivity.
- Ensure that WAN interfaces from the branch to the Controller node are up and have an IP address. To check for the interface status and presence of IP address, issue the **show interfaces brief** CLI command. In the following example, check that the ptvill interface to the Controller node is in the Up state, which indicates that IKE-based IPsec connectivity to the Controller node is established.

```
admin@SD-WAN-br2-cli> show interfaces brief
NAME       IP                  MAC               OPER   ADMIN  TNT  VRF
---------- ------------------- ----------------- ------ ------ ---- -----------
eth-0/0    [ 10.40.60.134/16 ]    00:50:56:8a:25:78  up     up     0    global
ptvi1      [ 41.41.40.2/32 ]      n/a               down   down   1    RT_Provider
ptvi11     [ 1.1.4.2/32 ]         n/a               up     up     1    RT_Provider
ptvi2      [ 41.2.2.2/32 ]        n/a               down   down        RT_Provider
tvi-0/1                           n/a               up     up
tvi-0/1.0  [ 10.10.12.2/24 ]      n/a               up     up     1    RT_Provider
tvi-0/2                           n/a               up     up
```

```
tvi-0/2.0   [ 20.20.22.3/24 ]      n/a              up    up    1    RT_Provider
vni-0/0                        00:50:56:8a:e5:cc  up    up
vni-0/0.0   [ 80.80.80.102/24 ]    00:50:56:8a:e5:cc  up    up    0    global
vni-0/1                        00:50:56:8a:00:e9  up    up
vni-0/1.0   [ 192.168.101.4/24 ]   00:50:56:8a:00:e9  up    up    0    grt-vrf
vni-0/2                        00:50:56:8a:96:34  down  down
```

- After establishing transport connectivity from a branch to a Controller node, at least one of the WAN interfaces is available, and the branch establishes IKE-based IPsec connectivity to the Controller node. If this is successful, the ptvi interface to the Controller node is in the Up state.
- If establishing the IKE-based IPsec connectivity fails, the ptvi interface is in the Down state. To debug, see to data path and IPsec debugging sections.
- After IPsec connectivity to at least one Controller node is established, the branch determines whether each of its WAN interfaces is behind a NAT device. To display the statistics for this activity, issue the **show orgs org sd-wan statistics vbp self** CLI command. For example:

```
admin@SD-WAN-br2-cli> show orgs org Provider sd-wan statistics vbp self
         LINK CIRCUIT     TX    TX     RX    RX
INTF NAME  ID   NAME       PKTS  BYTES  PKTS  BYTES
-----------------------------------------------------
vni-0/0.0  1    wan-isp-a   2030  178640 2030  32480
vni-0/1.0  2    wan-isp-b   2030  178640 24    384
```

- Issue the **show orgs org Provider sd-wan statistics vbp self** CLI command along with the **request clear statistics sd-wan vbp all** CLI command to determine if NAT binding resolution requests are being originated from the branch, and if response is arriving from the controller.
- Issue the **show orgs org ServiceProvider sd-wan detail** *site-id* CLI command to verify any resultant NAT binding discovered by the branch device. NAT binding is listed as public IP and public port for each WAN interface.

Troubleshoot VOS Device Deployment Failure

After you run the staging.py script and getting the management IP address, if deployment of a VOS branch device still fails, ensure that you have done the following:

- Appropriately configured prestaging and post-staging templates.
- Have connectivity between the Director node and a Controller node, and between a Controller node and a branch.

To deploy the VOS device on a branch:

1. Check the routes on the branch. The branch must have the southbound IP address of the Director node, here, 192.10.1.1
2. Check the route between the branch and the Director node

```
admin@BRANCH1001-cli> show route routing-instance grt
Routes for Routing instance : grt  AFI: ipv4
Codes: E1 - OSPF external type 1, E2 - OSPF external type 2
IA - inter area, iA - intra area,
L1 - IS-IS level-1, L2 - IS-IS level-2
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
RTI - Learnt from another routing-instance
+ - Active Route
Prot   Type  Dest Address/Mask  Next-hop  Age      Interface name
----   ----  -----------------  --------  ---      --------------
conn   N/A  +192.20.11.0/30     0.0.0.0   2w1d04h  vni-0/0.0
local  N/A  +192.20.11.2/32     0.0.0.0   2w1d04h  directly connected
```

3. Open the /var/versa/vnms/data/conf/vnms.properties file and check for the southbound IP address of the Director node in the VNF_MANAGEMENT_IP field, here, 192.10.1.1:

```
admin@BRANCH1001-cli> shell
admin@BRANCH1001-cli:/$ cat /var/versa/vnms/data/conf/vnms.properties
#added property
#Tue Jul 23 14:05:06 PDT 2019
DASHBOARD_THREAD_POOL_SIZE=50
VNMS_API_ENDPOINT_PORT=9182
VNMS_REBOOT_APPLIANCE_AFTER_IN_SEC=10
VNMS_NCS_COMMIT_TIMEOUT_IN_SECS=30
SERVICES_API_SECURE_ENDPOINT_PORT=9183
SERVICES_API_SECURE_ENDPOINT_HOST=https\://0.0.0.0
STARTUP_MODE=STANDALONE
ALARM_DATA_FORMAT=syslog
NETWORK_MAPPING=vni0/0\:WAN1,vni0/1\:WAN2,vni0/2\:LAN1
VNMS_API_ENDPOINT_HOST=https\://0.0.0.0
MAX_TASKS=5000
CONFD_API_APPLIANCE_MIN_VERSION=16.1R1S2-20170516
DESIGNATED_MASTER=TRUE
VNF_MANAGEMENT_IP=192.168.75.2
SB_ADDRESS_LIST=192.168.75.2
MANAGEMENT_IP=localhost
ALARM_PROTOCOL=tcp
SERVICES_API_ENDPOINT_HOST=https\://0.0.0.0
REDIS_DATASTORE_HOST=127.0.0.1
SERVICES_API_ENDPOINT_PORT=9182
AVAILABLE_ROUTING_INSTANCES=mgmt
REDIS_DATASTORE_PORT=6379
DASHBOARD_REFRESH_INTERVAL_IN_SECONDS=300
PACKAGE_UPLOAD_TIMEOUT_IN_MINS=60
CPU_PERCENT_THRESHOLD=70
MEMORY_PERCENT_THRESHOLD=75
DISK_PERCENT_THRESHOLD=70
MAX_AUTO_SNAPSHOTS=10
SECURE_ACCESS_APPLY_TEMPLATE_INTERVAL=15
SECURE_ACCESS_VNMS_UI_ENDPOINT_HOST=localhost
NCS_ADMIN_USER_SSH_PRIVATE_KEY_PATH=/var/versa/vnms/ncs/homes/admin/.ssh/id_rsa
NCS_ADMIN_USER_SSH_PUBLIC_KEY_PATH=/var/versa/vnms/ncs/homes/admin/.ssh/id_rsa.pub
MERGE_STRATEGY=json
SUPPORT_HTTP_OPTIONS_METHOD=false
HA_ACTION_CALLBACK_TIMEOUT=2700
SERVICES_TIMEOUT=900
CENIT_CLOUD_SERVER=wiz2.gowizcloud.com
SKIP_POLICY_DATA_XML_FETCH=FALSE
SECURITY_FILE_
TRANSFERS=true
```

4. If the address is not present in the file, edit the file and add it:

```
admin@BRANCH1001-cli~$ sudo vi /var/versa/vnms/data/conf/vnms.properties
```

5. Restart Versa services on the Director node for the changes to take effect.

Supported Software Information

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