Use the VSync Tool with VOS Devices

For supported software information, click here.

This article describes how to configure and monitor the IP address, IP port, and URL using Phase 2 of the VSync tool.

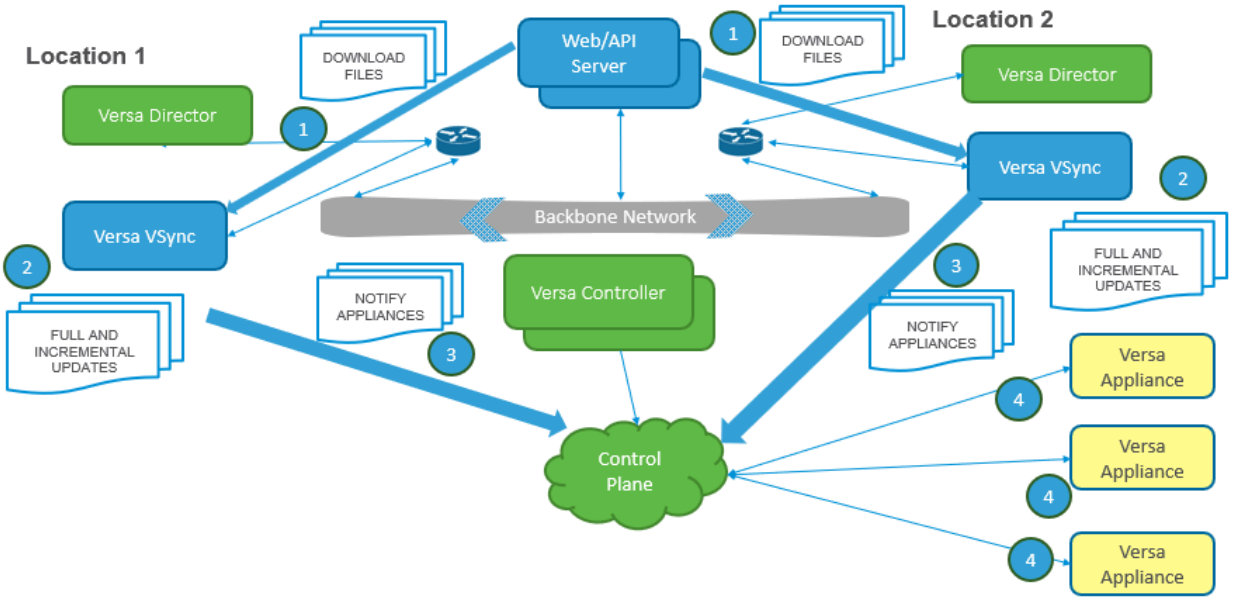
When your organization or enterprise maintains threat intelligence databases across multiple web and RESTful servers, you can use the VSync tool to distribute the threat intelligence information from all the databases to the Versa Operating System™ (VOS™) SD-Security devices in your SD-WAN network. The VSync tool automatically detects updates to these databases and distributes the new information to the VOS devices. The VSync tool allows you to enforce security policies based on address group objects and custom URL category objects.

Use Threat Intelligence Databases

Enterprises maintain threat intelligence databases, which include IP addresses, port numbers, and URLs, on web or RESTful API servers, and they can host different threat intelligence databases on different servers. You can configure a web server on which the VSync tool downloads threat files at a specified interval. The VSync tool supports the following types of threat files:

- IP addresses
- IP ports
- URLs

The following figure illustrates the placement of the VSync nodes in the network.



The figure illustrates the sequence of events in VSync tool operation:

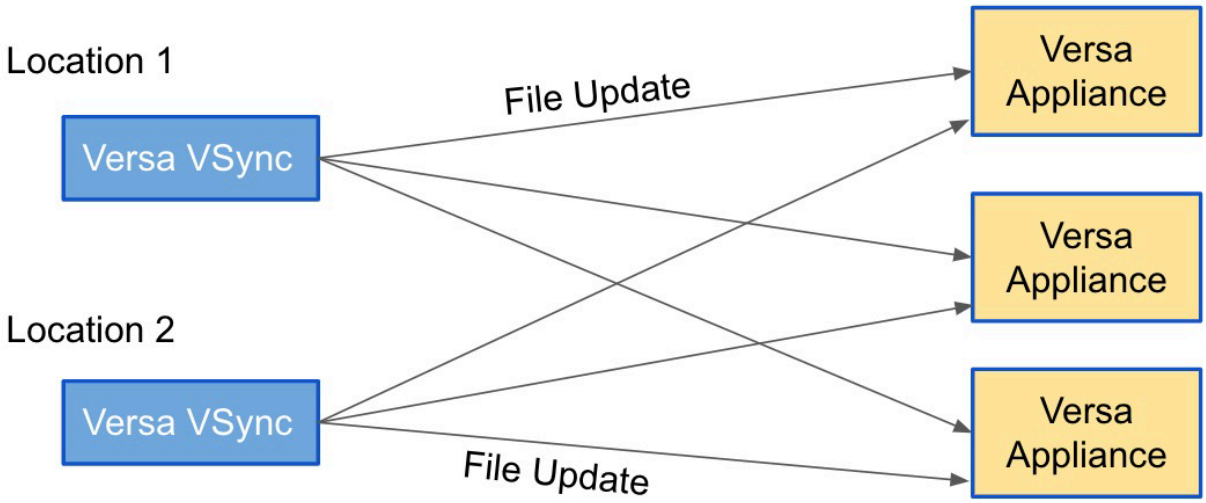
1. The VSync node downloads the latest version of the threat file.
2. The VSync node builds full and incremental updates.
3. The VSync node notifies the VOS devices (appliances) that a new version of the threat file is available.
4. The appliances download a full or an incremental feed from the VSync node.
5. The appliances install the new version of the threat file.

Depending on the changes in the web server database, the VSync tool creates a new version for the threat file. The VSync tool also creates a diff-file between the previously available threat file versions and the new version. Then VSync tool adds the new version of the threat file to the VOS device. See Add Threat Files from a VOS Device.

The VSync node creates full and incremental updates for the threat files. For files from the single VSync node, VOS ignores the request for a threat file with a lower version if a higher version or the same version of the threat file is available.

Configure VSync HA

To have VSync support high availability (HA) mode, you deploy two VSync nodes, as illustrated in the following figure. The figure shows that the two VSync nodes connect to a VOS device and trigger a VSync update, but the VOS device processes file update requests only from the currently active VSync node.



If the preferred-active VSync node is reachable, the VOS device denies the request to update a file from other VSync nodes and the preferred-active VSync node becomes the currently active node. When a file update request comes from a node other than the currently active node, the VOS device checks the connectivity of the preferred-active VSync node. If the preferred VSync node is reachable, the VOS device drops the request to update a file and the requested VSync node becomes standby VSync node. If the preferred-active VSync node is not reachable within the timeout period (default 5 seconds), the VOS device accepts the file update request from any VSync node. In this case, the requested VSync node becomes the currently active node and the preferred-active node becomes the standby node until it is reachable from the VOS device. This situation is considered as a VSync HA failover event.

When you do not configure a preferred-active node, the VSync node from which the first file update request comes to the VOS device becomes the currently active VSync node. When a file update request comes from a node other than the currently active node, the VOS device checks the connectivity to the currently active node. If the currently active node is reachable, the VOS device drops the file update request and the requested VSync node becomes standby node. If the currently active VSync node is not reachable within the timeout period (default 5 seconds), a VSync HA failover occurs: the requested VSync node becomes the currently active node and the currently active node becomes the standby node.

To set the preferred VSync node, issue the following command:

```
admin@branch1-cli> request vsync ha set preferred-active vsync-node vsync-node-name ip-address ip-address
status success
result Successfully configured preferred active Vsync node
```

To clear the preferred VSync node, issue the following command:

```
admin@branch1-cli> request clear vsync preferred-active
status success
result Preferred Vsync active node config cleared
```

To display the configured preferred VSync node, issue the following command:

```
admin@branch1-cli> show vsync ha vsync-nodes summary

TYPE       NAME         IP ADDRESS
-----------------------------------------
Preferred  vsync-node-1  10.192.199.81
Current    -            -
Standby    -            -
```

To configure the connectivity check timeout period on the VSync node, issue the following command:

```
admin@branch1-cli> request vsync ha set connection-check timeout seconds recheck-interval seconds
status success
result Success
```

Field	Description
timeout *seconds*	How long to wait before declaring the VSync node to be down. *Range:* 2 through 10 seconds *Default:* 5 seconds
recheck-interval *seconds*	When the other VSync node sends a file update request, how long to wait before checking the availability of VSync node. *Range:* 120 through 43200 seconds (2 minutes through 12 hours) *Default:* 120 seconds

To display the configured VSync node connectivity check timeout period, issue the following command:

```
admin@branch1-cli> show vsync ha vsync-nodes connection-check

              RECHECK
TIMEOUT       INTERVAL
--------------------------------
5             120
```

To enable HA functionality on VSync nodes, you must open port 9001 on the Controller node for all branches. To create a service object for destination port 9001 and append it to an existing policy rule on the Controller node, issue the following commands:

```
admin@branch1-cli(config)% set orgs org-services organization-name objects services service-name protocol TCP
admin@branch1-cli(config)% set orgs org-services organization-name objects services service-name destination-port 9001
admin@branch1-cli(config)% set orgs org-services organization-name security access-policies Default-Policy rules rule-name match services services-list service-name
```

For example:

```
admin@branch1-cli(config)% set orgs org-services versa objects services VSync-HA-Ports protocol TCP
admin@branch1-cli(config)% set orgs org-services versa objects services VSync-HA-Ports destination-port 9001
admin@branch1-cli(config)% set orgs org-services versa security access-policies Default-Policy rules Allow-From-CPE-Ports match services services-list VSync-HA-Ports
```

Add Threat Files from a VOS Device

To add a new version of a threat file, issue the following command. The following table explains the command options.

```
admin@branch1-cli> request orgs org-services organization-name vsync add
Possible completions:
  auto-install    : Install VSync threat file after download completes
  file-name       : VSync threat file name
  file-type       : VSync threat file type
  update-type     : Update type can be full or incremental
  url             : Directory URL
  version         : VSync version number of the file
  vsync-node      : VSync active node name
```

Field	Description
Auto-Install	Install the VSync threat file after the download is complete: • True—Perform the installation automatically. This is the default. • False—Set for debugging.
Filename	Enter the name of the VSync threat file.
File Type	Enter the type of threat file: • IP address • IP port • URL

Field	Description
Update Type	Enter the update type: • Full update • Incremental update
URL	Enter the URL of the web server directory where the VSync threat file csv is present.
Version	Enter the version number of the threat file.
VSync Node	Enter the name of the installed VSync node. The VSync node is used to identify the node from which the request to add a file in HA environment comes.

For a full update, the VOS device creates a URL for the update file path based on the version number in the request command.

To download a full update, issue issue the following command. Type the command on a single line.

> admin@branch1-cli> **request orgs org-services** *organization-name* **vsync add auto-install true file-name** *filename*
> **file-type** *file-type* **url** *server-url* **version** *number* **update-type full vsync-node** *vsync-node-name*

For example:

> admin@branch1-cli> **request orgs org-services o1 vsync add auto-install true file-name threat-file.csv file-type ip-address url http://bng-bugdump.versa-networks.com/temp-branch1/vsync version 111 update-type full vsync-node vsync-ha-4**
> status success
> result Download started for url http://bng-bugdump.versa-networks.com/temp-branch1/vsync/111/full/threat-file.csv with download-id 2005

To download an incremental update, issue the following command:

> admin@branch1-cli> **request orgs org-services** *organization-name* **vsync add auto-install true file-name** *filename*
> **file-type** *file-type* **url** *server-url* **version** *number* **update-type incremental vsync-node** *vsync-node-name*

For example:

> admin@branch-cli> **request orgs org-services o1 vsync add auto-install true file-name threat-file.csv file-type ip-address url http://bng-bugdump.versa-networks.com/temp-branch1/vsync version 102 update-type**
> **incremental vsync-node vsync-ha-1 file-size [5.1 3.2 5.3 8.4]**
> status success
> result Download started for url http://bng-bugdump.versa-networks.com/temp-branch1/vsync/102/incremental/100/threat-file.csv with download-id 2006

For incremental update, the VOS device creates a URL for the incremental update file path based on the version number and the previously available version of the threat file.

To cancel a download process, issue the following commands. Note that if the first **request cancel** command does not return the download ID, the first download request is cancelled. To determine the file download ID, issue the **download status** command.

```
admin@branch-cli> request orgs org-services organization-name vsync cancel ?
Description: Cancel running download of the file
Possible completions:
  download-id  :  Cancel vsync threat file download of this download ID
  file-type    :  Vsync threat file type
```

```
admin@branch1-cli> request orgs org-services organization-name vsync cancel file-type ?
Description: Vsync threat file type
Possible completions:
  ip-address  ip-port  url
```

For example:

```
admin@branch1-cli> request orgs org-services o1 vsync cancel file-type ip-address
status success
result Download cancelled for download-id 2002
```

```
admin@branch1-cli> request orgs org-services o1 vsync cancel file-type ip-address download-id 2004
status success
result Download cancelled for download-id 2004
```

To check the pending download status of the file, issue the following commands:

```
 admin@branch1-cli> request orgs org-services o1 vsync status ?
 Possible completions:
  download-id      : Show vsync threat file status of this download ID
  file-type        : vsync threat file type
  last-n-downloads : Show vsync threat file status of last 'n' downloads; max 50
```

```
admin@branch1-cli> request orgs org-services o1 vsync status file-type
Possible completions:
  ip-address  ip-port  url
```

To check the download status for the number of the downloads of a specific file type, issue the following command. Specify the number of downloads in the **last-n-downloads** option.

```
admin@branch1-cli> request orgs org-services o1 vsync status file-type url last-n-downloads 3
[Status: OK]
[Total download attempts: 2006]
[Total successful downloads: 2006]
----------------------------------------
[downloaded by: admin]
[download ID: 2006]
[download start time: 2022-02-18 00:48:49]
[download end time: 2022-02-18 00:48:50]
```

```
[download status: OK]
[download message: Download successful]
[downloaded filename: https://192.168.77.2/vsync/vsync-1/versa-url/7434/full/versa-url-urldata.csv]
[download size(bytes): 2260920]
[download percent: 100]
---------------------------------------
[downloaded by: admin]
[download ID: 2005]
[download start time: 2022-02-18 00:48:45]
[download end time: 2022-02-18 00:48:45]
[download status: OK]
[download message: Download successful]
[downloaded filename: https://192.168.77.2/vsync/vsync-1/versa-domain/6369/full/versa-domain-urldata.csv]
[download size(bytes): 15267]
[download percent: 100]
---------------------------------------
[downloaded by: admin]
[download ID: 2004]
[download start time: 2022-02-18 00:48:17]
[download end time: 2022-02-18 00:48:18]
[download status: OK]
[download message: Download successful]
[downloaded filename: https://192.168.78.2/vsync/vsync-2/versa-domain/6361/incremental/6360/versa-domain-
urldata.csv]
[download size(bytes): 247]
[download percent: 100]
```

To use the download ID to check the file download status, issue the following command:

```
admin@branch1-cli> request orgs org-services o1 vsync status file-type url download-id 2006
[Status: OK]
[Total download attempts: 2006]
[Total successful downloads: 2006]
[downloaded by: admin]
[download ID: 2006]
[download start time: 2022-02-18 00:48:49]
[download end time: 2022-02-18 00:48:50]
[download status: OK]
[download message: Download successful]
[downloaded filename: https://192.168.77.2/vsync/vsync-1/versa-url/7434/full/versa-url-urldata.csv]
[download size(bytes): 2260920]
[download percent: 100]
```

The following example shows the **request status** command output for the last download status for the file type URL:

```
admin@branc1-cli> request orgs org-services o1 vsync status file-type url
[Status: OK]
[Total download attempts: 4]
[Total successful downloads: 4]
[Last downloaded by: admin]
[Last download ID: 4]
[Last download start time: 2022-02-21 23:12:12]
[Last download end time: 2022-02-21 23:12:12]
```

```
[Last download status: OK]
[Last download message: Download successful]
[Last downloaded filename: https://10.40.134.70/vsync/vsync-1/vsync-test-domain/37/incremental/33/vsync-test-domain-urldata.csv]
[Last download size(bytes): 178]
[Last download percent: 100]
```

To remove a file that is not in use, issue the following command:

```
admin@branch1-cli> request orgs org-services organization-name vsync remove file-type url file-name vsync-test-domain-urldata.csv
status success
result File removed successfully
```

If you try to remove a file that is referred to in the configuration, the following message displays:

```
admin@branch1-cli> request orgs org-services organization-name vsync remove file-type ip-address file-name threat-file.csv
status failure
result IP-address file threat-file.csv is being used. Please first remove it from address-group.
```

To set an alarm destination, issue one of the following commands:

```
admin@branch1-cli> request alarms set destinations [ snmp ] alarm-type vsync-file-download-success-trap
status success
result alarm destination changed successfully
```

```
admin@branch1-cli> request alarms set alarm-type vsync-file-download-failure-trap  destinations [ snmp syslog ]
status success
result alarm destination changed successfully
```

```
admin@branch1-cli> request alarms set alarm-type vsync-invalid-incremental-patch-trap destinations [ none ]
status success
result alarm destination changed successfully
```

```
admin@branch1-cli> request alarms set alarm-type vsync-file-validation-failure-trap destinations [ snmp ]
status success
result alarm destination changed successfully
```

```
admin@branch1-cli> request alarms set alarm-type address-group-file-compilation-failure-trap destinations [ snmp ]
status success
result alarm destination changed successfully
```

```
admin@branch1-cli> request alarms set alarm-type ipguard-vsync-update-failure-trap [ snmp ]
status success
result alarm destination changed successfully
```

```
admin@branch1-cli> request alarms set alarm-type ipguard-vsync-update-success-trap   [ snmp ]
status success
result alarm destination changed successfully
```

To view the alarm destinations for yang configuration changes, issue the following command:

```
admin@branch1-app-188-2-14:~$ ls -ltr /opt/versa/var/oam/
total 24
-rw-r--r-- 1 versa versa 12 Dec  1 22:17 vsync-file-download-success.txt
-rw-r--r-- 1 versa versa 12 Dec  1 22:17 vsync-file-download-failure.txt
-rw-r--r-- 1 versa versa  5 Dec  1 22:17 vsync-invalid-incremental-patch.txt
-rw-r--r-- 1 versa versa  5 Dec  1 22:18 vsync-file-validation-failure.txt
-rw-r--r-- 1 versa versa  5 Dec  1 22:18 address-group-file-compilation-failure.txt
-rw-r--r-- 1 versa versa  5 Dec  1 22:18 address-group-file-compilation-success.txt
admin@branch1-app-188-2-14:~$ cat filename
```

For example:

```
admin@branch1-app-188-2-14:~$ cat /opt/versa/var/oam/vsync-file-download-success.txt
SNMP
Syslog
```

To clear VSync statistics, issue the following command:

```
admin@branch1-cli> request clear statistics vsync org org-name organization-name stat-type ?
Possible completions:
  all  common  ip-address  ip-port  url
```

For example:

```
admin@branch1-cli> request clear statistics vsync org o1 stat-type all
status success
result Cleared statistics
```

```
admin@branch1-cli> request clear statistics vsync org o1 stat-type common
status success
result Cleared statistics
```

```
admin@branch1-cli> request clear statistics vsync org o1 stat-type ip-address
status success
result Cleared statistics
```

```
admin@branch1-cli> request clear statistics vsync org o1 stat-type ip-port
status success
result Cleared statistics
```

```
admin@branch1-cli> request clear statistics vsync org o1 stat-type url
status success
result Cleared statistics
```

To display the VSync version number of the installed file, issue the following command:

```
admin@branch1-cli> show orgs org-services organization-name vsync version

                 BEING  VERSION
FILE NAME        USED   NUMBER   VSYNC NODE
-----------------------------------------------------------------
```

```
threat-file.csv       true     102     vsync-ha-1

                  BEING  VERSION  VSYNC
FILE NAME           USED   NUMBER   NODE
-------------------------------------------------------
urlf_test_threat.csv  false         -            -
```

Display VSync File Statistics

To display VSync file statistics, issue the following command:

```
admin@branch1-cli> show orgs org-services organization-name vsync statistics
```

For example:

```
admin@branch1-cli> show orgs org-services o1 vsync statistics
Possible completions:
  common     - Vsync common statistics
  ip-address - Vsync IP-address file statistics
  ip-port    - Vsync IP-port file statistics
  url        - Vsync URL file statistics
```

```
admin@Branch-11-cli> show orgs org-services o1 vsync statistics
                          NUM
    NUM FILE   NUM INC    NUM INC   INVALID   FILE    INVALID   NUM
ORG  ADD       UPDATE     UPDATES   URL       NAME    FILE      DUPLICATE
ID   REQUESTS  REQUESTS   ALLOWED   REQUESTS  CLASH   EXT       REQUESTS
-----------------------------------------------------------------------
5    0         0          0         0         0       0         0

                                FILE      ERROR   NUM      CANCEL
          FILE      FILE      INVALID     FORMAT    RSP     CANCEL   DOWNLOAD
ORG       DOWNLOAD  DOWNLOAD  INCREMENTAL VALIDATION FROM    DOWNLOAD REQUEST
ID FILE TYPE  SUCCESS   FAILURES PATCH      FAILURES   SERVER  REQUESTS FAILURES
-------------------------------------------------------------------------------
1  IP-address 0         0       0          0         0       0       0

                             FILE       ERROR   NUM      CANCEL
        FILE      FILE      INVALID     FORMAT     RSP     CANCEL   DOWNLOAD
ORG FILE  DOWNLOAD  DOWNLOAD INCREMENTAL VALIDATION  FROM    DOWNLOAD REQUEST
ID  TYPE  SUCCESS   FAILURES PATCH      FAILURES    SERVER  REQUESTS FAILURES
---------------------------------------------------------------------------
1   URL   0         0       0          0         0       0       0

                                FILE      ERROR   NUM      CANCEL
          FILE      FILE      INVALID     FORMAT     RSP     CANCEL   DOWNLOAD
ORG FILE      DOWNLOAD DOWNLOAD INCREMENTAL VALIDATION FROM    DOWNLOAD REQUEST
ID  TYPE      SUCCESS  FAILURES PATCH      FAILURES   SERVER  REQUESTS FAILURES
-------------------------------------------------------------------------------
1   IP-port   0        0        0          0         0       0       0
```

```
admin@Branch-11-cli> show orgs org-services o1 vsync statistics common
```

```
                          NUM                                  NUM
   NUM FILE  NUM INC   NUM INC  INVALID   FILE   INVALID  NUM       NUM FILE  VSYNC     NUM
VSYNC
ORG  ADD      UPDATE    UPDATES  URL      NAME   FILE     DUPLICATE  ADD REQ   NODE HA
NODES
ID   REQUESTS  REQUESTS  ALLOWED  REQUESTS  CLASH  EXT     REQUESTS   FAILURES
FAILOVER  UNREACHABLE
-------------------------------------------------------------------------------------------------------
1    0        0        0        0        0      0       0          0          0         0
```

```
admin@Branch-11-cli> show orgs org-services o1 vsync statistics ip-address
                                  FILE       ERROR   NUM       CANCEL
            FILE     FILE     INVALID     FORMAT     RSP     CANCEL    DOWNLOAD
ORG           DOWNLOAD  DOWNLOAD  INCREMENTAL  VALIDATION  FROM    DOWNLOAD  REQUEST
ID   FILE TYPE   SUCCESS   FAILURES  PATCH       FAILURES    SERVER  REQUESTS  FAILURES
-----------------------------------------------------------------------------------------
1    IP-address  0         0         0           0           0       0         0
```

```
admin@Branch-11-cli> show orgs org-services o1 vsync statistics ip-port
                                  FILE       ERROR   NUM       CANCEL
          FILE     FILE     INVALID     FORMAT     RSP     CANCEL    DOWNLOAD
ORG  FILE    DOWNLOAD  DOWNLOAD  INCREMENTAL  VALIDATION  FROM    DOWNLOAD  REQUEST
ID   TYPE    SUCCESS   FAILURES  PATCH       FAILURES    SERVER  REQUESTS  FAILURES
-----------------------------------------------------------------------------------------
1    IP-port  0         0         0           0           0       0         0
```

```
admin@Branch-11-cli> show orgs org-services o1 vsync statistics url
                                FILE       ERROR   NUM       CANCEL
        FILE     FILE     INVALID     FORMAT     RSP     CANCEL    DOWNLOAD
ORG  FILE  DOWNLOAD  DOWNLOAD  INCREMENTAL  VALIDATION  FROM    DOWNLOAD  REQUEST
ID   TYPE  SUCCESS   FAILURES  PATCH       FAILURES    SERVER  REQUESTS  FAILURES
-----------------------------------------------------------------------------------
1    URL   0         0         0           0           0       0         0
```

To display the preferred VSync node, the currently active VSync node, and the standby VSync node, issue the following command:

```
admin@branch1-cli> show vsync ha vsync-nodes summary

TYPE           NAME         IP ADDRESS
----------------------------------------
Preferred      vsync-node-1  10.192.199.81
Current        -             -
Standby        -             -
```

To display the history of the threat files that have been downloaded to the VSync node, issue the following command:

```
admin@branch11-cli> show orgs org-services organization-name vsync history url vsync-test-domain-urldata.csv

                                  VSYNC          PREVIOUS  DOWNLOAD     DOWNLOAD  UPDATE
COMPILATION
FILE NAME                 TIME             NODE     VERSION  VERSION   TYPE       STATUS    TYPE
```

```
STATUS      MESSAGE
-------------------------------------------------------------------------------------------------------------------------------
vsync-test-domain-urldata.csv  2022-01-11:04:19:16  vsync-1  1       NA       full       success  full   NA
Not in use
                               2022-01-20:13:51:47  vsync-1  4       1        incremental  success  NA   NA        Not in
use
                               2022-01-20:17:10:07  vsync-1  5       4        incremental  success  NA   NA        Not in
use
                               2022-01-20:19:03:03  vsync-1  6       5        incremental  success  NA   NA        Not in
use
                               2022-01-20:19:09:14  vsync-1  7       6        incremental  success  NA   NA        Not in
use
```

Configure IP Address Threat Files

The VSync tool helps to download threat files from web servers at specified intervals and execute request commands at VOS to use the latest available version of the threat files. The IP address threat file support allows to download multiple IP address threat files from different and multiple web servers. VOS supports configuration of multiple files.

You can add IP address threat files to VOS from Versa Director and VSync tool and both files can be used to configure IP address threat files. For IP address threat files, VOS processes only full update. Incremental update is not processed.

Note that you enter all commands on a single line. The examples are shown as two lines or more for readability.

To add an IP address threat files to a VOS device from a Director node, issue the following command:

```
admin@branch1-cli> request orgs org-services organization-name objects address-groups add url
file:///home/admin/ip-addr.csv
```

For example:

```
admin@branch1-cli> request orgs org-services o1 objects address-groups add url file:///home/admin/ip-
addr.csv
Download started for url file:///home/admin/ip-addr.csv
```

The VOS device stores the files in the /opt/versa/var/policy/1*organization-id*/ directory. If you update a file from the VSync tool that has the same name as one that is uploaded from the Director node, an error message displays.

For example:

```
admin@branch1-cli> request orgs org-services organization-name vsync add auto-install true file-name ip-
addr.csv file-type ip-address url
http://bng-bugdump.versa-networks.com/temp-branch1/vsync version 102 update-type incremental
vsync-node vsync-ha-1
file-size [ 5.1 3.2 5.3 8.4 ]
status failure
result Already uploaded files from the Director can not be updated from Vsync
```

To add threat files to a VOS device from the VSync tool for a full update, issue the following command:

```
admin@branch1-cli> request orgs org-services organization-name vsync add auto-install true file-name filename
file-type file-type url server-url version number update-type full vsync-node vsync-node-name
```

For example:

```
admin@branch1-cli> request orgs org-services o1 vsync add auto-install true file-name threat-file.csv file-type ip-address url
http://bng-bugdump.versa-networks.com/temp-branch1/vsync version 111 update-type full vsync-node vsync-ha-4
status success
result Download started for url http://bng-bugdump.versa-networks.com/temp-branch1/vsync/111/full/threat-file.csv with download-id 2004
```

To add threat files to a VOS device from the VSync tool for an incremental update, issue the following command:

```
admin@branch1-cli> request orgs org-services organization-name vsync add auto-install true file-name filename
file-type file-type url server-url version number update-type incremental vsync-node vsync-node-name
```

For example:

```
admin@branch1-cli> request orgs org-services o1 vsync add auto-install true file-name threat-file.csv file-type ip-address
url http://bng-bugdump.versa-networks.com/temp-branch1/vsync version 102 update-type incremental vsync-node vsync-ha-1
file-size [ 5.1 3.2 5.3 8.4 ]
status success
result Download started for url http://bng-bugdump.versa-networks.com/temp-branch1/vsync/102/incremental/100/threat-file.csv with download-id 2002
```

The VOS device stores the files in the /opt/versa/var/policy/1*organization-name*/vsync-ha-1*vsync-node-name* directory. If the format of the IP address file is invalid format or there is an error response from the server, the IP address file is moved to the /opt/versa/var/vsync-failure/o1*organization-name*/vsync-ha-1*vsync node name*/IP-address directory for debugging.

To display all the IP address files added from VSync tool and Director, issue the following command and then use autocompletion:

```
admin@branch1-cli(config)% set orgs org-services organization-name objects address-groups address-group-name address-files
```

For example:

```
admin@branch1-cli(config)% set orgs org-services o1 objects address-groups ad-gp-1 address-files
Possible completions:
 [ ip-addr-2.csv  ip-addr-common.csv  ip-addr.csv  threat-file.csv
```

After the IP address files are downloaded to the VOS device, you can configure an address group object with references to one or more IP address files so that the contents of all the IP address files are loaded into the address group object. You can then reference the address group object in the IP filtering profile object configuration and in any policy rule such

as security access and decryption policy.

When network traffic is evaluated by a policy rule or an IP filtering profile, if the policy rule or the IP filtering profile refers to an address group object that references one or more IP address files, the network traffic is evaluated for a match based on all the IP addresses in the IP address files.

To configure the file within address groups, issue the following command:

```
admin@branch1-cli(config)% set orgs org-services organization-name objects address-groups address-group-name address-files [ filename ]
```

For example:

```
admin@branch1-cli(config)% set orgs org-services o1 objects address-groups ad-gp-1 address-files [ threat-file.csv ip-addr.csv ]
```

```
[edit]
admin@branch1-cli(config)% show orgs org-services o1 objects address-groups ad-gp-1
address-files [ ip-addr.csv threat-file.csv ];
```

```
[edit]
admin@branch1-cli(config)% commit
Commit complete.
```

Use the address group configured in the IP filtering profile. The following example shows how to view the IP filtering profile:

```
admin@branch1-cli(config)% show orgs org-services organization-name security profiles ip-filtering
ipfp1 {
    black-list {
        ip-addresses {
            address-groups [ ad-gp-1 ];
        }
        action {
            predefined [ reject ];
        }
    }
}
```

View Address Groups

To view the address group configured, issue the following command:

```
admin@vsync-b1-cli(config)% show orgs org-services organization-name objects address-groups
Description: Group of address lists
Possible completions:
ad-gp1
Possible match completions:
```

```
description - Description of the address group list
address-list - Name of the prefix
address-group-list - Name of the group
address-files - address list files
```

To view the IP address files configured, issue the following command:

```
admin@vsync-b1-cli> show orgs org-services versa vsync version ip-address
                          BEING  VERSION  VSYNC
FILE NAME                       USED   NUMBER   NODE
-------------------------------------------------------------
ipv4-addresses-txt-file-ipdata.csv  true   6        vsync-01
```

To view the IP port file, issue the following command:

```
admin@vsync-b1-cli> show orgs org-services versa vsync version ip-port
             BEING  VERSION  VSYNC
FILE NAME       USED   NUMBER   NODE
-----------------------------------------
threat-file.db  true   15       vsync-02
```

VSync SNMP Traps

This section shows the output of all the VSync SNMP traps.

The following example output shows an address group file compilation message when data structure creation from file entries succeeds:

```
SNMPv2-MIB::sysUpTime.0 = Timeticks: (55622) 0:09:16.22
SNMPv2-MIB::snmpTrapOID.0 = OID:
POLICY-TRAP::addressGroupFileCompilationSuccess
   TRAPS-COMMON::alarmType.0 = STRING: addressGroupFileCompilationSuccess
   TRAPS-COMMON::alarmDevice.0 = STRING: policy
   TRAPS-COMMON::alarmObject.0 = STRING: "addressGroupFileCompilationSuccess"
   TRAPS-COMMON::alarmSpecificProblem.0 = ""
   TRAPS-COMMON::alarmClass.0 = INTEGER: new(0)
   TRAPS-COMMON::alarmEventType.0 = INTEGER: equipmentAlarm(5)
   TRAPS-COMMON::alarmProbableCause.0 = INTEGER: other(1024)
   TRAPS-COMMON::alarmTime.0 = STRING: 2021-11-30,4:49:51.0,-8:0
   TRAPS-COMMON::alarmSeverity.0 = INTEGER: indeterminate(2)
   TRAPS-COMMON::alarmHasClear.0 = INTEGER: false(2)
   TRAPS-COMMON::alarmKey.0 = STRING: "Addr-Obj:1:ad-gp-1:threat-file.csv"
   TRAPS-COMMON::alarmText.0 = STRING: "Address group file compilation successful: group-name: ad-gp-1,
file-name: threat-file.csv,
   version: 103, vsync-node: vsync-ha-1"
   TRAPS-COMMON::tenantName.0 = STRING: "o1"
```

The following example output shows an address group file compilation message when data structure creation from file entries fails:

```
SNMPv2-MIB::sysUpTime.0 = Timeticks: (60893) 0:10:08.93
```

```
SNMPv2-MIB::snmpTrapOID.0 = OID:
POLICY-TRAP::addressGroupFileCompilationFailure
   TRAPS-COMMON::alarmType.0 = STRING: addressGroupFileCompilationFailure
   TRAPS-COMMON::alarmDevice.0 = STRING: policy
   TRAPS-COMMON::alarmSpecificProblem.0 = ""
   TRAPS-COMMON::alarmClass.0 = INTEGER: new(0)
   TRAPS-COMMON::alarmProbableCause.0 = INTEGER: other(1024)
   TRAPS-COMMON::alarmTime.0 = STRING: 2021-11-30,5:7:56.0,-8:0
   TRAPS-COMMON::alarmSeverity.0 = INTEGER: major(5)
   TRAPS-COMMON::alarmHasClear.0 = INTEGER: false(2)
   TRAPS-COMMON::alarmText.0 = STRING: "Address group file compilation failure: group-name: ad-gp-1, file-
name: threat-file.csv,
   version: 105, vsync-node: vsync-ha-2, msg: "
   TRAPS-COMMON::tenantName.0 = STRING: "o1"
   TRAPS-COMMON::alarmObject.0 = STRING: "addressGroupFileCompilationFailure"
   TRAPS-COMMON::alarmEventType.0 = INTEGER: equipmentAlarm(5)
   TRAPS-COMMON::alarmKey.0 = STRING: "Addr-Obj:1:ad-gp-1:threat-file.csv"
```

The following example output shows the VSync file download success message when a full update is downloaded, here for version 100, which has an incremental version of 0.

```
SNMPv2-MIB::sysUpTime.0 = Timeticks: (123847) 0:20:38.47
SNMPv2-MIB::snmpTrapOID.0 = OID:
VSYNC-TRAP::vsyncFileDownloadSuccess
   TRAPS-COMMON::alarmType.0 = STRING: vsyncFileDownloadSuccess
   TRAPS-COMMON::alarmDevice.0 = STRING: vsync
   TRAPS-COMMON::alarmObject.0 = STRING: "vsyncFileDownloadSuccess"
   TRAPS-COMMON::alarmSpecificProblem.0 = ""
   TRAPS-COMMON::alarmClass.0 = INTEGER: new(0)
   TRAPS-COMMON::alarmEventType.0 = INTEGER: equipmentAlarm(5)
   TRAPS-COMMON::alarmProbableCause.0 = INTEGER: other(1024)
   TRAPS-COMMON::alarmTime.0 = STRING: 2021-11-25,4:53:49.0,-8:0
   TRAPS-COMMON::alarmSeverity.0 = INTEGER: indeterminate(2)
   TRAPS-COMMON::alarmHasClear.0 = INTEGER: false(2)
   TRAPS-COMMON::alarmText.0 = STRING: "Vsync file downloaded successfully: file-type: IP-address, file-
name: threat- file.csv, incremental-on-version: 0, new-version: 100, vsync-node: vsync-ha-2"
   TRAPS-COMMON::tenantName.0 = STRING: "o1"
   TRAPS-COMMON::alarmKey.0 = STRING: "Vsync:1:IP-address:threat-file.csv"
```

The following example output shows the VSync file download success message when an incremental patch between two full versions, here for versions 100 and 101. The value of incremental on version is 100.

```
SNMPv2-MIB::sysUpTime.0 = Timeticks: (142294) 0:23:42.94
SNMPv2-MIB::snmpTrapOID.0 = OID:
VSYNC-TRAP::vsyncFileDownloadSuccess
   TRAPS-COMMON::alarmType.0 = STRING: vsyncFileDownloadSuccess
   TRAPS-COMMON::alarmDevice.0 = STRING: vsync
   TRAPS-COMMON::alarmObject.0 = STRING: "vsyncFileDownloadSuccess"
   TRAPS-COMMON::alarmSpecificProblem.0 = ""
   TRAPS-COMMON::alarmClass.0 = INTEGER: new(0)
   TRAPS-COMMON::alarmEventType.0 = INTEGER: equipmentAlarm(5)
   TRAPS-COMMON::alarmProbableCause.0 = INTEGER: other(1024)
   TRAPS-COMMON::alarmTime.0 = STRING: 2021-11-25,4:56:53.0,-8:0
```

```
    TRAPS-COMMON::alarmSeverity.0 = INTEGER: indeterminate(2)
    TRAPS-COMMON::alarmHasClear.0 = INTEGER: false(2)
    TRAPS-COMMON::alarmText.0 = STRING: "Vsync file downloaded successfully: file-type: IP-address, file-
name: threat-file.csv, incremental-on-version: 100, new-version: 101, vsync-node: vsync-ha-2"
    TRAPS-COMMON::tenantName.0 = STRING: "o1" TRAPS-COMMON::alarmKey.0 = STRING: "Vsync:1:IP-
address:threat-file.csv"
```

The following example output shows the VSync file download failure message for a full update, here for version is 108, which has an incremental version value of 0.

```
SNMPv2-MIB::sysUpTime.0 = Timeticks: (174154) 0:29:01.54
SNMPv2-MIB::snmpTrapOID.0 = OID:
VSYNC-TRAP::vsyncFileDownloadFailure
    TRAPS-COMMON::alarmType.0 = STRING: vsyncFileDownloadFailure
    TRAPS-COMMON::alarmDevice.0 = STRING: vsync
    TRAPS-COMMON::alarmObject.0 = STRING: "vsyncFileDownloadFailure"
    TRAPS-COMMON::alarmSpecificProblem.0 = ""
    TRAPS-COMMON::alarmClass.0 = INTEGER: new(0)
    TRAPS-COMMON::alarmEventType.0 = INTEGER: equipmentAlarm(5)
    TRAPS-COMMON::alarmProbableCause.0 = INTEGER: other(1024)
    TRAPS-COMMON::alarmTime.0 = STRING: 2021-11-25,5:2:12.0,-8:0
    TRAPS-COMMON::alarmSeverity.0 = INTEGER: warning(4)
    TRAPS-COMMON::alarmHasClear.0 = INTEGER: false(2)
    TRAPS-COMMON::alarmText.0 = STRING: "Vsync file downloading failure: file-type: IP-address, file-name:
threat-file.csv, incremental-on-version: 0, new-version: 108, vsync-node: vsync-ha-2, msg:
    404 File Not Found" TRAPS-COMMON::tenantName.0 = STRING: "o1"
    TRAPS-COMMON::alarmKey.0 = STRING: "Vsync:1:IP-address:threat-file.csv"
```

The following example output shows the VSync file download failure message when an incremental patch between two full versions is downloaded, here for versions 105 and 107. The value of incremental on the version is 105.

```
SNMPv2-MIB::sysUpTime.0 = Timeticks: (196727) 0:32:47.27
SNMPv2-MIB::snmpTrapOID.0 = OID:
VSYNC-TRAP::vsyncFileDownloadFailure
    TRAPS-COMMON::alarmType.0 = STRING: vsyncFileDownloadFailure
    TRAPS-COMMON::alarmDevice.0 = STRING: vsync
    TRAPS-COMMON::alarmObject.0 = STRING: "vsyncFileDownloadFailure"
    TRAPS-COMMON::alarmSpecificProblem.0 = ""
    TRAPS-COMMON::alarmClass.0 = INTEGER: new(0)
    TRAPS-COMMON::alarmEventType.0 = INTEGER: equipmentAlarm(5)
    TRAPS-COMMON::alarmProbableCause.0 = INTEGER: other(1024)
    TRAPS-COMMON::alarmTime.0 = STRING: 2021-11-25,5:5:58.0,-8:0
    TRAPS-COMMON::alarmSeverity.0 = INTEGER: warning(4)
    TRAPS-COMMON::alarmHasClear.0 = INTEGER: false(2)
    TRAPS-COMMON::alarmText.0 = STRING: "Vsync file downloading failure: file-type: IP-address, file-name:
threat-file.csv, incremental-on-version: 105, new-version: 107, vsync-node: vsync-ha-2,
    msg: 404 File Not Found" TRAPS-COMMON::tenantName.0 = STRING: "o1"
    TRAPS-COMMON::alarmKey.0 = STRING: "Vsync:1:IP-address:threat-file.csv"
```

The following example output shows the VSync file downloaded message when an incremental patch between versions, here versions 100 to 103, is invalid and so the full version 103 cannot be created.

```
SNMPv2-MIB::sysUpTime.0 = Timeticks: (301786) 0:50:17.86
SNMPv2-MIB::snmpTrapOID.0 = OID:
VSYNC-TRAP::vsyncInvalidIncrementalPatch
    TRAPS-COMMON::alarmType.0 = STRING: vsyncInvalidIncrementalPatch
    TRAPS-COMMON::alarmDevice.0 = STRING: vsync
    TRAPS-COMMON::alarmObject.0 = STRING: "vsyncInvalidIncrementalPatch"
    TRAPS-COMMON::alarmSpecificProblem.0 = ""
    TRAPS-COMMON::alarmClass.0 = INTEGER: new(0)
    TRAPS-COMMON::alarmEventType.0 = INTEGER: equipmentAlarm(5)
    TRAPS-COMMON::alarmProbableCause.0 = INTEGER: other(1024)
    TRAPS-COMMON::alarmTime.0 = STRING: 2021-11-25,5:23:28.0,-8:0
    TRAPS-COMMON::alarmSeverity.0 = INTEGER: major(5)
    TRAPS-COMMON::alarmHasClear.0 = INTEGER: false(2)
    TRAPS-COMMON::alarmText.0 = STRING: "Vsync failed to apply incremental patch: file-type: IP-address,
file-name: threat-file.csv, incremental-on-
    version: 100, new-version: 103, vsync-node: vsync-ha-3"
    TRAPS-COMMON::tenantName.0 = STRING: "o1" TRAPS-COMMON::alarmKey.0 = STRING:"Vsync:1:IP-
address:threat-file.csv"
```

The following example output shows an empty file received from the server. This SNMP trap applies only for IP address and URL files.

```
SNMPv2-MIB::sysUpTime.0 = Timeticks: (5011307) 13:55:13.07
SNMPv2-MIB::snmpTrapOID.0 = OID:
VSYNC-TRAP::vsyncFileValidationFailure
    TRAPS-COMMON::alarmType.0 = STRING: vsyncFileValidationFailure
    TRAPS-COMMON::alarmDevice.0 = STRING: vsync
    TRAPS-COMMON::alarmObject.0 = STRING: "vsyncFileValidationFailure"
    TRAPS-COMMON::alarmSpecificProblem.0 = ""
    TRAPS-COMMON::alarmClass.0 = INTEGER: new(0)
    TRAPS-COMMON::alarmEventType.0 = INTEGER: equipmentAlarm(5)
    TRAPS-COMMON::alarmProbableCause.0 = INTEGER: other(1024)
    TRAPS-COMMON::alarmTime.0 = STRING: 2021-11-25,18:28:24.0,-8:0
    TRAPS-COMMON::alarmSeverity.0 = INTEGER: major(5)
    TRAPS-COMMON::alarmHasClear.0 = INTEGER: false(2)
    TRAPS-COMMON::alarmText.0 = STRING: "Vsync file validation failed: file-type: IP-address, file-name:
threat-file.csv, version: 106, vsync-node:
    vsync-ha-3, msg: Empty file"
    TRAPS-COMMON::tenantName.0 = STRING: "o1"
    TRAPS-COMMON::alarmKey.0 = STRING: "Vsync:1:IP-address:threat-file.csv"
```

The following example output shows an invalid file or a file parsing error. This SNMP trap applies only for IP address files.

```
SNMPv2-MIB::sysUpTime.0 = Timeticks: (27668) 0:04:36.68
SNMPv2-MIB::snmpTrapOID.0 = OID:
VSYNC-TRAP::vsyncFileValidationFailure
    TRAPS-COMMON::alarmType.0 = STRING: vsyncFileValidationFailure
    TRAPS-COMMON::alarmDevice.0 = STRING: vsync TRAPS-COMMON::alarmObject.0 = STRING:
"vsyncFileValidationFailure"
    TRAPS-COMMON::alarmSpecificProblem.0 = ""
    TRAPS-COMMON::alarmClass.0 = INTEGER: new(0)
    TRAPS-COMMON::alarmEventType.0 = INTEGER: equipmentAlarm(5)
```

```
    TRAPS-COMMON::alarmProbableCause.0 = INTEGER: other(1024)
    TRAPS-COMMON::alarmTime.0 = STRING: 2021-11-25,19:7:39.0,-8:0
    TRAPS-COMMON::alarmSeverity.0 = INTEGER: major(5)
    TRAPS-COMMON::alarmHasClear.0 = INTEGER: false(2)
    TRAPS-COMMON::alarmText.0 = STRING: "Vsync file validation failed: file-type: IP-address, file-name:
threat-file.csv, version: 105, vsync-node:
    vsync-ha-1, msg: failed to parse file: '/opt/versa/var/vsync/o1/vsync-ha-1/IP-address/threat-file.csv/105/full/
threat-file.csv', line-number: '7'"
    TRAPS-COMMON::tenantName.0 = STRING: "o1"
    TRAPS-COMMON::alarmKey.0 = STRING: "Vsync:1:IP-address:threat-file.csv"
```

The following example output shows the VSync node reachability trap when the VSync node HA fails.

```
SNMPv2-MIB::sysUpTime.0 = Timeticks: (357321) 0:59:33.21
SNMPv2-MIB::snmpTrapOID.0 = OID:
VSYNC-TRAP::vsyncNodeHaFailover
    TRAPS-COMMON::alarmType.0 = STRING: vsyncNodeHaFailover
    TRAPS-COMMON::alarmDevice.0 = STRING: oam
    TRAPS-COMMON::alarmObject.0   = STRING: "vsyncNodeHaFailover"
    TRAPS-COMMON::alarmSpecificProblem.0 = ""
    TRAPS-COMMON::alarmClass.0 = INTEGER: new(0)
    TRAPS-COMMON::alarmEventType.0 = INTEGER: equipmentAlarm(5)
    TRAPS-COMMON::alarmProbableCause.0 = INTEGER: other(1024)
    TRAPS-COMMON::alarmTime.0 = STRING: 2021-12-15,4:2:14.0,-8:0
    TRAPS-COMMON::alarmSeverity.0 = INTEGER: critical(6)
    TRAPS-COMMON::alarmHasClear.0 = INTEGER: false(2)
    TRAPS-COMMON::alarmText.0 = STRING: "Vsync node HA failover: Vsync node vsync-ha-1/10.192.108.81
is not reachable, so node vsync-ha-3/10.192.108.82 became master"
    TRAPS-COMMON::alarmKey.0 = STRING: "VSN-0"
    TRAPS-COMMON::tenantName.0 = STRING: "N/A"
```

The following example ouput shows the VSync node reachability trap when the VSync nodes are unreachable.

```
SNMPv2-MIB::sysUpTime.0 = Timeticks: (369521) 1:01:35.21
SNMPv2-MIB::snmpTrapOID.0 = OID:
VSYNC-TRAP::vsyncNodesUnreachable
    TRAPS-COMMON::alarmType.0 = STRING: vsyncNodesUnreachable
    TRAPS-COMMON::alarmDevice.0 = STRING: oam
    TRAPS-COMMON::alarmObject.0 = STRING: "vsyncNodesUnreachable"
    TRAPS-COMMON::alarmSpecificProblem.0 = ""
    TRAPS-COMMON::alarmClass.0 = INTEGER: new(0)
    TRAPS-COMMON::alarmEventType.0 = INTEGER: equipmentAlarm(5)  TRAPS-
COMMON::alarmProbableCause.0 = INTEGER: other(1024)
    TRAPS-COMMON::alarmTime.0 = STRING: 2021-12-15,4:4:16.0,-8:0
    TRAPS-COMMON::alarmSeverity.0 = INTEGER: critical(6)
    TRAPS-COMMON::alarmHasClear.0 = INTEGER: false(2)
    TRAPS-COMMON::alarmText.0 = STRING: "Vsync nodes unreachable: vsync-ha-3/10.192.108.82, vsync-
ha-1/10.192.108.81"
    TRAPS-COMMON::alarmKey.0 = STRING: "VSN-0"
    TRAPS-COMMON::tenantName.0 = STRING: "N/A"
```

The following example output shows the URLF VSync update success message.

```
2021-12-20 03:37:09 10.48.30.204(via UDP: [10.48.30.204]:161->[10.48.30.218]:5000) TRAP, SNMP v1,
community public
iso.3.6.1.4.1.42359.2.2.2.2.16.2 Enterprise Specific Trap (2) Uptime: 3:34:17.39
iso.3.6.1.4.1.42359.2.2.2.3.1.2.0 = STRING: "urlfVsyncUpdateSuccess"
iso.3.6.1.4.1.42359.2.2.2.3.1.3.0 = STRING: "urlf"
iso.3.6.1.4.1.42359.2.2.2.3.1.4.0 = STRING: "urlfVsyncUpdateSuccess"
iso.3.6.1.4.1.42359.2.2.2.3.1.6.0 = ""
iso.3.6.1.4.1.42359.2.2.2.3.1.7.0 = INTEGER: 0
iso.3.6.1.4.1.42359.2.2.2.3.1.8.0 = INTEGER: 5
iso.3.6.1.4.1.42359.2.2.2.3.1.9.0 = INTEGER: 163
iso.3.6.1.4.1.42359.2.2.2.3.1.11.0 = Hex-STRING: 07 E5 0C 14 03 23 3B 00 2D 08 00
iso.3.6.1.4.1.42359.2.2.2.3.1.12.0 = INTEGER: 3
iso.3.6.1.4.1.42359.2.2.2.3.1.13.0 = INTEGER: 1
iso.3.6.1.4.1.42359.2.2.2.3.1.14.0 = STRING: "URLF module succeeded to process vsync update
   file: versa-url-urldata.csv, version: 1278"
iso.3.6.1.4.1.42359.2.2.2.3.1.15.0 = STRING: "Tenant1"
iso.3.6.1.4.1.42359.2.2.2.3.1.18.0 = STRING: "versa-url-urldata.csv"
iso.3.6.1.4.1.42359.2.2.2.2.16.1.1.0 = INTEGER: 0
```

```
SNMPv2-MIB::sysUpTime.0 = Timeticks: (61444) 0:10:14.44
SNMPv2-MIB::snmpTrapOID.0 = OID:
URLF-TRAP::urlfVsyncUpdateFailure
   TRAPS-COMMON::alarmType.0 = STRING: urlfVsyncUpdateFailure
   TRAPS-COMMON::alarmDevice.0 = STRING: versa-flexvnf
   TRAPS-COMMON::alarmObject.0 = STRING: "urlfVsyncUpdateFailure"
   TRAPS-COMMON::alarmSpecificProblem.0 = ""
   TRAPS-COMMON::alarmClass.0 = INTEGER: new(0)
   TRAPS-COMMON::alarmEventType.0 = INTEGER: equipmentAlarm(5)
   TRAPS-COMMON::alarmProbableCause.0 = INTEGER: softwareError(163)
   TRAPS-COMMON::alarmTime.0 = STRING: 2022-2-23,23:26:35.0,-8:0
   TRAPS-COMMON::alarmSeverity.0 = INTEGER: critical(6)
   TRAPS-COMMON::alarmHasClear.0 = INTEGER: true(1)
   TRAPS-COMMON::alarmText.0 = STRING: "URLF module failed to process vsync update, Reason: file: fail_
pattern.csv, version: 1"
   TRAPS-COMMON::tenantName.0 = STRING: "versa"
   TRAPS-COMMON::alarmKey.0 = STRING: "fail_pattern.csv"
   URLF-TRAP::urlfVSNId.0 = INTEGER: 0
```

View IP Address File Statistics

To display IP address file statistics, issue the following command:

```
admin@tb0-cli> show orgs org-services organization-name objects address-object-file statistics

      NUM          NUM       NUM FILE    NUM GROUP    NUM FILE       NUM FILE
ORG    INVALID       EMPTY     ADDR LIMIT  ADDR LIMIT   COMPILATION    COMPILATION
ID     FILE FORMAT    ADDR FILE  EXCEEDED    EXCEEDED     SUCCESSFUL     FAILURES
-------------------------------------------------------------------------------
5      0             0      0          0          0              0
```

To clear IP address file statistics, issue the following command:

```
admin@tb0-cli> request clear statistics object address-object-file org org-name organization-name

status success
result Cleared statistics
```

To perform an SNMP walk for the IP address file statistics, issue the following command:

```
admin@tb0-:~$ snmpwalk -v2c -c public 10.192.108.14:161
iso.3.6.1.4.1.42359.2.2.1.2.1.4.4
iso.3.6.1.4.1.42359.2.2.1.2.1.4.4.1.2.5 = STRING: "0"
iso.3.6.1.4.1.42359.2.2.1.2.1.4.4.1.3.5 = STRING: "0"
iso.3.6.1.4.1.42359.2.2.1.2.1.4.4.1.4.5 = STRING: "0"
iso.3.6.1.4.1.42359.2.2.1.2.1.4.4.1.5.5 = STRING: "0"
iso.3.6.1.4.1.42359.2.2.1.2.1.4.4.1.6.5 = STRING: "0"
iso.3.6.1.4.1.42359.2.2.1.2.1.4.4.1.7.5 = STRING: "0"
```

Configure an IP Port VSync File

You can create an IP port VSync file, which is a text file, to block a list of destination IP addresses and destination IP port numbers. The VSync node converts the addresses and ports in this file to an internal Versa format, and VOS devices then drop any sessions that match the entries in the file.

In the text file, you enter one IPv4 address/range and port number/range in one of the following formats. Note that the horizontal line is the pipe (|) symbol.

- *ipv4-address*|*port number*. For example,1.1.1.1|80
- *ipv4-address*|. For example, 1.1.1.1|
- ipv4-adress|port range. For example, 1.1.1.1|80-90
- |*port number*. For example, |80
- |*port range*. For example, |80-90
- *ipv4-address range*|*port number*. For example,1.1.1.1-1.1.1.10|80
- *ipv4-address*| range. For example, 1.1.1.1-1.1.1.10|
- ipv4-adress range|port range. For example, 1.1.1.1-1.1.1.10|80-90

Do not include any white space or special characters in the text file. Only trailing spaces are allowed. The text file can have a maximum of 65534 entries. Any additional entries are ignored. The IPv4 address range in a single entry cannot be more than 65536. The number of entries that contain a range cannot be more than 512.

The VOS device stores the valid IP port files in the /opt/versa/var/vsync/*organization-name*/*vsync-node-name*/IP-port directory. If the format of the IP port file is invalid format, or if there is an error response from the server, the IP port file is moved to the /opt/versa/var/vsync-failure/*organization-name*/vsync-ha-1*vsync node name*/IP-port directory for debugging.

To view statistics, issue the following command. You can fetch the same statistics using SNMP walk. The following table explains the fields in the output.

```
admin@branch1-cli> show orgs org-services test-org objects persistent-actions vsync file threat-file.db
                   UPDATE   UPDATE   SESSION
                   SUCCESS  FAILURE  MATCH
 NAME                  CNT      CNT      CNT
-------------------------------------------------------
 threat-file.db          1      1        1
```

Field	Description
Name	Name of the threat file.
Update Success CNT	How many times the IP port VSync file compilation was successful.
Update Failure CNT	How many times the IP port VSync file compilation failed.
Session Match CNT	How many times a session matches an entry in the IP port VSync file.

To clear the statistics, issue the following command:

```
admin@tb0-cli> request clear statistics object persistent-action org org-name organization-name test-org vsync-file-name threat-file.db
```

When the IP port VSync file compilation succeeds or fails, the VOS device sends alarms and SNMP traps. The following is an example of the SNMP traps.

```
IPGUARD-TRAP::ipguardNotification Enterprise Specific Trap (1) Uptime: 0:07:45.86
        TRAPS-COMMON::alarmType.0= STRING: ipguardVsyncUpdateFailure
        TRAPS-COMMON::alarmDevice.0 = STRING: ipguard
        TRAPS-COMMON::alarmobject.0 = STRING: "ipguardVsyncUpdateFailure"
        TRAPS-COMMON::alarmSpecificProblem.0 = ""
        TRAPS-COMMON::alarmClass.0 = INTEGER: new(0)
        TRAPS-COMMON::alarmEventType.0 = INTERGER: equipmentAlaram(5)
        TRAPS-COMMON::alarmProbableCause.0 = INTEGER: softwareError(163)
        TRAPS-COMMON::alarmTime.0 = STRING:2021-11-17,16:4:21.0,-8:0
        TRAPS-Common::alarmSeverity.0 = INTEGER: warning(4) TRAPS-COMMON::alarmHasClear.0 =
INTEGER: true(1)
        TRAPS-COMMON::alarmText.0 = STRING: "Ipguard module failed to process vsync update/opt/versa/var/
vsync/test-org/vsync-node-2/IP-port/threat-
        file.db/100/full/threat-file.db"
        TRAPS-COMMON::tenantName.0 = STRING: "test-org" IPGUARD-TRAP::ipguardVsyncFileName.0 =
STRU+ING: "/opt/versa/var/vsync/test-org/vsync-node-2/IP-port/threat-file.db/100/full/threat-file.db"
        TRAPS-COMMON::alarmKey.0 = STRING: "/opt/versa/var/vsync/test-org/vsync-node-2/IP-port/threat-file.
db/100/full/threat-file.db"
        TRAPS-COMMON::threasholdStatus.0 = INTEGER: set(1)IPGUARD-TRAP::ipguardVSNID.0 = INTEGER:
0
```

```
SNMPv2-MIB::snmpTrapOID.0 = OID: VERSA-MIB::serviceNotification.15.2.2
    TRAPS-COMMON::alarmType.0 = STRING: ipguardVsyncUpdateSuccess
    TRAPS-COMMON::alarmDevice.0 = STRING: abc
    TRAPS-COMMON::alarmObject.0 = STRING: "ipguardVsyncUpdateSuccess"
```

```
    TRAPS-COMMON::alarmSpecificProblem.0 = ""
    TRAPS-COMMON::alarmClass.0 = INTEGER: new(0)
    TRAPS-COMMON::alarmEventType.0 = INTEGER: equipmentAlarm(5)
    TRAPS-COMMON::alarmProbableCause.0 = INTEGER: softwareError(163)
    TRAPS-COMMON::alarmTime.0 = STRING: 2022-2-24,11:4:41.0,+1:0
    TRAPS-COMMON::alarmSeverity.0 = INTEGER: warning(4)
    TRAPS-COMMON::alarmHasClear.0 = INTEGER: true(1)
    TRAPS-COMMON::alarmText.0 = STRING: "Ipguard module succeeded to process vsync update /opt/versa/
var/vsync/Tenant-1/vsync-23465/IP-port/threat-file.db/70/full/threat-file.db"
    TRAPS-COMMON::tenantName.0 = STRING: "Tenant-1"VERSA-MIB::serviceNotification.15.1.2.0 =
STRING: "/opt/versa/var/vsync/Tenant-1/vsync-23465/IP-port/threat-file.db/70/full/threat-file.db"
    TRAPS-COMMON::alarmKey.0 = STRING: "/opt/versa/var/vsync/Tenant-1/vsync-23465/IP-port/threat-file.db/
70/full/threat-file.db"
    TRAPS-COMMON::thresholdStatus.0 = INTEGER: set(1)
    VERSA-MIB::serviceNotification.15.1.1.0 = INTEGER: 0
```

Configure URL Filtering

The VSync URL feed provides updates of a URL file that that contains domains, patterns, and regular expressions (regex) that are associated with a user-defined category. All domains are loaded directly into memory. All patterns and regular expressions are compiled and stored in a hyperscan database.

There are three types of compilation:

- Full regex compilation
- Incremental regex compilation
- Exclude regex compilation

Note that multitenancy is not supported. It is assumed that there is only a single tenant.

The regex URL updates are compiled every time until a threshold (Default value is 1000 and can change upto 1-3000) and are considered as full regex and stored in full hyperscan database. After this threshold reaches, any update is treated as incremental update on top of the existing full regex database. The incremental updates can be addition or deletion of regex URLs. Addition of regex URLs go into incremental regex database and deletion of regex URLs go into exclude regex database. When incremental updates (addition or deletion) happen, only the incremental or exclude database is compiled. The compilation of existing full database does not happen.

The compilation of updates into full regex is done asynchronously when the incremental update of regex URL reaches the threshold. Any number of new update requests from VSync wait in a queue until the full update is completed. These new update requests are compiled as incremental updates on top of the new full update. The new updates are not available in the datapath and any URL lookup can access the older version. The full or incremental update compiled are written to a cache file that can restore the database if the system goes through a reboot or service restart.

A VOS device stores valid URL files in the /opt/versa/var/vsync/*organization-name*/*vsync-node-name*/URL directory. If the format of the URL file is invalid or if the file contains an error response from the server, the URL file is moved to the /opt/versa/var/vsync-failure/*organization-name*/*vsync-node-name*/URL directory.

You can receive an alarm notification in case of the following events:

- VSync URL file validation fails
- Feed compiles successfully
- Feed compilation fails

To check the compilation status, issue the following command:

```
admin@vos-cli> show orgs org-services versa security url-filtering statistics compile

REGEX   REGEX   LOAD  LOAD    LOAD
COMPILE COMPILE INCR  EXCLUDE FULL
SUCCESS FAIL    CACHE CACHE   CACHE
CNT     CNT     CNT   CNT     CNT
----------------------------------------
16      0       2     0       5
```

```
admin@vos-cli> show security url-filtering compile-status

          INCR  EXCLUDE
TNT       REGEX REGEX REGEX   COMPILE
ID  STATUS COUNT COUNT COUNT   TIME     MESSAGE
------------------------------------------------------------------------------
2   Skip   203   0     0       00:00:00 Full hsdb loaded from cache
```

To configure the maximum number of entires per file, issue the following command:

```
admin@vos-cli> request orgs org-services versa url-filtering url-files set-limits max-urls 65000
```

To set SNMP and syslog alarms destinations, issue the following commands:

```
admin@versa-vos-cli> request alarms set alarm-type urlf-vsync-update-success-trap destinations
Possible completions:
      all - Send alarms to all destination types
      none - Disable alarm
      snmp - Send traps to SNMP targets
      syslog - Generate syslog for the alarm
```

```
admin@versa-vos-cli> request alarms set alarm-type urlf-vsync-update-failure-trap destinations [ all ]
status success
result alarm destination changed successfully
```

```
admin@versa-vos-cli> request alarms set alarm-type urlf-vsync-update-success-trap destinations [
syslog ]
status success
result alarm destination changed successfully
```

Set Up a JSON Configuration File

The VSync tool operates by running the VSync process, vsyncd. You define the vsyncd configuration parameters in a

JSON file. By default, the file is /opt/versa/vsync/var/vsyncd-cfg.json. You can find a sample configuration file at /opt/versa/vsync/var/vsyncd-cfg.json.sample. To define the VSync tool parameters for your environment, make a copy of the sample configuration file and change the values as appropriate.

The JSON configuration file consists of three sections:

- General configuration
- Director configuration
- Threat intelligence source configuration

General Configuration Section

In the general configuration section, you specify paths to various files and directories, and timeout values. The following is an example of the JSON configuration in the general section. The following table describes the configuration parameters.

```
{
        "vsync-name"                : "vsync-1",
        "workingdir"                : "/opt/versa/vsync/var",
        "logfile"                   : "/var/log/versa/vsync/versa-vsyncd.log",
        "vsync-ip"                  : "127.0.0.1",
        "download-timeout"          : "300",
        "max-rsync-procs"           : "20",
        "appl-keyfile"              : "/opt/versa/vsync/var/id_rsa_appl",
        "sync-on-start"             : "true",
        "status-check-frequency"    : "300",
        "include-dev-names"         : [ "Branch-A" ],
        "exclude-dev-names"         : [ "Branch-B" ],
        "include-hosts"             : [ "10.1.0.10"],
        "exclude-hosts"             : [ "10.1.0.11"]
        "vsync-retry-request"       : "true",
}
```

Parameter	Description
vsync-name	Unique name of the VSync node.
workingdir	Directory in which to store VSync files.
logfile	Name of VSync log file on the local disk to which to log all vsyncd operations.
vsync-ip	Vsync host IP address.
download-timeout	Time to wait for a file to download before terminating the download operation.

Parameter	Description
	Range: None *Default:* 300 seconds
max-rsync-procs	Maximum number of concurrent rsync copy processes that can run on the VSync node. If you need to configure a value larger than the default value, contact Versa Networks Customer Support for assistance. *Default:* 20
appl-keyfile	Path to the SSH key file used to authenticate connections to VOS devices.
sync-on-start	Set to true to synchronization with the threat intelligence source when VSync services start.
status-check-frequency	Frequency in seconds to wait before checking for a previous download or installation of URL, domain name, IP port or IP address file. *Default*: 300 seconds
include-dev-names	List of VOS branch device names to update with the URL, domain name, IP port or IP address file.
exclude-dev-names	List of VOS branch device names to not update with the URL, domain name, IP port or IP address file.
include-hosts	List of VOS branch IP addresses to update with the URL, domain name, IP port and IP address file.
exclude-hosts	List of VOS branch IP addresses to not update with the URL, domain name, IP port and IP address file.
vsync-retry-request	Enable the VSync server to automatically retry the request for files of same type.

Director Configuration Section

```
"versa-dir-info"          : {
```

```
        "host"            : "10.48.45.195",
         "rest-port"      : "9182",
        "rest-user"       : "Administrator",
        "rest-password"   : "Versa123@",
        "refresh-interval" : "86400"
},
```

Parameter	Description
host	Host name or IP address of the Director node.
rest-port	REST API port on the Director node. *Default:* 9182
rest-user	Username to use for basic authentication of the REST APIs.
rest-password	Password to use for basic authentication of the REST APIs.
refresh-interval	How often to refresh the VOS device or tenant information. *Range:* 2 through 4,000,000 seconds

IP Port Configuration Section

```
{
        "name"          : "vsync-ip-port",
        "src"           : http://spack.versa-networks.com/vsync/threat-feeds/ip-port.txt,
        "format"        : "txt",
        "start-time"    : "00:00:00",
        "frequency"     : "3600",
        "ip-port-file"  : "true",
        "target-objects" : [
                {

                        "tenant"    : "Versa",
                        "address-group" : "pg1"
                }
        ]
}
```

Parameter	Description
name	Name of the IP port source file.

Parameter	Description
src	URL of the resource or REST API.
format	Format of the source IP port file: • txt
start time	Time of day at which to start an update, in the format *hh*:*mm*:*ss*
frequency	How often, in seconds to update the threat intelligence from the source.
Ip-port-file	Set to true if the source presents content as IP port.
target-objects	Name of the tenant and name of the object to update with the threat intelligence source.
tenant	Name of the tenant organization.

IP Address Configuration Section

```
{
        "name"                    : "vsync-ip-address",
         "src"                   : https://spack.versa-networks.com/html/app2.txt,
        "format"                  : "txt",
        "ipaddr-for-empty-file"    : "169.44.1.1/32",
        "empty-file-if-no-xlations": "true",
        "start-time"              : "00:00:00",
        "frequency"               : "3600",
        "target-objects"          : [
                {
                        "tenant" : "Versa",
                         "address-group" : "ag2"
                }
        ]
}
```

Parameter	Description
name	Name of the IP Address source file.
src	URL of the resource or REST API.

Parameter	Description
format	Format of the IP Address source file: • txt
Ipaddr-for-empty-file	Add a dummy entry in IP address files when source file is empty.
empty-file-if-no-xlations	Set to true if the translation results in 0 line then add a dummy entry. *Default:* False
start-time	Time of day at which to start an update, in the format *hh*:*mm*:*ss*.
frequency	How often, in seconds, to update the threat intelligence from source.
target-objects	Name of the tenant and name of the object to update with information from the threat intelligence source.
tenant	Name of the tenant organization.
address-group	Name of an address-group configured for the tenant in VOS device.

URL File Configuration

```
{
        "name"                    : "vsync-url",
        "src"                     : https://spack.versa-networks.com/html/Threat-URL-list.txt,
        "auth-header"               : "XXXXXXXXXXXXXXXXXXXXXX",
        "format"                  : "txt",
        "start-time"              : "00:00:00",
        "frequency"               : "3600",
        "empty-file-if-no-xlations" : "true",
        "url-for-empty-file"        : "abcdefghijklmnopqrstuvwxyz0123456789",
        "url-file"                : "true",
        "url-match-strings"         : "true",
        "url-match-control-file"    : "/opt/versa/vsync/var/match_ctl.txt",
        "url-control-file-mode"     : "match",
        "target-objects" : [
                {
                        "tenant" : "Versa",
                        "url-category" : "uc1"
```

```
            }
        ]
}
```

Parameter	Description
name	Name of the URL source.
src	URL of the resource or REST API
auth-header	Value to use as the authorization header when sending the HTTPS request for the REST API.
format	Format of the source threat intelligence file: • txt
start-time	Time of day at which to start an update, in the format *hh*:*mm*:*ss*.
frequency	How often, in seconds, to update the threat intelligence from the source.
empty-file-if-no-xlations	Set to true if the translations results in 0 line then add a dummy entry.
url-for-empty-file	Add a dummy entry in URL files when source file is empty.
urlfile	Set to true if the source presents content as a URL.
url-match-strings	If set to true, the URLs from the source URL threat feed file match an exact string. If set to false, the URLs from the source URL threat feed file match regex pattern on the device.
url-match-control-file	List of regular expression
target-objects	Name of the tenant and name of the object to update with information from the threat intelligence source.
tenant	Name of the tenant organization.
url-category	Name of a URL category configured for the tenant on the

Parameter	Description
	VOS devices.

Manage and Monitor VSync Tool Operation

When organization maintains threat intelligence databases across multiple web servers, you can use the VSync tool to distribute the threat intelligence information from all the Database to the VOS. The VSync tool automatically detects updates to these databases and distributes the new information to the VOS devices.

You use the VSync tool for the following operations:

- Connects to Director node using REST APIs to fetch device and organization list.
- Converts the data to Versa specified format (csv, sqlite, or DB).
- Generate full updates and the last four incremental updates and copy them to the VSync host server.
- Connect to VOS devices using SSH.
- Execute request commands to notify VOS devices about updates so that the VOS devices can reload the contents of the files. Based on the content of the updated files, VOS devices enforce network and security policies.

The VSync tool maintains version number for each source file. If there are any changes in web server source file, the VSync tool generates full updates and incremental updates of last four versions. If the previous source file and current source file are same, the VSync tool does not send update notications to the VOS devices. The VSync tool supports only one source file of the IP port.

After you install the VSync tool and then log out and log in at least once, you can use the **vsync** command to manage and monitor the operation of the VSync tool. The following table describes the **vsync** command options.

vsync Command	Description
disable	Disable synchronization of threat intelligence database updates to the VOS device. For example: [versa@vsync-host-2: ~] # **vsync disable** VSync updates to appliances is Disabled [versa@vsync-host-2: ~] # **vsync status** VSync updates to appliances is Disabled versa-vsyncd is Running [-] process 7764
enable	Enable synchronization of threat intelligence database updates to the VOS device. For example: [versa@vsync-host-2: ~] # **vsync enable**

vsync Command	Description
	VSync updates to appliances is Enabled [versa@vsync-host-2: ~] # **vsync status** VSync updates to appliances is Enabled versa-vsyncd is Running [-] process 7764
encrypt	Encrypt the Director password. For example: [versa@vsync-host-2: ~] # **vsync encrypt my-password** [versa@vsync-host-2: ~] # **cat /opt/versa/vsync/var/.passwd** gAAAAABiA18I-j_JLsquKwz3752SyZzbjvR0QOYMYxPdSIqUHlhD1DUZckB-SNJ4HXyEY8EWgGNWr1p9RMoO8BiUWy375s3PyA==
gen-cert	Generate an SSL certificate for HTTPS server. For example: [versa@vsync-host-2: ~] # **vsync gen-cert** Declare -r BASHOPTS="cmdhist:complete_fullquote:extquote:force_fignore:hostcomplete:interactive_comments:progcomp:promptvars:sourcepath" declare -ir BASHPID declare -ar BASH_VERSINFO=([0]="4" [1]="4" [2]="19" [3]="1" [4]="release" [5]="x86_64-pc-linux-gnu") declare -ir EUID="1000" declare -ir PPID="19402" declare -r SHELLOPTS="braceexpand:hashall:interactive-comments" declare -ir UID="1000" declare -r key_validity="365" [2022-02-08 22:29:38-08:00]: Started generating certificates... [2022-02-08 22:29:38-08:00]: Server private key and csr created successfully [2022-02-08 22:29:39-08:00]: CA key created successfully [2022-02-08 22:29:39-08:00]: Creating server certificate... [2022-02-08 22:29:39-08:00]: Server certificate created successfully

vsync Command	Description
	[2022-02-08 22:29:39-08:00]: Server certificate bundle created successfully [2022-02-08 22:29:39-08:00]: All certificates and keys are successfully created. [2022-02-08 22:29:39-08:00]: Exiting.. [versa@vsync-host-2: ~] # **sudo service nginx reload**
help gen-cert	Display the available VSync commands. For example: [versa@vsync-host-2: ~] # **vsync help gen-cert** vsync gen-cert Generate vsync server certificate
list file-source summary	Display a list of VOS devices. For example: [versa@vsync-host-2: ~] # **vsync list file-source summary** SOURCE NAME PING STATUS FORMAT TYPE FILE --- vsync-test-ip-addr REACHABLE txt IP-ADDRESS vsync-test-url REACHABLE txt URL vsync-test-domain REACHABLE txt URL vsync-test-azure REACHABLE xml IP-ADDRESS vsync-ip-port REACHABLE txt IP-PORT • Source name—VSync source file source name • Ping status—Check status of web server to fetch threat intelligence database • Format type—Source file format type • File—Source file type
list appliance summary	Display the VOS devices connectivity status from VSync.

vsync Command	Description
	For example: admin@vsync-host-1:~$ **vsync list appliance summary** DEVICE IP PING NAME ADDRESS STATUS --- HA-Pair-1 10.21.64.103 REACHABLE HA-Pair-2 10.21.64.104 REACHABLE • Device name—VOS device name • IP address—IP address of VOS device • Ping status—Check VOS devices are reachable from vsync
refresh	Refresh the list of VOS devices. For example: [versa@vsync-host-2: ~] # **vsync refresh devicelist**
restart	Restart all VSync processes. For example: [versa@vsync-host-2: ~] # **vsync restart** * Restarting versa-vsync...
show file-appliance detail	Display statistics about threat file notifications to the appliances. For example: admin@vsync-host-1:~$ **vsync show appliance detail** IP SOURCE TYPE VERSION NOTIFY TIME ADDRESS NAME REQUEST --- --- 10.21.64.104 vsync-test-ip-addr IP-ADDRESS 28 success 2021-12-23 04:52:31.173742 10.21.64.104 vsync-test-url URL 10 success 2021-12-23 04:52:31.181623

vsync Command	Description
	• IP address—IP address of the VOS device • Source name—Name of the source file • Type—Type of the source file • Version—Version number of source file • Notify request—Satus of vsync notify request to download and Install latest threat intelligence database to VOS devices • Time—Timestamp of latest threat file notify to appliance
show file-source detail	Displays statistics about threat file notifications to the source. For example: [versa@vsync-host-2: ~] # **vsync show file-source detail** SOURCE DOWNLOAD TOTAL TRANSLATED IGNORED NAME STATUS COUNT COUNT COUNT --- vsync-test-url success 80 79 0 vsync-test-url success 78 77 0 vsync-test-ip-addr success 77 77 0 • Source name—Nam of VSync source file • Download Status—Download status of threat intelligence database from the web server • Total count—Number of entries fetched from the source file • Translated count—Number of entries translated to the Versa-specified format • Ignored count—Number of entries that were ignored and not translated
start	Start all VSync processes. For example: [versa@vsync-host-2: ~] # **vsync start** * Starting versa-vsync...

vsync Command	Description
status	Display the status of the VSync service. For example: [versa@vsync-host-2: ~] # **vsync status** VSync updates to appliances is Disabled versa-vsyncd is Running [-] process 19827
stop	Stop all VSync processes. For example: [versa@vsync-host-2: ~] # **vsync stop** * Stopping versa-vsync...
update *branch name*	Create and update threat objects on a particular VOS device. For example: [versa@vsync-host-2: ~] # **vsync update HA-Pair-2**
update all	Create and update threat objects on all VOS devices. For example: [versa@vsync-host-1: ~] # **vsync update all**
version	Display the VSync version. For example: [versa@vsync-host-2: ~] # **vsync version** 2.0.0-39c40e4
whitelist	Enforce allow lists on VSync HTTPS server, to allow only VOS devices to fetch threat files. For example: [versa@vsync-host-2: ~] # **vsync whitelist** [versa@vsync-host-2: ~] # **sudo service nginx reload**

By default, after installation, the sending or updating to VOS devices is disabled, and you must explicitly enable it.

To enable HTTPS fetching from VSync nodes, you must open port 443 on the Controller node for all branches. To create a service object for destination port 443 and append it to an existing policy rule on the Controller node, issue the following commands:

```
admin@branch1-cli(config)% set orgs org-services organization-name objects services service-name protocol TCP
admin@branch1-cli(config)% set orgs org-services organization-name objects services service-name destination-port 443
admin@branch1-cli(config)% set orgs org-services organization-name security access-policies Default-Policy rules rule-name
match services services-list service-name
```

For example:

```
admin@branch1-cli(config)% set orgs org-services versa objects services VSync-HA-Ports protocol TCP
admin@branch1-cli(config)% set orgs org-services versa objects services VSync-HA-Ports destination-port 443
admin@branch1-cli(config)% set orgs org-services versa security access-policies Default-Policy rules Allow-From-CPE-Ports match
services services-list VSync-HA-Ports
```

Supported Software Information

Releases 20.2.4 and later support all content described in this article.

Additional Information

Use the VSync Tool (for VSync Version 1)