Use the VSync Tool

For supported software information, click here.

This article describes how to install, configure, and monitor the VSync tool for Phase 1 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^{TM} (VOS^{TM}) 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.

Overview of the VSync Tool

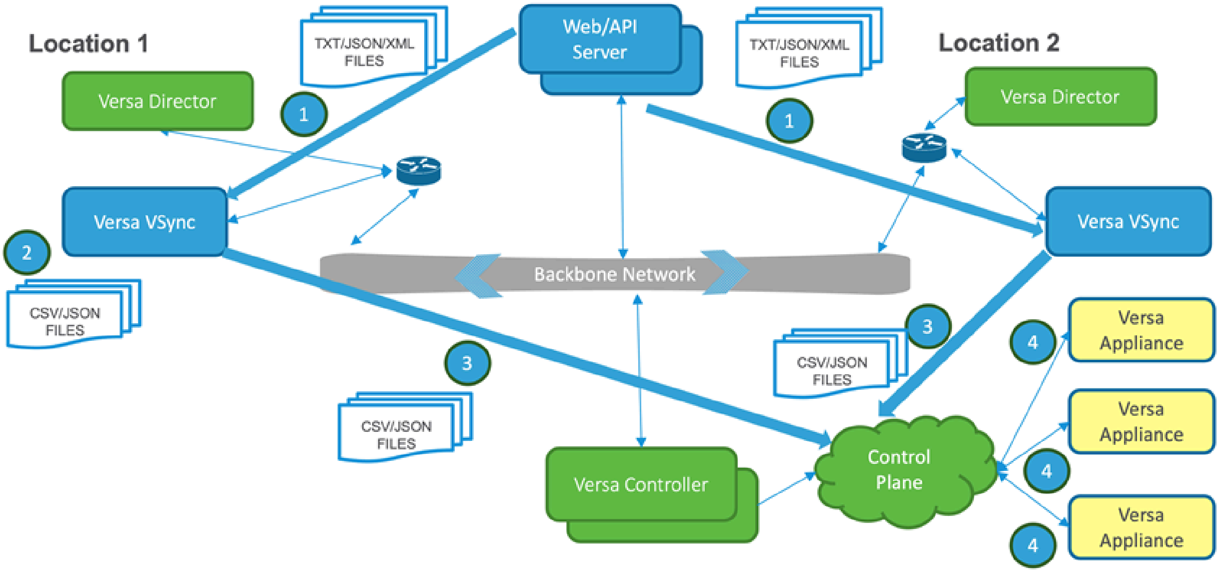
Enterprises commonly maintain their threat intelligence databases, which include IP addresses, IP address or port numbers, and URLs, on web or RESTful API servers, and they can host different threat intelligence databases on different servers. The dynamic threat feeds and sources are typically hosted on a web server in the enterprise network or in the public cloud (for example, Project Honeypot). Each threat intelligence database harvests information from multiple threat feeds, security infrastructures, and other sources, and this threat intelligence information needs to be updated in real-time on the enterprise's security devices, such as firewalls, in order to enforce the enterprise's security policies. The adoption of SD-WAN and SD-Security has led to broader distribution of security and firewall technologies, and the number of devices on which security policies are enforced has grown from a just a few to many thousands, and, in the case of multicloud infrastructure, even more. The VSync tool provides a high-performance, scalable method for distributing enterprise threat intelligence databases to SD-Security VOS devices.

You can configure the VSync tool to receive updates from any number of sources of threat intelligence databases, and you can enforce security policies based on address group objects, custom application objects, and custom URL category objects. The VSync tool automatically detects any updates to the database content from these sources, such as the addition or deletion of IP addresses or URLs. You can configure the VSync tool to periodically retrieve information from the database sources, and the VSync tool then automatically updates the consolidated data to all targeted firewalls and VOS branch devices. The firewall and VOS branch devices load the new content into the address group, application, and custom URL category objects that you have configured, and then they start enforcing network and security policies based on the updated content. The VSync tool connects to the Director node using REST APIs to fetch device and organization list.

Deployment Overview

You can install the VSync tool on any Ubuntu 18.04 server. Although it is possible to run the VSync tool on the Director node itself, it is recommended that you run it on a dedicated Ubuntu 18.04 server, because the VSync tool can place a substantial load on its host, which might affect normal Director operations and performance. This is especially true when the size of the threat intelligence feed is substantial and a large number of branch or firewall devices need to be updated. Also, the timing and consistency of the threat intelligence updates to the firewalls or branch devices is critical for effective policy enforcement. Therefore, it is desirable that normal Director operations have no impact on the delivery of the threat databases to the firewall and branch devices.

When pushing threat intelligence feeds to the firewall and branch devices, the VSync tool bypasses the Director node completely. For this reason, it is recommended that you host the VSync tool on the Director's southbound network so that it has direct connectivity to the Controller node and to the firewall or branch nodes over the IPsec tunnels established between the Controller node and the firewall or branch devices. 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 tool connects to Web/API server to download or receive threat data.
2. The VSync tool converts the data to CSV format.
3. The VSync tool copies the files to the VOS devices.
4. The VSync tool executes request commands so that the VOS devices reload the contents of the files. Based on the content of the updated files, the VOS devices then enforce network and security policies.

System Requirements

You can install the VSync tool on a virtual machine (VM) or a bare-metal server running Ubuntu 18.04. It is recommended that you use a bare-metal server for better performance. The VSync tool server must have at least 2 CPU cores, 4 GB RAM, and a 40-GB hard drive. However, depending on the size and frequency of the threat intelligence updates and the number of VOS devices that need to be updated, you may need to use a server with more computation power, memory, and storage.

The following table describes the system requirements when VOS devices are updated daily with 100 MB.

VSync Server Resources	**100 VOS Devices**	**1000 VOS Devices**	**2000 VOS Devices**
CPU cores	4	8	12
RAM	8 GB	16 GB	32 GB
Disk storage	80 GB	120 GB	160 GB
Network interfaces	2 x 1 Gbps	2 x 1 Gbps	2 x 1 Gbps

Network Connectivity Requirements

It is recommended that you install the VSync tool on a server with at least two 1-Gbps network interfaces. You use one of the interfaces as the northbound interface (typically, eth0) and the second as the southbound interface (typically eth1). You connect the northbound interface of the VSync server to the same network to which the northbound interface of the Director node connects. You connect the southbound interface to the same network to which the southbound interface of the Director node connects.

Communication with Intelligence Sources

The VSync tool downloads threat intelligence files from either a web server or a RESTful API server using the HTTPS protocol. You can configure multiple threat intelligence sources, each of which can be available from a different web server or REST API server. You can configure an optional authorization header to send as part of download requests, and you can configure a different authorization header for each threat intelligence source.

The following design considerations apply to various deployment scenarios:

- If the threat intelligence source files are available on the internet or from public cloud storage, the preferred communication path is using the northbound interface. You must configure the appropriate firewalls or proxies to allow the VSync tool to download the feeds.
- If the threat intelligence source files are available on the internal network, the preferred communication path is using the southbound interface. If you deploy the VSync tool in HA mode, it is recommended that each VSync tool node

be collocated with the Director node at each location of the HA deployment. Both the nodes running the VSync tool must be able to communicate with the threat intelligence source using the southbound interface over the backbone network.

- If you deploy the Director node and VSync tool in a service provider environment, and if the threat intelligence sources are located within the customer environment, the preferred communication path is using the northbound interface to reach the customer network. The customer must configure their firewall to allow the VSync tool to download the threat intelligence files from the sources identified in their network.

Communication with VOS Devices

For the VSync tool to communicate with VOS devices, the preferred path is to use the southbound interface, which connects to the control plane network. Threat intelligence updates are first sent to the Controller nodes, which then send the data to the VOS devices over IPsec tunnels that are already established between the Controller and VOS devices. It is recommended that you use use the Director node as a reference to configure the routing information related to the southbound (control plane) network, to ensure connectivity between the VSync tool and the VOS devices.

HA Considerations

If you deploy the Versa solution in high availability (HA) mode in different locations, it is recommended that you deploy one instance of the VSync tool at each location. At each location, you connect the northbound interface of the VSync tool to the same network to which the northbound interface of the Director node connects, and you connect the southbound interface of VSync tool to the same network to which the southbound interface of the Director node connects. This arrangement ensures that both instances of the VSync tool have access to each other and to the southbound interfaces of the Director node using the southbound interfaces.

International Characters and Encoding of URLs

- When you specify URLs that include international characters encoded as UTF-8, UTF-16, or UTF-32, VOS devices normalize the UTF-8, UTF-16, and UTF-32 strings.
- When URLs contain non-ASCII characters in them, you can encode the URLs using percent-encoding or percent-u-encoding. If you encode the URLs using any standard URL encoding method, the VOS software supports normalization of the URLs to URL byte streams.
- Before HTTP URLs are matched against the URL patterns or strings specified in the domain or URL files, the HTTP URLs are normalized or decoded as applicable.
- The VSync tool supports only percent-encoded URLs in the source URL or domain threat feed files.

Performance and Scaling

The VSync tool has been tested in an SD-WAN topology consisting of 1000 appliances and three threat feed sources. The threat feeds were one IP address file source and two URL file sources, and each file contained 64,000 entries.

Install the VSync Tool

To use the VSync tool, you must install it on two nodes. Each Versa VSync node must have at least two interfaces, one that connects to the northbound network of the Director node and one that connects to the southbound network of the Director node, as illustrated by the figure in the Deployment Overview section, above. Also, both Versa VSync nodes must have access to the web server from which the configurations are to be downloaded. You may need to use a third interface for this purpose.

The VSync tool is available as a self-extracting archive that you install on a server that is running the Ubuntu 18.04 operating system.

To install the VSync tool on each node:

1. Copy the VSync tool software package to the VOS device or other host device using a file transfer utility, such as SCP.
2. Run the self-extracting archive. For example:

   ```
   [admin@vsync-host1] $ ls
   versa-vsync-20210429-190706-258d7eb-1.1.1-B.bin
   [admin@vsync-host1] $ sudo  ./versa-vsync-20210429-190706-258d7eb-1.1.1-B.bin
   [sudo] password for admin:
   Verifying archive integrity...  100%   All good.
   Uncompressing Versa VSync Incremental Binary   100%
   ```

3. If you installed the VSync tool on a VOS device, delete the VOS software package. After you remove the VOS package, the Ethernet ports on the VOS device become available so that you can configure interface IP addresses and other properties using Linux management tools.

   a. Check that the VOS package is present:

      ```
      sudo dpkg -l | grep -i flex
      ```

   b. Delete the VOS package:

      ```
      sudo dpkg -r versa-flexvnf
      ```

4. Configure the interfaces on the VOS device:
   a. Configure IP addresses on the VOS device's northbound and southbound interfaces. The IP address for northbound interface must be in the same subnet as the northbound interface on the Director node, and likewise for the southbound interface.
   b. If necessary, configure other interfaces, such as the management interfaces and the interface to connect to web servers.
   c. Configure routes on the southbound interface to reach the overlay IP address of the CPE devices.
5. Change the default admin user password on the VOS device.
6. Log out of the VOS device, and then log in again.
7. Verify that the software is installed properly. For more information, see Manage and Monitor VSync Tool Operation.

```
[admin@vsync-host1]  $  dpkg  -l | grep vsync
ii   Versa-vsync                1.1.1           amd64     Versa VSync
[admin@vsync-host1]  $ vsync status
VSync updates to appliances is Disabled
versa-vsyncd               is Stopped
[admin@sync-host1]  $
```

8. Verify that the network and routing information for the northbound and southbound interfaces has been configured based on the southbound interface network or routing information on the Director node.
9. Verify network connectivity works between the VSync host and the Director node and between the VSync node and the threat intelligence sources.

Configure the VSync Tool

This section describes how to configure the VSync tool.

Add the VSync Southbound IP Address to the Device Template

To allow the VSync tool to communicate with VOS device's, the southbound IP address of VSync node must be in the VOS device's template. You can add this address to the device template, or you can issue the following command on the VOS device:

```
set devices template template-name config system vnf-manager-ip-addresses vsync-southbound-ip-address
```

If there are multiple redundant VSync nodes, you must add the IP addresses of both VSync nodes as VNF managers.

Copy the SSH Key to the VSync Node

To allow the VSync node to access VOS devices and securely copy files to them without requiring passwords, copy the SSH private key from the Director node to the VSync node. The SSH private key is created by the Director node as part of the zero-touch provisioning (ZTP) process. For example:

```
[admin@vsync-host1]$ scp Administrator@10.100.197.2:/var/versa/vnms/ncs/homes/admin/.ssh/id_dsa
/opt/versa/vsync/var/id_rsa_appl
Administrator@10.100.197.2's password:
id-rsa        100% 1675   1.7mb/s  00.00
[admin@vsync-host1]$ sudo chown versa:versa /opt/versa/vsync/var/id_rsa_appl
[sudo] password for admin:
[admin@vsync-host1]$ sudo chmod 600 /opt/versa/vsync/var/id_rsa_appl
```

Then edit the SSH configuration file, /etc/ssh/ssh_config, using either vi or nano, and add the following line at the end to define the ssh-dsa key type, which is ssh-dss, so that this public key type is available for user authentication:

```
PubkeyAcceptedKeyTypes +ssh-dss
```

By default, the VSync tool also uses the /opt/versa/vsync/var/id_rsa_appl file as the SSH key file used to authenticate VOS devices. If the VOS device SSH key file is in a different location, set the path to that location in the JSON configuration file, as discussed below.

For Releases 20.2.3 and later, Director nodes use the DSA key for SSH access to VOS devices. The SSH key on the Director node is in the /var/versa/vnms/ncs/homes/admin/.ssh/id_dsa file.

Set Up the JSON Configuration File

The VSync tool operates by running a VSync process, called 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

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 table describes the configuration parameters.

```
{
  "vsync-name"            :"vsync-12345"
  "workingdir"            : "/opt/versa/vsync/var",
  "logfile"               : "/var/log/versa/vsync/versa-vsyncd.log",
  "download-timeout"      : "300",
  "max-rsync-procs"       : "20"
  "appl-keyfile"          : "/opt/versa/vsync/var/id-rsa-app1",
  "sync-on-start"         : "true",
  "status-check-frequency" : "300",
  "include-dev-names"     : [ "Branch-A" ],
  "exclude-dev-names"     : [ "Branch-B" ],
```

Parameter	Description
vsync-name	Unique name of the VSync node.
workingdir	Directory in which to store temporary files.
logfile	Name of VSync log file on the local disk to which to log all vsyncd operations. The default file is/var/log/versa/vsync/versa-vsyncd.log. VSync logging uses the Ubuntu log rotation and log retention processes. By default, when a vsyncd log file reaches 20 MB, it is automatically rotated. Log files are rotated seven times

Parameter	Description
	before they are removed. To change the log rotation settings, edit the /etc/logrotate.d/vsync-agg file.
download-timeout	How long to wait for a file to download before terminating the download operation. *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 greater 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 force synchronization with the threat intelligence source when vsyncd starts or restarts regardless of the start time configured on the threat intelligence source, and then start enforcing the configured frequency.
status-check-frequency	Frequency, in seconds, to wait before checking for a previous download or installation of the URL, domain name, or IP address file. *Default*: 300 seconds
include-dev-names	List of VOS branch device names to update with the URL, domain name, or IP address files. To specify multiple names, enter a comma-separated list in JSON format. If you specify this parameter, only the listed branch devices are updated with the URL, domain name, or IP

Parameter	Description
	address files. If you omit this parameter, all branch devices of the tenants specified in the configuration file are updated.
exclude-dev-names	List of VOS branch device names to not update with the URL, domain name, or IP address files. To specify multiple names, enter a comma-separated list in JSON format. If you specify this parameter, only the listed branch devices are excluded from being updated with the URL, domain name, or IP address files. If you omit this parameter, all branch devices of the tenants specified in the configuration file are excluded.

In the Director configuration section, you specify information about the Director node. The following is an example of the JSON configuration in the Director section. The table describes the configuration parameters.

```
"versa-dir-info"   : {
  "host"            : "10.200.1.4",
  "rest-port"        : "9182",
  "rest-user"        : "Administrator",
  "rest-password"    : "Versa@123",
  "refresh-interval" : "86400"
},
```

Parameter	Description
host	Host name or IP address of the Director node.
rest-port	Number of the REST API port on the Director node. The default port is 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.

Parameter	Description
	Range: 2 through 4,000,000 seconds

In the threat intelligence source section, you specify one or more sources. For each source, you set parameters for the start time and frequency of intelligence updates and the intelligence source format. The following is an example of the JSON configuration in the threat intelligence source section. The table describes the configuration parameters.

```
"vsync-entries"      : [
  {
     "name"                      : "versa-test-url",
     "src"                       : "https://spack.versa-networks.com/html/Threat-URL-list.txt",
     "auth-header"               : "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
     "format"                    : "txt",
     "start-time"                : "00.00.00",
     "frequency"                 : "3600",
     "max-entries-per-file"      : "50000",
     "max-files"                 : "5",
     "no-file-cnt-in-fname"      : "true"
     "url-for-empty-file"        :
"abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ",
     "empty-file-if-no-xlations" : "true",
     "urlfile"                   : "true",
     "url-match-strings"         : "true",
     "target-objects"  :  [
       {
         "tenant"               :  "ACME",
         "url-category"         :  "uc1"
       }
     ]
  }
```

Parameter	Description
name	Name of the threat intelligence source.
src	URL of the resource, REST API, STIX, or TAXII.
auth-header	(Optional.) Value to use as the authorization header when sending the HTTPS request for the resource or REST API.
format	Format of the source threat intelligence file: • json • txt

Parameter	Description
	- xml
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.
max-entries-per-file	Maximum number of input lines to process from the source file and place into the output file. If the source file contains more entries, the file is truncated or split into multiple output files, depending on the value of the max-files parameter. If you omit a value for this parameter or set it to –1, no limit is enforced, and all entries are translated into a single output file.
max-files	Maximum number of output files to generate from the source file. If the source file contains more entries than fit into the maximum number of files, all excess entries are ignored or truncated. If you omit a value for this parameter or set it to –1, no limit is enforced and the entries are placed into as many output files as required. When there is one output file, the filename suffix is 1.csv. To omit the .1 from the suffix and have the suffix be just .csv, set the no-file-cnt-in-fname parameter to true. When there are multiple output files, the filename suffixes are .1.csv, .2.csv, and so on.
no-file-cnt-in-fname	If you set the max-files parameter to 1 and the no-file-cnt-in-fname parameter to true, the output filename does not include a number (that is, the filename suffix is .csv instead of .1.csv or .2.csv) and the file is not included in the maximum file count.
url-for-empty-file	Add a dummy entry in URL files when source file is empty. In the configuration file, you can specify either url-for-empty-file or ipaddr-for-empty-file, but not both.
ipaddr-for-empty-file	Add a dummy entry in IP address files when source file is empty. In the configuration file, you can specify either

Parameter	Description
	url-for-empty-file or ipaddr-for-empty-file, but not both.
empty-file-if-no-xlations	Set to true if the translation results in 0 line then add a dummy entry. Use this option when a file contains blanks or new lines, or is corrupted and results in no valid entry. The default value is false, which adds a dummy entry to empty source files whose size is 0 byte. *Default:* False
urlfile	(Optional.) Set to true if the source presents content as a URL. Set to false if the source presents content as IP address data. *Default:* False
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.
target-objects	Name of the tenant and name of the object to update with information from the threat intelligence source. The object name can be an address group, an application, or a URL category. The values of these fields must match the tenant and object names configured on the VOS devices.
tenant	Name of the tenant organization. The tenant name must match a name configured on the VOS device.
url-category	Name of a URL category configured for the tenant on the VOS device. The name must match a name configured on the VOS device.

Associate Objects with Files

As the final step in configuring the VSync tool, in the device template you associate address group objects, custom application objects, and custom URL category objects with files. Currently, you must perform this configuration from the CLI on the Director node. You cannot configure it from the Director GUI. This section provides examples of associating objects with files.

The following example associates an address group object and address file with the tenant ACME-Tenant in the template named ACME. Note that you enter the **set** command on a single line. The example here shows it as two lines for readability.

```
Administrator@Director> configure
Entering configuration private mode
Administrator@Director% set devices template ACME config orgs org-services ACME-Tenant objects
address-groups group Azure-Addresses address-files [ azure-ipdata.csv ]
Administrator@Director% commit
```

The following example associates a URL filter object and an address file with the same tenant and template. Again, you enter the **set** command on a single line. The example here shows it as two lines for readability.

```
Administrator@Director% set devices template ACME config orgs org-services ACME-Tenant
url-filtering user-defined-url-categories url-category Test-URLs url-file versa-test-urldata.csv
Administrator@Director% commit
```

Modify Limits for IP Addresses, Domain Names, and URL File Entries

By default, a VOS device cannot load an IP address file, a URL files, or a domain file if the file contains more than 64,000 entries. To adjust the maximum number of file entries, you run the vsync_cfg_appl.py script on the VSync host. This script has the following parameters:

The following usage information indicates the required parameters, in addition to the default configuration available in vsyncd configuration file.

```
admin@Director02:/home/admin$ cd /opt/versa/vsync/python/vsyncd
admin@Director02:/opt/versa/vsync/python/vsyncd$ ./vsync_cfg_appl.py -h
Usage: vsync_cfg_appl.py [options]

Options:
-h, --help            show this help message and exit
-c cfilepath, --cfgfile=cfilepath
                      Path to config file in json format
-t tenant, --tenant=tenant
                      Tenant name
-k keyfile, --keyfile=keyfile
                      SSH keyfile for appliances
-l logfile, --logfile=logfile
                      Log file to write logs to
-f ipflimit, --ip-file-limit=ipflimit
                      Limit for max IP Address per file
-g ipgrouplimit, --ip-group-limit=ipgrouplimit
                      Limit for max IP Address per Group
-u urlflimit, --url-file-limit=urlflimit
```

```
                    Limit for max URL entries  per file
```

The following command shows an example of running the vsync_cfg_appl.py script. Note that you enter the command on a single line. The example here shows it as multiple lines for readability.

```
admin@Director02:/opt/versa/vsync/python/vsyncd$ ./vsync_cfg_appl.py
-c /opt/versa/vsync/var/vsyncd-cfg-test.json
-t VersaProvider -k /opt/versa/vsync/var/id_rsa_appl2 -l /var/tmp/vcfg.log -f 32768
```

This example command includes the following options:

- **–c** option—Specifies the configuration in the /opt/versa/vsync/var/vsyncd-cfg-test.json file, from which to obtain information about all affected VOS devices and VOS device connectivity.
- **–t** option—Specifies the tenant, VersaProvider, whose VOS devices to update.
- **–k** option—Specifies the keyfile, /opt/versa/vsync/var/id_rsa_appl2, to use to authenticate with the VOS devices.
- **–l** option—Writes logs to the /var/tmp/vcfg.log file.
- **–f 32768** option—-Configures a maximum number of 32,768 entries in the IP address file (equivalent to the max-entries-per-file value in the JSON configuration file).

Manage and Monitor VSync Tool Operation

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 are the **vsync** command options:

vsync Command Option	Description
disable	Disable synchronization of threat intelligence database updates to the VOS device.
enable	Enable synchronization of threat intelligence database updates to the VOS device.
restart	Restart all versa-vsync processes.
start	Start all versa-vsync processes.
status	Display the status of the versa-vsync service.
stop	Stop all versa-vsync processes.

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

In an HA deployment, you can manually enable the updates to VOS devices on only one of the VSync nodes and disable the updates on the other VSync nodes.

Error Logs

The following table describes the error log messages generated by the VSync tool.

Error Message	Cause	Action To Take
Another download in progress; will check again in seconds	Cannot download the latest version of the IP/URL/domain/IP port file because the previous file download is still in progress.	Check the network connectivity and the size of the file being downloaded, and adjust the frequency of the updates if necessary.
Download failed: HTTP status code	Download of the IP/URL/domain/IP port file failed from the API/web server.	Check the network connectivity from the VSync host to the API/web server. Ensure that the API/web server is up and is running with valid authentication credentials.
Download failed	Download IP/URL/domain/IP port file failed from the API/web server.	Check the network connectivity from the VSync host to the API/web server. Ensure that the API/web server is up and is running with valid authentication credentials.
Download timeout exceeded	Download of the IP/URL/domain/IP port file from the API/web server timed out.	Check the network connectivity from the VSync host to the API/web server. Ensure that the API/web server is up and is running with valid authentication credentials.
Did not receive expected response code	REST API call to Director node or API/web server failed.	Check connectivity and REST API authentication credentials to Director node and API/web server.
Exception at REST API CALL	REST API call to Director node to fetch tenant list and parse the response failed.	Check connectivity and REST API authentication credentials to Director node.
Failed to GET progress for task	REST API to Director node to fetch tenant list and parse the response failed.	Check connectivity and REST API authentication credentials to Director node.

Error Message	Cause	Action To Take
Installer did not start; attempting again	Unable to start translation and installation of source file after download.	Check the system load and limits, and the permissions of the VSync process to launch new processes.
Install failed	Processing of the threat intelligence file failed because of an I/O error.	Ensure that there is sufficient disk space, and check thee ownership and permissions of the /opt/versa/vsync/var directory.
Install failed	Processing of threat intelligence file failed because of a translation error	Check the translation errors in the translation log file in the /opt/versa/vsync/var/*threat-source* directory.
No active download in progress	An attempt to cancel a download process failed because the download process already completed.	You can ignore this message.
Rsync to returned output	Copying a file from the VSync host to a device failed.	Check the error message in the rsync output and take appropriate action.
Rync to returned error	Copying a file from the VSync host to a device failed.	Check the error message in the rsync output and take appropriate action.
Unable to determine device list for the tenant list	REST API call to Director node to fetch tenant list and parse the response failed.	Check connectivity and REST API authentication credentials to Director node.
Unable to determine IP address list for the tenant list	REST API call to Director node to fetch tenant list and parse the response failed.	Check connectivity and REST API authentication credentials to Director node.
Unable to parse response for API	REST API call to Director node to fetch tenant list and parse the response failed.	Check connectivity and REST API authentication credentials to Director node.
URL parse error on line	The URL on the indicated line is not a well-formed URL.	Follow up with the provider of the URL threat feed file.

Error Message	Cause	Action To Take
URL translation error on line	The URL on the indicated line cannot be translated into the VOS format.	Follow up with Versa Networks Technical Support.
Unable to rename	I/O errors occurred when downloading and saving IP/URL/domain/IP port files.	Ensure that there is sufficient disk space, and check the ownership and permissions of the /opt/versa/vsync/var directory.
Unable to remove old error from snapshot file	I/O errors occurred when downloading and saving IP/URL/domain/IP port files.	Ensure that there is sufficient disk space, and check the ownership and permissions of the /opt/versa/vsync/var directory.
Unable to remove old snapshot file	I/O errors occurred when downloading and saving IP/URL/domain/IP port files.	Ensure that there is sufficient disk space, and check the ownership and permissions of the /opt/versa/vsync/var directory.
Unable to spawn installer	Unable to start translation and installation of source file after download.	Check the system load and limits, and permissions of the VSync process to launch new processes.
Unable to open config json file	Vsyncd process could not open the configuration file.	Check the ownership and permissions of the /opt/versa/vsync/var directory.
Unable to create working directory	Vsyncd process could not create a working directory to save temporary files.	Check the ownership and permissions of the /opt/versa/vsync/var directory.
Unable to create logger with logpath	Vsyncd process could not create the log file.	Check the ownership and permissions of the /opt/versa/vsync/var directory.
Unable to get download timeout from config	Vsyncd process could not parse the configuration file	Check the configuration file syntax, and retry.

Error Message	Cause	Action To Take
Unable to connect/authenticate with Versa Director	REST API call to Director node to fetch tenant list and parse the response failed.	Check connectivity and REST API authentication credentials to Director node.
Unable to set permissions for appliance SSH key file	I/O errors logged when saving files to the working directory.	Ensure that there is sufficient disk space, and check the ownership and permissions of the /opt/versa/vsync/var directory.
Unable to read and process regexes from URL control file	Vsyncd process could not parse the URL control file.	Check the URL control file syntax, and retry.
Unable to process vsync entry skipping this entry	Vsyncd process could not parse the configuration file.	Check the configuration file syntax, and retry.
Unable to process vsync entry/entries	Vsyncd process could not parse the configuration file.	Check the configuration file syntax, and retry.

Information Logs

The following table describes the informational log messages generated by the VSync tool.

Messages	Description
After include/exclude hosts list, no hosts to update; skipping config update	Vsyncd skipped installation of the file because no hosts to be updated were specified.
Auto install configured, installing	Vsyncd is about to install an IP/URL/domain/IP port file.
Auto install not requested, skipping installation	Vsyncd skipped the installation of the downloaded file.
Converting txt file to Versa CSV format file	Vsyncd started converting the downloaded file to VOS CSV format.

Messages	Description
Converting urls from offset to Versa CSV format file	Vsyncd started converting the downloaded file to VOS CSV format.
Converting json file	Vsyncd started converting the downloaded file to VOS JSON format.
Converting xml file to Versa CSV format file	Vsyncd started converting the downloaded file to VOS CSV format.
Converting IP src txt file to Versa CSV format file	Vsyncd started converting the downloaded file to VOS CSV format.
Converting ipaddrs from offset to Versa CSV format file	Vsyncd started converting the downloaded file to VOS CSV format.
Cleaning up older snapshots	Vsyncd is cleaning up older snapshots of the downloaded file.
Device is not reachable, ignoring it	Device is not reachable, and it is not updated with IP/URL/domain/IP port files. Vsyncd checks reachability again at the next device refresh interval.
Device is reachable at IP address	Vsyncd can connect to the device, so it can update the IP/URL/domain/IP port files on the device.
Device has tenants	List of tenants provisioned on the device.
Done setting permissions for *device*	Vsyncd successfully set the permissions of the copied files on the device.
Done converting urls	Vsyncd successfully converted the downloaded file to VOS format.

Messages	Description
Downloading url to file	Vsyncd is about to download a IP/URL/domain/IP port file.
Download successful	Vsyncd downloaded the IP/URL/domain/IP port file successfully.
Done copying files using rsync to appliances	Vsyncd successfully copied the file to devices.
Downloader finished successfully	Vsyncd successfully downloaded the IP/URL/domain/IP port file.
Done converting ipaddrs	Vsyncd successfully converted the downloaded file to VOS format.
Extracting URL from element attribute	Vsyncd is trying to extract the URL from the webpage that has the IP/URL/domain/IP port files.
Extract URL found URL	Vsyncd is trying to extract the URL from the webpage that has the IP/URL/domain/IP port files.
Extracting URL failed to match URL pattern	Vsyncd is unable to find the URL of IP/URL/domain/IP port file on the referenced website.
Extracting URL from xml	Vsyncd is trying to extract the URL from the webpage that has the IP/URL/domain/IP port files.
Extracting URL from path	Vsyncd is trying to extract the URL from the webpage that has the IP/URL/domain/IP port files.
Extracted URL	Vsyncd found the URL of IP/URL/domain/IP port file on the referenced website.
Fab cmd	Python fabric command has been executed to set permissions on devices.
Fab cmd result: *status*	Status of setting permissions of copied files on devices.

Messages	Description
Installer running filepath	Vsyncd started installing the downloaded file.
Installation is complete	Vsyncd completed the installation of the file on the devices.
Invoking REST API	Vsyncd is about to invoke the specified REST API call.
IP translation: starting conversion of IP addresses from offset	Starting translation of the IP addresses file that was just downloaded.
Installing file to appliances	Vsyncd started copying the translated file to devices.
IP address list after processing include/exclude list: *ip-address*	List of IP addresses of devices that receive the current file update.
Max file count exceeded while converting urls	When the target file is split into multiple VOS CSV files and a maximum file limit has been configured, the limit has been reached. All entries in the source file after the limit are ignored.
Max file count exceeded while converting ipaddrs; ignoring all URLs after line	When the target file is split into multiple VOS CSV files and a maximum file limit has been configured, the limit has been reached. All entries in the source file after the limit are ignored.
Number of translated entries 0	No entries from the source file have been translated to VOS format. Vsyncd updates the empty file on the devices.
Processing URL extraction	Vsyncd is trying to extract the URL from the webpage that has the IP/URL/domain/IP port files.
Processing vsync entry with name	Vsyncd could not parse the configuration file.
Reloading url data for tenant on appliances	Vsyncd started notifying devices to reload the new version of the file.

Messages	Description
Reloading ip data for tenant on appliances	Vsyncd started notifying devices to reload the new version of the file
Reloading ip data on tenant appliance	Vsyncd started notifying devices to reload the new version of the file
Started copying file using rsync to appliances	Vsyncd started copying the translated file to the devices.
Spawning downloader process	Vsyncd is about to download the IP/URL/domain/IP port file.
Setting permissions for files copied to appliances	Vsyncd started setting permissions of the copied files on the devices so that the files can be processed by the corresponding module.
Tenant list	List of tenants that are affected by the installation of current IP/URL/domain/IP port files on the devices.
Tenant list does not map to any devices; skipping sync	Tenants specified in the configuration file are not provisioned on any of the devices that are curreently provisioned on the Director mpde
Tenant list after include/exclude host	List of IP addresses of devices that receive the current file update.
Tenant list: IP address list after processing include/ exclude list	List of IP addresses of devices that receive the current file update.
Terminating downloader process	Vsyncd is terminating the download process because of a timeout.
Terminating installer process	Vsyncd is terminating the install process because of a timeout.

Messages	Description
Tenant is on devices	List of devices on which the tenant is provisioned.
Translated url file is empty	No entries from the source file were translated to VOS format. Vsyncd updates the empty file to the devices.
Translated IP Address file is empty	No entries from the source file were translated VOS Versa format. Vsyncd updates the empty file to the devices.
URL extraction failed	Vsyncd could not find the URL of IP/URL/domain/IP port file on the referenced website.
Unsupported format for URL extraction	Vsyncd could not extract the URL from the webpage that has the IP/URL/domain/IP port files.
Unable to get download timeout from config; error details:	Vsyncd process could not parse the configuration file.
Unable to connect/authenticate with Versa Director:	REST API call to the Director node to fetch the tenant list and parse the response failed.
Unable to process vsync entry message	Vsyncd process could not parse the configuration file.
Unable to process vsync entries	Vsyncd process could not parse the configuration file.
Unknown file format	Format of the source file is unknown Only the XML, TXT, and JSON formats are supported.
VSync to appliances currently disabled; will check again in seconds	Vsyncd is running in standby mode, so it is not updating the devices with new versions of IP/URL/domain/IP port files.

VSync Limitations and Recommendations

If you configure the feeds for IP addresses, domain, and URLs so that each file contains 64,000 entries, the following performance issues may occur:

- Performance may decrease by 1-2 percent.
- Memory utilization may increase by 40 to 50 MB.
- When loading the URL patterns file, CPU utilization of control CPU may reach 100 percent.
- IP address and URL file compilation can take between 5 seconds and 20 minutes depending on the platform. During this time, checking the status of the data plane processing is blocked and any pending configuration commits are queued until the URL pattern compilation completes. After the URL pattern compilation completes, the configuration commits are processed and applies to NGFW.

In this scenario, the following limits are recommended:

- Each IP address file should have 65,535 IP addresses.
- Domain files are processed as URL pattern matches. The number of URL patterns (domains) per file is limited to a maximum of 2048 domains per file.
- URL files are processed as string matches. You can configure a maximum of up to 128,000 URL entries per file.

Supported Software Information

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

Additional Information

Configure Address Objects
Configure Layer 7 Objects