Troubleshoot SD-WAN Branches

For supported software information, click here.

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

Check Branch Staging and Lifecycle

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

Required Controller Configuration

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

- Configure the service provider's tenant organization belonging to the Service Provider 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 needs to 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 Versa Director.

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 Versa Director. To see 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 factory-default configuration.

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

  In response to the branch connect notification, Versa Director pushes staging configuration to the branch device and requests reboot of branch device.

- After rebooting in staging configuration, branch is connected to controller. 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.

- After rebooting in final configuration, branch is connected to controller. 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 is not seen, branch is not able to connect to controller after staging. See Stage-3 Debugging on Branch.

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

- Branch is disconnected from the Controller node. This is applicable only after the completion of staging.

  > 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 check details of WAN interfaces used for SD-WAN uplink connectivity, issue the **show orgs org sd-wan site wan-intfs** CLI command. For example:

```
admin@Controller1-cli> show orgs org ServiceProvider sd-wan site wan-intfs
                                                                    MIN
         CIRCUIT     LINK              NAT              PUBLIC  LINK       SHAPING  SHAPING
INTF NAME  NAME       ID      ENDPT IP      STATUS   PUBLIC IP     PORT    ENCRYPTION  RATE
RATE
-------------------------------------------------------------------------------------------------
vni-0/0.0  Braodband1  1       192.168.211.2  unknown  0.0.0.0       4790    optional    0       0
vni-0/1.0  Broadband2  2       192.168.212.2  unknown  0.0.0.0       4790    optional    0       0
vni-0/2.0  MPLS        3       192.168.213.2  unknown  192.168.213.2 4790    optional    0       0
```

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

```
admin@Controller1-cli> show orgs org ServiceProvider sd-wan site statistics vni
         RX            TX            TX   RX
VNI NAME   PKTS   RX BYTES  PKTS   TX BYTES  BPS  BPS
-----------------------------------------------------
vni-0/0.0  96780  50753136  62047  12240536  0    0
vni-0/1.0  13423  2469832   34393  7409432   0    0
```

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

Low-Level vty Commands

Low-level commands for in-depth debugging are available from infmgr shell. From the Linux shell prompt, issue the **vsh connect infmgr** to get to the infmgr shell.

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 ServiceProvider 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 for a specific node, issue the following version of the **show p2mp nbrs detail** CLI command:

```
infmgr> show p2mp nbrs detail ServiceProvider Branch1-SanFrancisco
```

Stage 3 Debugging on a Controller Node

An SD-WAN Controller node manages multiple branch/hub sites for one or more customer tenants. The typical debug workflow involves getting 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 ServiceProvider sd-wan site summary
Branches in connected state      :   6
Branches in disconnected state   :   0
Branches in erroneous state      :   1
```

- Display brief information about all SD-WAN sites managed by the Controller node:

```
admin@Controller1-cli> show orgs org ServiceProvider sd-wan site brief
SITE                    MANAGEMENT                CONNECTIVITY  IS
ID SITE NAME              IP          TYPE    UP TIME    STATUS     CTRLR
-------------------------------------------------------------------------------------------------------------------------
10 East-Coast-Controller-1  10.10.110.2  local   1h:3m:49s  -          yes
8001  Branch1-SanFrancisco  10.10.111.2  remote  1h:3m:30s  Connected  no
8002  Branch2-Phoneix       10.10.112.2  remote  1h:3m:33s  Connected  no
8003  Hub-SaltLakeCity      10.10.113.2  remote  46m:25s    Connected  no
8004  Branch4-Detroit       10.10.114.2  remote  1h:3m:19s  Connected  no
8005  Branch5-Tampa         10.10.115.2  remote  1h:3m:20s  Connected  no
8006  Hub-Denver            10.10.116.2  remote  1h:3m:17s  Connected  no
```

- Display connectivity event history for all SD-WAN sites in error state, as well as in the Up and Down states:

```
admin@Controller1-cli> show orgs org ServiceProvider sd-wan site history current-status ?
Possible completions:
 DOWN  ERRONEOUS  UP
admin@Controller1-cli> show orgs org ServiceProvider sd-wan site history current-status
ERRONEOUS
Branch History:
 Branch-id        : 65
 Branch-name      : Hub-SaltLakeCity
 current-status   : ERRONEOUS
 Logs             :
 Record :
  Event-message   : Poststaging done
  Timestamp       : 2016-03-30 17:23:14
 Record :
  Event-message   : Poststaging done
  Timestamp       : 2016-03-30 17:37:50
```

Branch-Specific Commands

- Check the details of a specific SD-WAN site:

```
admin@Controller1-cli> show orgs org ServiceProvider sd-wan site detail 8001
Branch Id      :  8001
State          :  Connected
Uptime         :  1h:3m:51s
Branch Name    :  Branch1-SanFrancisco
Chassis Id     :  001branch1
Global Tenant Id  :  1
Management IP  :  10.10.111.2
SA Available   :  no
ESP Tunnel Info
Local Endpoint  :  10.10.110.2
Remote Endpoint :  10.10.111.2
VXLAN Tunnel Info
Local Endpoint  :  10.10.10.2
Remote Endpoint :  10.10.11.2
```

```
LINK  ACCESS       LOCAL  NAT     PUBLIC       PUBLIC  LINK       SHAPPING  MIN SHAPPING
 ID  CIRCUIT      IP     STATUS  IP           PORT    ENCRYPTION  RATE      RATE
-------------------------------------------------------------------------------------
 1    101.101.101.1       Unknown 101.101.101.1 12983   plain-text  0         0
```

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

```
admin@Controller1-cli> show orgs org ServiceProvider sd-wan site history branch-name Branch1-SanFrancisco
Branch History:
 Branch-id        : 8001
 Branch-name      : Branch1-SanFrancisco
 current-status   : UP
 Logs             :
 Record :
  Event-message   : IKE attempted
  Timestamp       : 2016-03-30 17:23:08
 Record :
  Event-message   : IKE completed
  Timestamp       : 2016-03-30 17:23:12
```

- Check traffic statistics per network path to a specific SD-WAN site:

```
admin@Controller1-cli> show orgs org ServiceProvider sd-wan site statistics aggregate 8001
SITE  PTVI   ENCAP     RX    RX     TX    TX
ID    INDEX  TYPE      PKTS  BYTES  PKTS  BYTES
-----------------------------------------------------
8001  1066   plaintext  0     0      0     0
8001  1076   encrypted  0     0      0     0
```

- 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 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 site statistics vbp branch** CLI command. For example:

```
admin@Controller1-cli> show orgs org ServiceProvider sd-wan site 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 site 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 site statistics vbp self** CLI command. For example:

```
admin@SD-WAN-br2-cli> show orgs org Provider sd-wan site 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
```

- Run the show orgs org Provider sd-wan site 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.
- Run the show orgs org ServiceProvider sd-wan site 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 Versa Director and a Controller node, and between a Controller node and a branch.

To deploy the VOS device on a branch:

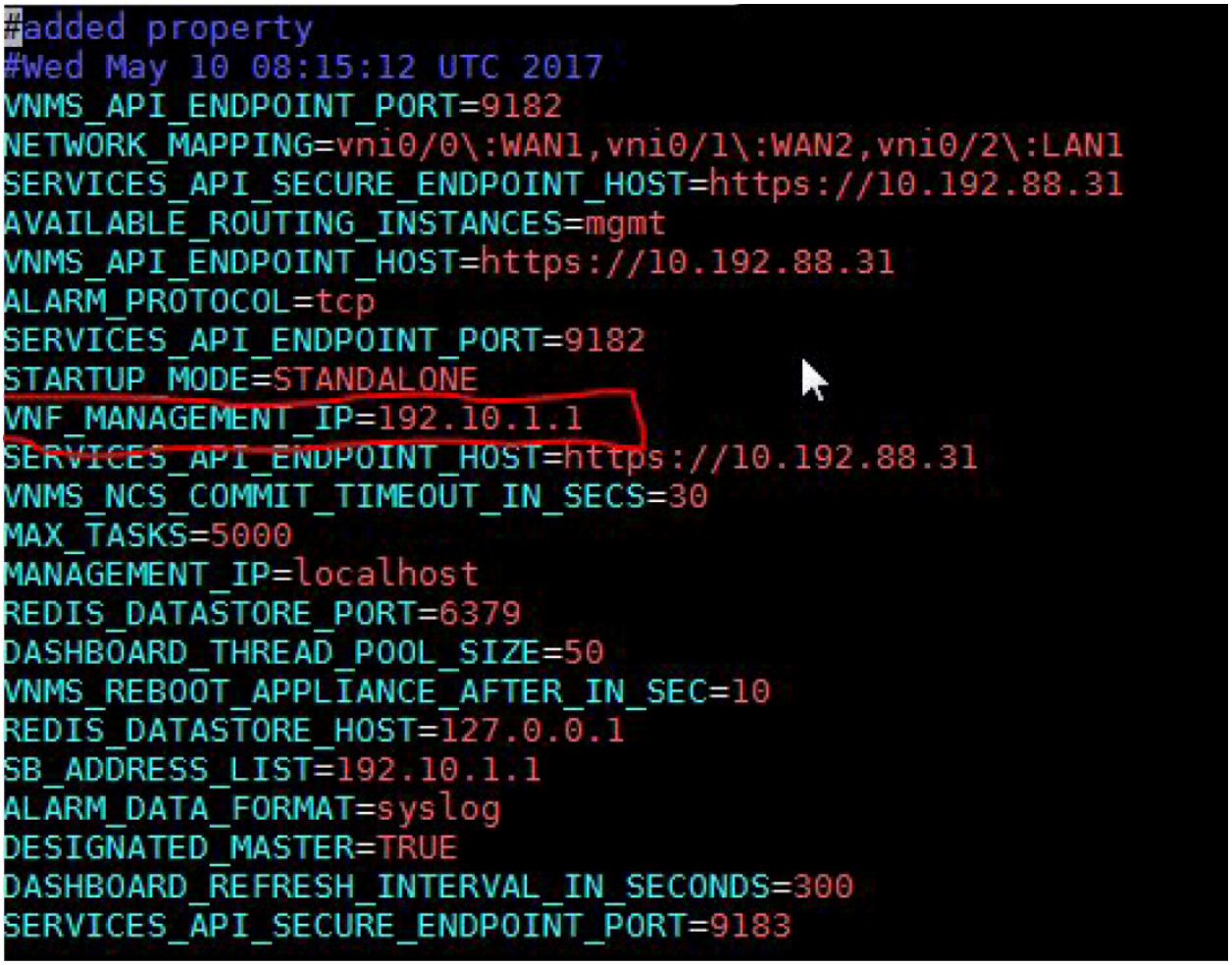
1. Check the routes on the branch. The branch must have the southbound IP address of the Versa Director, here, 192.10.1.1
2. Check the route between the branch to the Versa Director.

```
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 Versa Director, here, 192.10.1.1. If the address is not present in the file, edit the file and add it.

4. Open the log file:

```
admin@LAB2-DIRECTOR:~$ sudo vi /var/versa/vnms/data/conf/vnms.properties
```



Supported Software Information

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