
Configure Log Export Functionality

 For supported software information, click [here](#).

You can configure Versa Operating System™ (VOS™) devices, both Controller nodes and branch devices, to send log data to Analytics nodes, syslog servers, or third-party Netflow collectors, which perform data analysis and provide reports and data visualization. To do this, you enable the log export functionality (LEF) on the VOS device. VOS devices export log data in IPFIX and syslog formats.

Features and services on the VOS device generate logs, and LEF forwards the logs to Analytics log collector nodes over TCP or UDP connections called LEF connections.

To export log data from VOS devices to an Analytics node or a syslog server, you configure a log export template, a collector, and a LEF profile, and you then select the LEF profile when configuring a feature or service. The logs for the feature or service are forwarded to the active collector named in the LEF profile. You can also configure groups of collectors. For information about forwarding logs for specific features and services, see [Apply Log Export Functionality](#).

To export log data from VOS devices to a Netflow collector, you also configure a log export template, a collector, and a LEF profile. However, the Netflow collector connection protocol and IPFIX format can differ from that used by Analytics nodes, and differs between Netflow implementations. For some Netflow implementations, you must also configure a traffic-monitoring policy rule associated with the LEF profile.

You can set LEF monitoring controls on VOS devices, such as maximum number of source IP addresses to export. For more information, see [Configure Firewall and SD-WAN Usage Monitoring Controls](#).

Configure Log Export to an Analytics Node or Syslog Server

To configure log export to an Analytics node or syslog server, you do the following:

- Configure a template for log export.
- Configure one or more collectors—A collector specifies a remote device that receives TCP or UDP connections (called LEF connections) from the VOS device. The connections are used to transfer the logs. The collector destination is commonly an ADC service that distributes log connections to multiple nodes, but the destination can be a specific node.
- Optionally, configure a collector group—For collectors with TCP-based destinations, you can configure a collector group to provide high availability (HA) in case a single collector device is unavailable. For collectors with UDP-based destinations, configure you can collector groups if you plan to use a collector group list. For more information, see [Configure a Collector Group](#), below.


- For Releases 21.2.1 and later, you can configure a collector group list to send logs to multiple log collector groups.
- Configure a LEF profile.
- Associate the LEF profile with a feature or service—For more information, see [Apply Log Export Functionality](#).

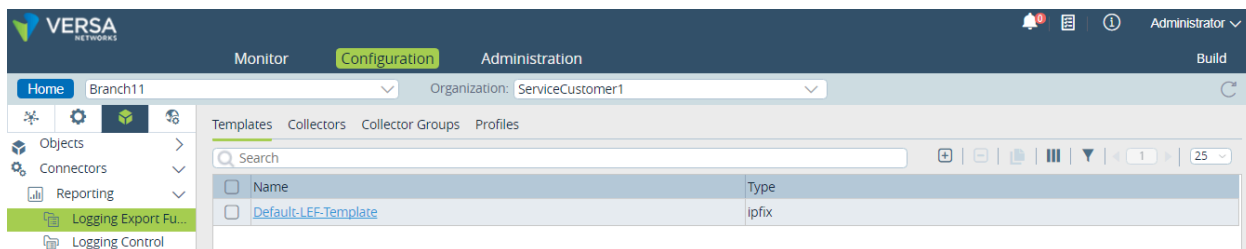
You can also configure log export control and traffic-monitoring policy.


Configure a Template

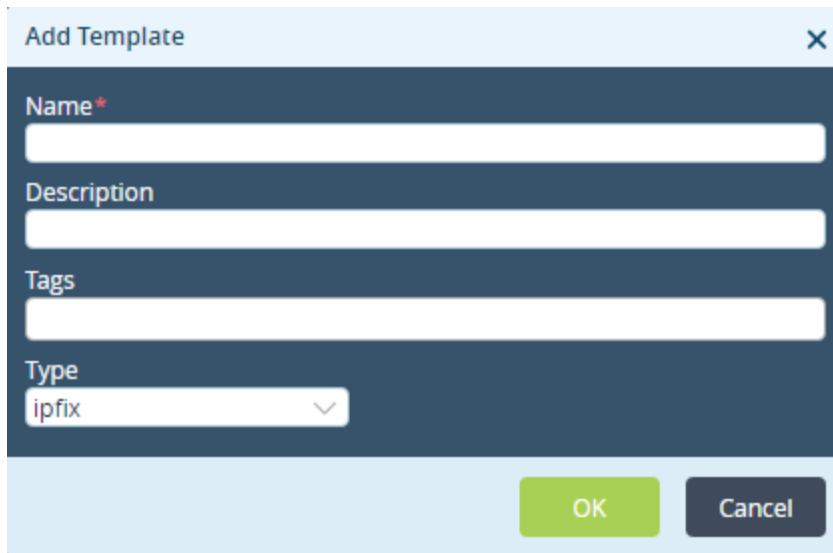
A LEF template indicates either IPFIX or syslog format. Configure an IPFIX-type LEF template for use with LEF collectors that send logs to Analytics nodes or Netflow collectors. Configure a syslog-type LEF template for use with LEF collectors that send logs to syslog servers.

To configure a template for log export:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a branch in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors  > Connectors > Reporting > Logging Export Function in the left menu bar.




4. Select the Templates tab, and click the  Add icon in the main pane to add a new template. The Add Template popup window displays. Enter information for the following fields.



The 'Add Template' dialog box has a title bar with a close button (X). It contains four input fields: 'Name' (required, indicated by an asterisk), 'Description', 'Tags', and 'Type'. The 'Type' field is a dropdown menu currently showing 'ipfix'. At the bottom right are 'OK' and 'Cancel' buttons.

Field	Description
Name	Enter a name for the template name.
Description	Enter a brief description of the template.
Tag	Enter a keyword or phrase that allows you to filter the captive portal action. This is useful when you have many policies and want to view those that are tagged with a particular keyword.
Type	Select the template type IPFIX. The other template type is Syslog.

5. Click OK.

To delete an existing template, select the checkbox corresponding to the template and click the  Delete icon on the top right corner.

To filter the configuration screen table information, click the  Filter icon on the top right corner.

Configure a Collector

You configure LEF collectors to define information about a LEF connection information, including the destination IP address, protocol (TCP or UDP), and port number of the connection.

While logs are waiting to be transferred over LEF connections, VOS devices store the logs in queues. Each LEF collector established three queues:

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_Log...


Updated: Wed, 23 Oct 2024 08:26:43 GMT

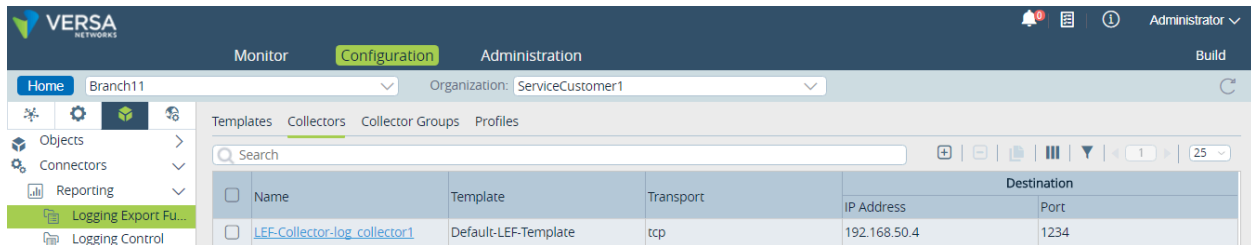
Copyright © 2024, Versa Networks, Inc.


- High priority—Stores high-priority logs, such as alarm logs
- Medium priority—Stores medium-priority logs, such as usage and performance monitoring logs
- Low priority—Stores all other logs

If a LEF connection disconnects or cannot be established, the VOS device retains the logs in the queues for a hold interval, after which it drops the logs. In Releases 21.2.3 and later you can configure how long the collector holds the logs for each log priority.

To configure a LEF collector:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a branch in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors  > Connectors > Reporting > Logging Export Function in the left menu bar.



4. Select an organization in the Organization field.
5. Select the Collectors tab, and then click the  Add icon. In the Add Collector popup window, enter information for the following fields.

Collector

Name*

Description

Tags

Template*

--Select--

Transport

UDP

+ Create Template

Destination

☒ IP Address

☐ FQDN

Port*

Source Address

Routing Instance

--Select--

Transmit Rate (logs/sec)

10000

Pending Queue Limit

2048

Pending Queue Hold Interval

60

Pending HP Queue Hold Interval

900

Template Resend Interval (sec)

60

OK

Cancel

Field	Description
Name	Enter a name for the collector.
Description	Enter a text description for the collector.
Tag	Enter a keyword or phrase that allows you to filter the collector. This is useful when you have many collectors and want to view those that are tagged with a particular keyword.
Template	Select a template.

Field	Description
Transport	Select UDP as the protocol for transporting the log files.
+ Create Template	Click to create a new log template. For more information, see Configure a Template .
Destination (Group of Fields)	
◦ IP Address	Click, and enter the IP address of the destination. For an ADC service, enter the IP address of an ADC service tuple. For information about configuring an ADC service, see Configure an Application Delivery Controller .
◦ FQDN	Click, and enter the FQDN of the destination. VOS uses the DNS server associated with the selected routing instance for resolution. For information about associating a DNS server with a routing instance, see Configure DNS Servers .
◦ Port	Enter the port number of the destination.
Source Address	Enter the IP address of the branch.
Routing Instance	Select the routing instance to use to reach the destination.
Transmit Rate	<p>Enter the rate at which the logs are exported per second.</p> <p><i>Range:</i> 0 through 4,290,496,295 logs per second</p> <p><i>Default:</i> 10000 logs per second</p>
Pending Queue Limit	<p>Enter the maximum number of log messages that the collector buffers. If the number of messages in a queue exceeds this value, for example, because a LEF connection is slow or down, the log messages are dropped.</p> <p><i>Range:</i> 0 through 4,290,496,295</p> <p><i>Default:</i> 2048</p>

Field	Description
Pending Queue Hold Interval	<p>(For Releases 21.2.3 and later.) Enter how long the collector retains logs in the low- and medium-priority queues, in seconds</p> <p><i>Range:</i> 0 through 4,290,496,295 seconds</p> <p><i>Default:</i> 60 seconds</p>
Pending High-Priority Queue Hold Interval	<p>(For Releases 21.2.3 and later.) Enter how long the collector retains logs in the high-priority queue, in seconds.</p> <p><i>Range:</i> 0 through 4,290,496,295 seconds</p> <p><i>Default:</i> 900 seconds</p>
Template Resend Interval	<p>Enter how often to resend the template, in seconds.</p> <p><i>Range:</i> 0 through 4,290,496,295 seconds</p> <p><i>Default:</i> 60 seconds</p>


6. Click OK.

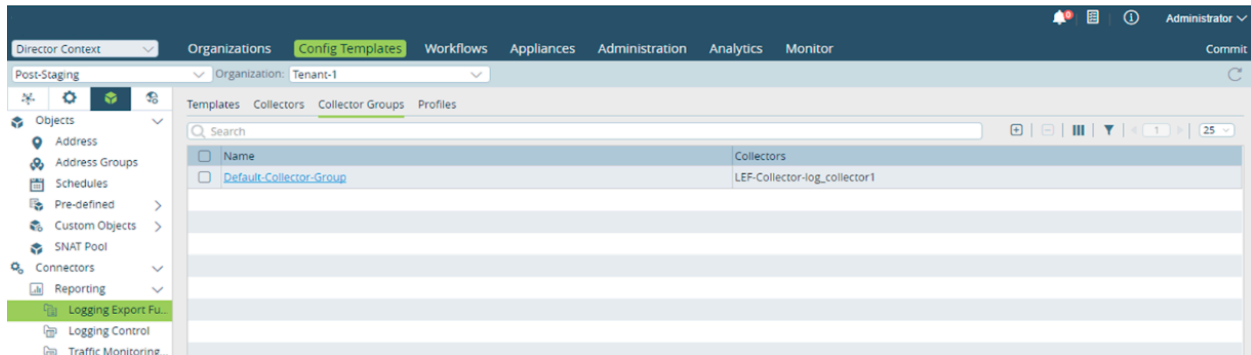
Configure a Collector Group


You can configure a collector group to provide high availability in case a single collector device is unavailable or fails, or if you plan to use a collector group list. For groups with two or more collectors, all collector destinations must be TCP-based servers, because failure detection is based on the TCP three-way handshake process. If the VOS device can establish a TCP session with the server, it is considered active at all times. For collector destinations that use UDP, such as syslog servers, failover to the backup is not be detected and therefore you must configure a separate collector group for each system.


To configure a collector group:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a branch in the main pane. The view changes to Appliance view.

2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors  > Connectors > Reporting > Logging Export Function in the left menu bar.



4. Select an organization in the horizontal menu bar.
5. Select the Collector Groups tab and click the  Add icon. In the Add Collector Group popup window, enter information for the following fields.

Field	Description
Name	Enter a name for the collector group.
Description	Enter a text description of the collector group.
Tag	Enter a keyword or phrase that allows you to filter the captive portal action. This is useful when you have many policies and want to view those that are tagged with a particular keyword.
Primary Collector	(For Releases 20.2.1 and later.) Select a collector to be the primary, or active, collector for the collector group. If the primary collector is down, the next active collector is chosen from the group. When the primary collector comes back up and stays up for a configurable interval, it becomes the active collector again.
Suspend Backup Collectors	<p>(For Releases 20.2.1 and later.) Click to suspend backup collectors. For Releases 20.2.4 and later and for Releases 21.1.3 and later, the suspending of backup collectors is enabled by default.</p> <p>The collectors in a collector group establish TCP connections even if no active logs are being sent over the connection. These connections terminate on the Analytics local collectors, each of which, by default, can terminate a maximum of 512 connections. However, it is sometimes difficult to determine whether these connections are carrying logs, so some collector nodes may have more log activity than others. To ensure that only connections carrying logs are terminated, you can place backup collectors into a suspended state until the active collector has been down for a specific time interval. When that interval is exceeded, the backup collector connections are reinitiated. If a backup connection comes up, it becomes the primary (active) collector. The other collectors in the collector group remain suspended as long as they are not the primary collector.</p>
Collectors	Select a collector, and click the  Add icon.
+ Add New Collector	Click to add a collector to the list.

6. Click OK.

Configure a Collector Group List

For Releases 21.2.1 and later.

You configure a collector group list to send logs to multiple collectors for redundancy or for serving different applications. A collector group list is a list of collector groups and is part of a LEF profile configuration. When you associate this LEF profile with a service, such as NGFW, or with the traffic-monitoring function for the organization, the LEF sends logs to the active collector of each collector group in the list.

You configure a collector group list from the CLI on a branch or controller VOS device, by issuing the following command. For information about accessing the CLI, see [Access the CLI on a VOS Device](#)

```
set orgs org-services organization-name lef profiles logging-profile-name collector-group-list collector-group-1
[collector-group-2]
```

For example, the following configuration shows a collector group list consisting of two collector groups, Collector-Group1 and Collector-Group2, for the LEF profile named Default-Logging-Profile:

```
Branch1$ cli
Branch1> configure
Branch1% show orgs org-services Tenant1 lef profiles
profiles {
  profile Default-Logging-Profile {
    collector-group-list [Collector-Group1 Collector-Group2];
  }
}
```

Configure a LEF Profile

You can configure one or more LEF profiles, and you can assign one of them as the default profile. When a default LEF profile is assigned, the following log types are automatically forwarded to its active collector:

- Alarm logs (alarmLog), unless a separate profile is designated as the default for alarms
- LTE summary logs (lteEventLog, lteStatsLog)
- MOS summary logs (sdwanPathMosLog)
- SD-WAN SLA metrics logging (sdwanB2BSlamLog)
- SD-WAN traffic-conditioning logs (sdwanPathCondLog)
- System logs (systemLoadLog)

For Releases 22.1.1 and later, you can set a profile to be the default for alarm logs.


To configure a LEF profile:

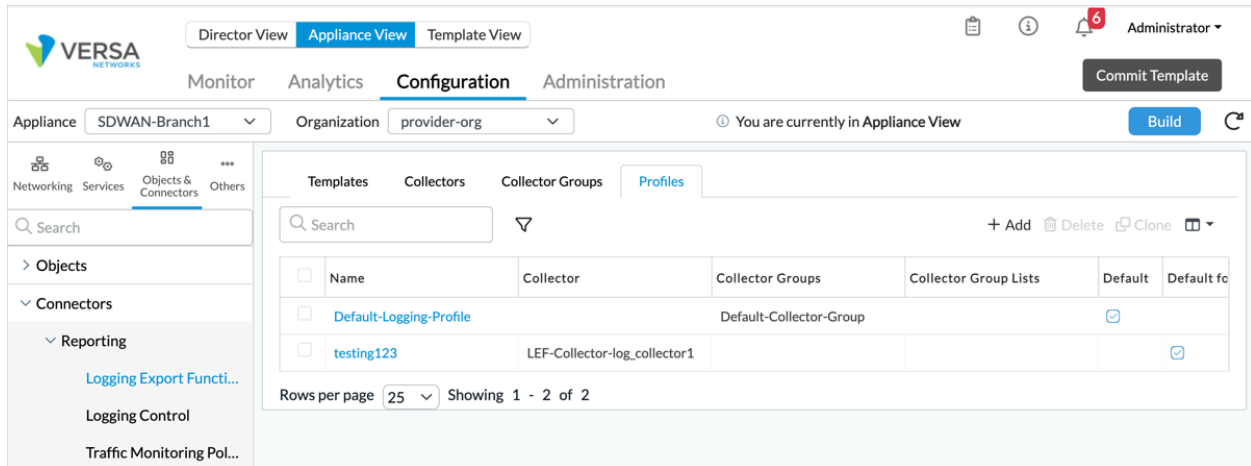
1. In Director view:


https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_Log_...

Updated: Wed, 23 Oct 2024 08:26:43 GMT

Copyright © 2024, Versa Networks, Inc.

- a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a branch in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
 3. Select Objects & Connectors  > Connectors > Reporting > Logging Export Function in the left menu bar.



4. Select the Profiles tab, and click the  Add icon. In the Add Profile popup window, enter information for the following fields.

Add Profile

Name *

Description

Tags

☒ Collector

☐ Collector Group

--Select--

+ Create Collectors

☐ Collector Group

+ Add New Collector Group

☐ Default

☐ Default for alarms

OK

Cancel


Field	Description
Name	Enter a name for the LEF profile.
Description	Enter a brief description of the LEF profile.
Tag	Enter a keyword or phrase that allows you to filter the LEF profile. This is useful when you have many profiles and want to view those that are tagged with a particular keyword.
Collector	Click, and then select a collector to associate it with the LEF profile. You can associate a profile with either a collector or collector group.
Collector Group	Click, and then select a collector group to associate it with the LEF profile. You can associate a profile with either a collector or collector group.
Default	Click to make this the default LEF profile for the organization.
Default for Alarms	(For Releases 22.1.1 and later.) Click to make this the default LEF profile for alarms. Only one LEF profile can be the default for alarms. If another LEF profile is currently the default for alarms, this option is automatically deselected from the other profile.

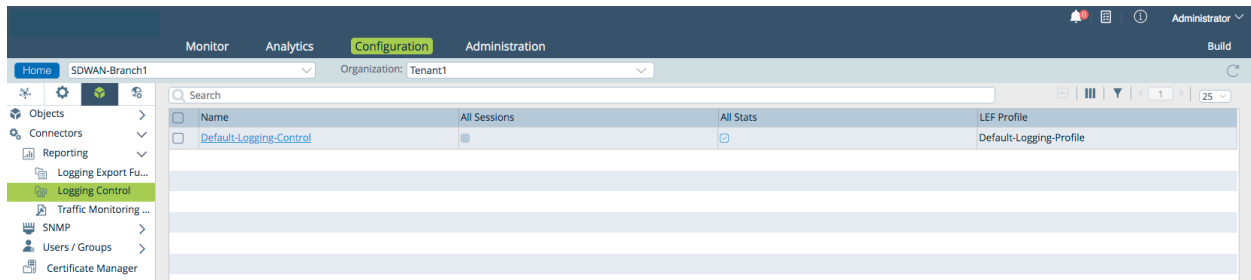
5. Click OK.


Configure Log Export Control

You can configure log export to capture either statistical data or session data.

To configure the type of logs to export:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a branch in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors  > Connectors > Reporting > Logging Control in the left menu bar



- To edit the log export configuration, click the log export control name in the main pane (Default-Logging-Control in the example above), or click the  Add icon to add log export control. In the Add/Edit Logging Control popup window, enter information for the following fields.

Add Logging Control

Name*

Description

Tags

☐ All Stats

☐ All Sessions

LEF Profile

--Select--

Events

end

OK


Cancel

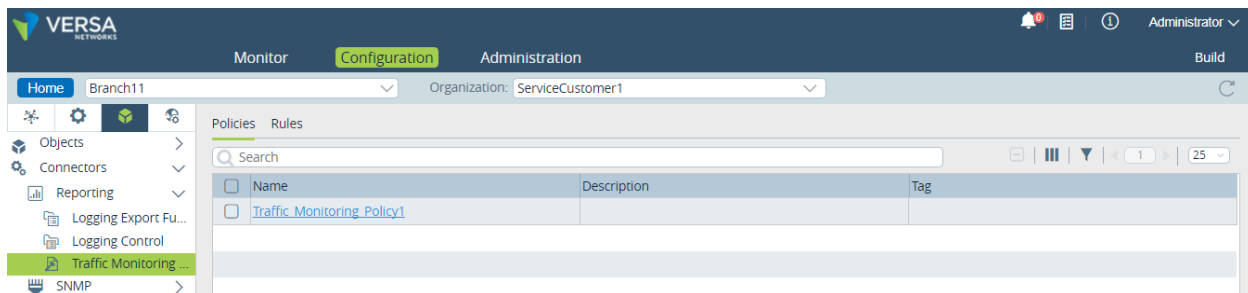
Field	Description
Name	Enter a name for the log export control.
Description	Enter a brief description of the log export control.
Tag	Enter a keyword or phrase that allows you to filter the log export control. This is useful when you have many controls and want to view those that are tagged with a particular keyword.
All Stats	Click to forward global firewall per-flow logs. See Configure Firewall Logging in Apply Log Export Functionality .
All Sessions	Click to export traffic-monitoring logs globally for all flows. See Configure SD-WAN Traffic and Web-Monitoring Logging in Apply Log Export Functionality .
LEF Profile	Select the name of a LEF profile.

5. Click OK.

Configure Traffic-Monitoring Policy

To define the rules for exporting log information, you configure a traffic-monitoring policy:

- In Director view:
 - Select the Configuration tab in the top menu bar.
 - Select Devices > Devices in the horizontal menu bar.
 - Select an organization in the left menu bar.
 - Select a branch in the main pane. The view changes to Appliance view.
- Select Objects & Connectors  > Connectors > Reporting > Traffic Monitoring in the left menu bar.
- Select the Policies tab in the horizontal menu bar.



4. Click the  Add icon. In the Add Policies popup window, enter information for the following fields.

Add Policies

Name*


Description

Tags

OK

Cancel

Field	Description
Name	Enter a name for the traffic-monitoring policy.
Description	Enter a text description for the policy.
Tag	Enter a keyword or phrase that allows you to filter the policy name. Tagging is useful when you have many policies and want to view those that are tagged with a particular keyword.

5. Click OK.
6. Select the Rules tab in the horizontal menu bar.
7. Click the  Add icon. The Add Rules popup window displays. Select the General tab, and enter information for the following fields.

Add Rules
✕

General
Source/Destination
Applications/URL
Headers/Schedule
Enforce

Name*

Description

Tags

OK
Cancel

Field	Description
Name	Enter a name for the traffic-monitoring rule.
Description	Enter a description for the rule.
Tag	Enter a keyword or phrase that allows you to filter the rule. Tagging is useful when you have many rules and want to view those that are tagged with a particular keyword.

8. Click OK.
9. Select one or more the following tabs to define the policy rule. For information about the fields on these tabs, see [Configure Policy-Based Forwarding](#).
 - a. Source/Destination Addresses—Enable log export based on the source or destination IP address of the traffic or the zone of the traffic.
 - b. Header/Schedule—Enable log export based on specific header information.
 - c. Application/URL—Enable log export for specific applications or URL.
10. Select the Enforce tab, and enter information for the following fields.

Edit Rules - Rule-Wildcard

General

Source

Destination

Headers/Schedule

Applications/URL

Enforce

Flow Logging Setting

Start

End

Start and End

Interim

Never

Send to Netflow Collector

LEF Profile

--Select--

Default Profile

+ LEF Profile

Web Monitoring

Send SASE Web Data

LEF Profile

--Select--

Default Profile

+ LEF Profile

Performance Monitoring

TCP Monitoring

LEF Options

Send Extended Application Metadata

Send HTTP Metadata for HTTP Sessions

Send Packet Capture Data

Count

Match

All

Unclassified App ID

Unknown App ID

DNS Monitoring

Send DNS Metadata

LEF Profile

--Select--

Default Profile

+ LEF Profile

OK

Cancel

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_Log...

Updated: Wed, 23 Oct 2024 08:26:43 GMT

Copyright © 2024, Versa Networks, Inc.

18

Field	Description
Flow Logging Setting (Group of Fields)	Select when to export flow logging records.
◦ Start	Click to log data at the start of each session.
◦ End	Click to log data at the end of each session.
◦ Start and End	Click to log data at the start and end of each session.
◦ Interim	Click to log data at interim times when the flow is active for a long period of time. The default interim time is 1 minute, and this time is not configurable.
◦ Never	Click to never send log data.
◦ Send to Netflow Collector	Click to log data using a template that is compatible with Netflow collectors.
LEF Profile	Select the LEF profile to associate with the traffic-monitoring rule. Click Default Profile to associate the rule with the default LEF profile.
LEF Options (Group of Fields)	<p>Select one or more LEF options to associate with the traffic-monitoring rule:</p> <ul style="list-style-type: none"> ◦ Send Extended Application Metadata—Selecting this option causes SD-WAN traffic log messages to include application metadata, such as application risk, productivity, family, and subfamily. See SD-WAN Traffic Logs. ◦ Send HTTP Metadata for HTTP Sessions—Selecting this option populates the Web Monitoring table when you select the Analytics > Dashboards > Logs tab. ◦ Send Packet Capture Data—Selecting this option sends packet capture data to Analytics nodes. See Configure Packet Capture Logging in Apply Log Export Functionality.
◦ Count	Enter the count for the packet capture.
◦ Match	Select a match option:

	<ul style="list-style-type: none"> ◦ All ◦ Unclassified App ID ◦ Unknown App ID
DNS Monitoring (Group of Fields)	<i>(For Releases 22.1.1 and later.)</i>
◦ Send SASE Web Data	Click to send saseWebLog logs to Analytics at the end of a flow for web traffic if a rule match occurs.
◦ LEF Profile	Select the LEF profile to associate with the DNS traffic-monitoring traffic-monitoring rule.
◦ Default Profile	Click to associate the rule with the default LEF profile.
Web Monitoring (Group of Fields)	<i>(For Releases 22.1.1 and later.)</i>
◦ Send DNS Metadata	Click to send logs for DNS traffic to Versa Analytics.
◦ LEF Profile	Select the LEF profile to associate with the web-monitoring rule.
◦ Default Profile	Click to associate the rule with the default LEF profile.
Performance Monitoring (Group of Fields)	Click to enable TCP monitoring of the policy rules.
◦ TCP Monitoring	Click to enable application performance monitoring (APM). For more information, see Configure Application Performance Monitoring .

11. Click OK.

Configure Log Export to a Netflow Collector

Netflow collectors that support the IETF-standard Netflow Version 10 can process log data sent in IPFIX format. (Netflow Version 10 is derived from Netflow Version 9.) However, even though the IPFIX record format is defined in the IETF standard, the template fields are not standardized. This can cause interoperability issues if a mandatory field is missing in a vendor's implementation. The template fields in the log data exported by VOS devices to Netflow collectors are compatible with most Netflow implementations. To ensure that your Netflow implementation is compatible with the flows exported by the VOS log export functionality, consult the following tables.

Versa Networks has performed interoperability testing with Riverbed NetProfiler, SolarWinds, Cisco Stealthwatch, and CA Technologies Netflow collectors.

Netflow templates define the fields that are sent in a Netflow record. There are two types of Netflow templates:

- Templates that send flow records only at the beginning, only at the end of a flow, or both at the beginning and end of a flow. These templates reduce the number of logs sent for a flow. The end-of-the-flow log contains the total number of packets or bytes for the flow. This template type uses Template ID 317 for IPv4 records and Template ID 318 for IPv6 records. Only a few vendors, such as SolarWinds and CA technologies, use this type of template.
- Templates that send interim flow records periodically. These templates are used when the flow is active for a long period of time. Flow records are sent every 1 minute, and this value is not configurable. The statistics in each record are for the difference between the previous interval's record and the current interval's record. If a flow ends before the 1-minute time expires, a final log is sent with the statistics for that period. This template type uses Template ID 326 for IPv4 records and Template ID 327 for IPv6 records. Most Netflow collectors support this template.

The following table describes the fields in a Netflow template that send flow records only at the beginning or the end of a flow, or both at the beginning and at the end of a flow.

Field Name	IETF Field ID	Length (Bytes)	Comments
sourceIPv4Address, or sourceIPv6Address	8 27	4 16	—
destinationIPv4Address, or destination IPV6Address	12 28	4 16	—
sourceTransportPort	7	2	—
destinationTransportPort	11	2	—
protocolIdentifier	4	1	—
flowDirection	61	1	Forward or reverse
lineCardId	141	4	Not relevant
tenantId	522 (Versa vendor specific)	2	Useful in multitenancy to identify a tenant
applianceId	574 (Versa vendor specific)	2	Not relevant
flowStartMilliseconds	152	8	Start time since system reboot
flowEndMilliseconds	153	8	End time since system reboot
ingressInterface	10	4	SNMP index of the input interface

Field Name	IETF Field ID	Length (Bytes)	Comments
egressInterface	14	4	SNMP index of the output interface
octetTotalCount	85	8	Total number of bytes since the beginning of the flow
packetTotalCount	86	8	—
eventType	540 (Versa vendor specific)	1	Indicates the start or end of the flow
appld	519 (Versa vendor specific)	4	Identifier of the application carried in the flow


The following table describes the fields in a Netflow template that send flow records periodically during a flow that is active for a long period of time.

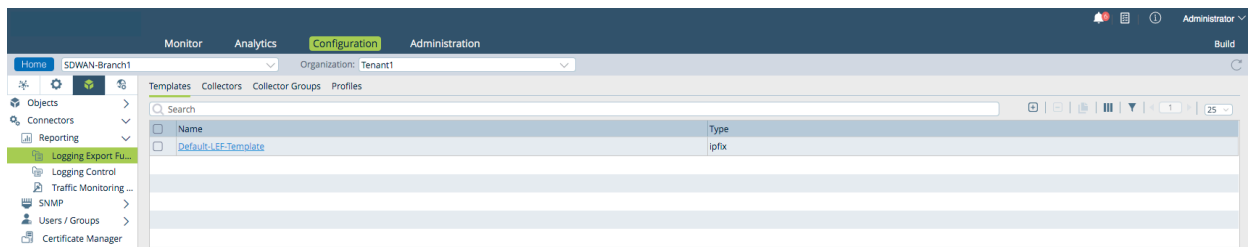
Field Name	IETF Field ID	Length (Bytes)	Comments
sourceIPv4Address, or sourceIPv6Address	8 27	4 16	—
destinationIPv4Address, or destination IPV6Address	12 28	4 16	—
sourceTransportPort	7	2	—
destinationTransportPort	11	2	—
protocolIdentifier	4	1	—
flowDirection	61	1	Forward or reverse
lineCardId	141	4	Not relevant
tenantId	522 (Versa vendor specific)	2	Useful in multitenancy to identify a tenant
applianceId	574 (Versa vendor specific)	2	Not relevant
flowStartMilliseconds	152	8	Start time since system reboot


Field Name	IETF Field ID	Length (Bytes)	Comments
flowEndMilliseconds	153	8	End time since system reboot
ingressInterface	10	4	SNMP index of the input interface
egressInterface	14	4	SNMP index of the output interface
octetTotalCount	1	8	Total number of bytes since the beginning of the flow
packetTotalCount	2	8	—
appld	519 (Versa vendor specific)	4	Identifier of the application carried in the flow
ipClassOfService	5	1	—

To send Netflow logs to third-party collectors, you create a new Netflow collector, a collector group (optional), and a profile. You can then associate this profile with a traffic-monitoring rule that defines the type of data to be exported.

Configure a Netflow Collector

- In Director view:
 - Select the Administration tab in the top menu bar.
 - Select Appliances in the left menu bar.
 - Select an appliance in the main panel. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Objects  > Connectors > Reporting > Logging Export Function in the left menu bar.



- Select the Collectors tab in the horizontal menu bar.
- Click the  Add icon. In the Add Collector popup window, enter information for the required fields (indicated by a red asterisk). Entering information for other fields is optional.

Add Collector
X

Name*

Description

Tags

Template*
--Select--
Transport
UDP

+ Create Template

Destination

IP Address*
Port*

Source Address
Routing Instance
--Select--

Transmit Rate (logs/sec)
10000
Pending Queue Limit
2048

Template Resend Interval (sec)
60



OK
Cancel

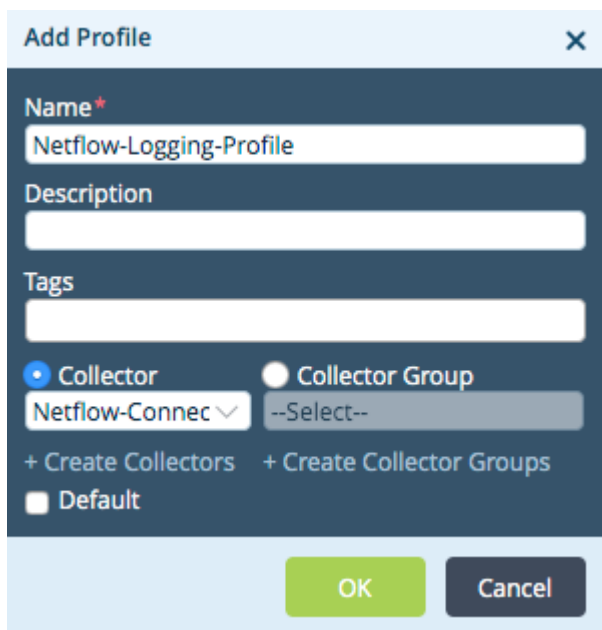
Field	Description
Name	Enter a name for the collector.
Template	Select the template to use. Choose a template that uses type IPFIX.
Transport	Enter the protocol to use to reach to collector destination: <ul style="list-style-type: none"> TCP UDP
Destination (Group of Fields)	
<ul style="list-style-type: none"> IP Address 	Enter the IP address of the collector destination.

Field	Description
◦ Port	Enter the port number of the collector destination.

6. Click OK.

Configure a Netflow Profile

1. If you are continuing from the previous section, skip to Step 4. Otherwise, in Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select an appliance in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects  > Connectors > Reporting > Logging Export Function in the left menu bar.
4. Select the Profiles tab in the horizontal menu bar.
5. Click the  Add icon to add a new profile. In the Add Profile screen, enter the information for the required fields (indicated by a red asterisk). Entering information for other fields is optional.




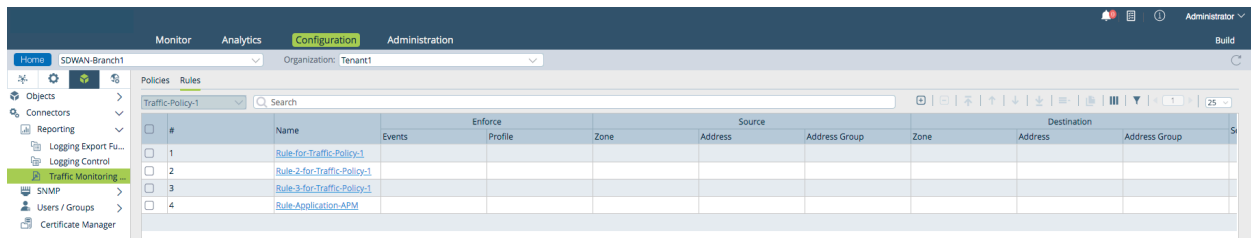
Field	Description
Name	Enter a name for the collector.
Collector	Click and select the collector to use.

- Click OK.

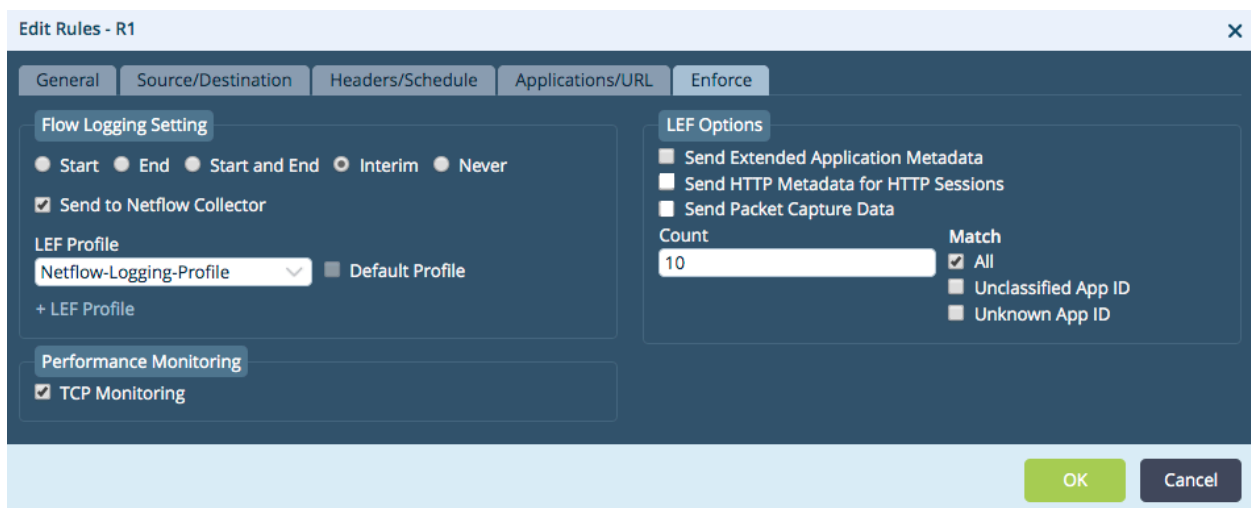
Configure Traffic-Monitoring Policy for Exporting Logs to a Netflow Collector

You can enable traffic-monitoring rules to selectively enable flow logging for traffic that matches a rule. The match is based on Layer 3 through Layer 7 fields, such as source, destination, protocol, ports, application, and URL category. If you do not configure match criteria, the rule is treated as a wildcard rule, matching all traffic.

- If you are continuing from the previous section, skip to Step 3. Otherwise, in Director view:
 - Select the Administration tab in the top menu bar.
 - Select Appliances in the left menu bar.
 - Select an appliance in the main panel. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Objects  > Connectors > Reporting > Traffic Monitoring in the left menu bar.
- Select the Rules tab in the horizontal menu bar.



- Click a rule in the main pane. The Edit Rules popup window for that rule displays.



- Select the Enforce tab, and enter information for the following fields.

Field	Description
Flow Logging Setting (Group of Fields)	Select when to export flow logging records.
<ul style="list-style-type: none"> Start 	Click to log data at the start of each session. Select this option for templates that send flow records only at the beginning, only at the end of a flow, or both at the beginning and end of a flow. Only a few vendors, such as SolarWinds and CA technologies, use this type of template.
<ul style="list-style-type: none"> End 	Click to log data at the end of each session. Select this option for templates that send flow records only at the end of a flow or both at the beginning and end of a flow. Only a few vendors, such as SolarWinds and CA technologies, use this type of template.
<ul style="list-style-type: none"> Start and End 	Click to log data at the start and end of each session.
<ul style="list-style-type: none"> Interim 	Click to log data at interim times when the flow is active for a long period of time. The default interim time is 1 minute, and this time is not configurable. Most Netflow collectors support this template.
<ul style="list-style-type: none"> Never 	Click to never send log data.
Send to Netflow Collector	<p>Click to send logs to a Netflow collector, using a template that is compatible with Netflow. These flow logs contain the fields described in the Netflow templates section, above.</p> <p>For interoperability with SolarWinds, Cisco Stealthwatch, and CA Technologies Netflow collectors, click this option.</p> <p>If you do not select this option, the flow logs are sent using the Versa flow-monitoring template.</p>
Collector	Click and select the collector to use.

7. Click OK.

Transfer Log Files

You can transfer log files from a VOS device to a remote system using a Director node as an intermediary. You can do this using either an out-of-band port or the management IP address of the VOS device to perform the transfer to the Director node. From the Director node, you can then use any standard file-transfer tools to copy the files to the remote system.

On VOS devices, log files are stored in the `/var/log/versa` directory.

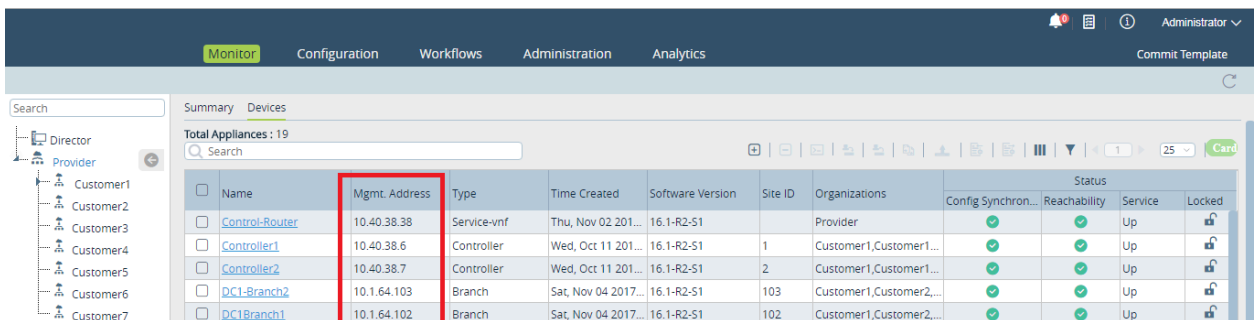
Transfer Log Files using an Out-of-Band Port

By default, all hardware devices are preconfigured to use the IP address 10.10.10.10 on eth0 as the out-of-band port. To change the port, modify the `/etc/network/interfaces` file. After you configure the eth0 interface, connect it to your management network and use SCP to transfer log files between the VOS device and the Director node.

Transfer Log Files using the Management IP Address

To transfer log files to a Director node using the management IP address of the VOS device:

1. In Director, look up the management IP address of the VOS device.
 - a. In Director view, select the Monitor tab.
 - b. In the left menu bar, select a provider organization.
 - c. In the main pane, select Devices. The following screen displays.



Name	Mgmt. Address	Type	Time Created	Software Version	Site ID	Organizations	Config Synchron...	Reachability	Service	Locked
Control-Router	10.40.38.38	Service-vmf	Thu, Nov 02 201...	16.1-R2-S1		Provider	✓	✓	Up	🔒
Controller1	10.40.38.6	Controller	Wed, Oct 11 201...	16.1-R2-S1	1	Customer1,Customer1...	✓	✓	Up	🔒
Controller2	10.40.38.7	Controller	Wed, Oct 11 201...	16.1-R2-S1	2	Customer1,Customer1...	✓	✓	Up	🔒
DC1-Branch2	10.1.64.103	Branch	Sat, Nov 04 2017...	16.1-R2-S1	103	Customer1,Customer2...	✓	✓	Up	🔒
DC1Branch1	10.1.64.102	Branch	Sat, Nov 04 2017...	16.1-R2-S1	102	Customer1,Customer2...	✓	✓	Up	🔒

- d. In the Management Address column, identify the management IP address of the VOS device.
2. Log in to a shell on the Director node.
 3. To copy a log file from the VOS device to the Director node, issue the following shell command, where *management-ip-address* is the IP address from Step 1d and *path-to-file* is the name of the log file.

```
admin@Director$ scp admin@management-ip-address:path-to-file ./
```

For example:

```
admin@Director$ scp admin@10.1.64.102:/var/log/versa/alarms ./
admin@10.1.64.102's password:
```

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Releases 20.2.1 and later support configuring a primary collector and suspending backup collectors.
- For Releases 20.2.4 and later and for Releases 21.1.3 and later, the suspending of backup collectors is enabled by default.
- Releases 21.2.1 and later support collector group lists.
- Releases 21.2.3 and later support fields pending queue and high-priority queue hold interval for collectors.
- Releases 22.1.1 and later support web and DNS monitoring; you can designate a LEF profile to be the default for alarm logs.

Additional Information

[Apply Log Export Functionality](#)

[Configure an Application Delivery Controller](#)

[Configure Application Performance Monitoring](#)

[Configure Firewall and SD-WAN Usage Monitoring Controls](#)

[Configure Log Collectors and Log Exporter Rules](#)

[Configure Policy-Based Forwarding](#)

[Configure the Versa Advanced Logging Service](#)

[Versa Analytics Configuration Concepts](#)

[Versa Analytics Scaling Recommendations](#)