
Configure Application Performance Monitoring

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

Versa Operating System™ (VOS™) application performance monitoring (APM) is a method for passively measuring TCP-based application performance metrics that is more representative of the user experience than generic active network probes. Generic active network-level probes provide only limited details about an application's performance. For example, ICMP probes measure only round-trip time and loss at the network layer. Also, generic active network-level probes are less suited for real-time monitoring,

You can use APM to gauge the performance of business applications and services by monitoring your organization's IT resources to help determine whether your IT environment meets the desired performance standards. Because VOS devices are a session-based systems, a VOS device is aware of the sessions, traffic flows, and other attributes related to the traffic flow. APM uses this information to provide insight into performance and user experience.

APM is based on TCP monitoring, and it performs passive application monitoring, or single-ended measurement, of TCP metrics for performance measurement, which include the connection setup time, the server connection reset rate, the application response time, the retransmission rate, and the network round-trip time. For example, APM tracks the timestamps between TCP messages, such as those between SYN and SYN-ACK messages and between SYN-ACK and ACK messages, and it also tracks the SYN-to-ACK network response time (NRT). APM derives other metrics from sequence numbers and from missing or received packets.

To enable passive APM, you configure TCP performance monitoring under a traffic monitoring rule. The VOS device collects APM metrics inline as traffic passes through the device. These metrics are reported in two ways:

- Historical reporting—Performance metrics for a tenant, user, destination prefix, application, and egress WAN link or path are aggregated every 5 minutes and exported to Analytics nodes.
- Live reporting—(For Releases 22.1.1 and later.) Performance metrics for the previous 2 minutes for matched application per egress. You can view these metrics from the Director Monitor tab, and they are pulled on-demand from the VOS device.

APM can be resource-intensive, so you should consider the following when deciding whether and when you want to enable it:

- APM aggregates logging data before sending it to Analytics nodes, and it sends data for each tenant, application, source IP address, destination IP address and WAN interface separately. This process requires significant bandwidth on both the VOS device and the Analytics node. To minimize the impact of the log aggregation, it is recommended that you enable APM selectively only on traffic of interest.
- Enabling APM monitoring can degrade the performance of the VOS device, because it adds load to the system that

is equal to that imposed when the application offload function is disabled. Application offload is a function that performs application inspection when you enable unified threat management (UTM) capabilities, such as antivirus.

APM Metrics

The sections below describe the various APM metrics that are available as part of live and historical reporting.

TCP Raw Metrics

Metric	Description
SYN to SYN-ACK (SSA) RTT	Estimate of the round-trip time (RTT) between a SYN and a SYN-ACK message. receiving the SYN-ACK message from a server.
SYN-ACK to ACK (SAA) RTT	Estimate of the RTT between a SYN-ACK and an ACK message. An increase in the SAA RTT indicates a delay in receiving the ACK message. Both the SAA and SSA RTTs are an indication of latency to the server. High values suggest underlay-routing changes that are causing traffic to traverse a longer path.
SYN-to-ACK NRT	Indicates that the end-to-end RTT for establishing a session is equal to the sum of the SSA and SAA RTTs. This metric is used to estimate the network latency that occurs when a session is being established. When you experience a long pause in a browser before a webpage is populated. However, depending on the application, for example, for a bulk traffic application, the latency may be perceived as an initial delay. For an interactive application, the further increase in latency can have a detrimental effect on user experience. This metric is used in statistics when optimizing a network to determine whether a server is too far away.
Connection Refused	Counter that increases when a client sends a SYN message and the server returns a RST message. This indicates that the application is currently unavailable on a server.
Connection Aborted	Connection Refused and Connection Aborted are an indication of problems with the server. The server sends a RESET message after the three-way handshake completes.
TCP Retransmission Forward	Number of data segments retransmitted in the forward direction. For example, if 100 acknowledgement packets are sent and 20 of them are retransmitted, the forward retransmission rate is 20%.
TCP Retransmission Reverse	Number of data segments retransmitted in the reverse direction. For example, if 100 acknowledgement packets are sent and 20 of them are retransmitted, the forward retransmission rate is 20%.
SYN Retransmission	Counter that increases when a SYN message is resent. It indicates that a SYN packet was dropped or lost.

Metric	Description
	packet was sent, or a SYN message has been sent but a SYN-ACK message has not been received. This indicates that network packet loss is occurring while a session is being established. To determine whether wider packet loss problems might be occurring in the network, also examine the values of the TCP retransmission forward and reverse counters.
SYN-ACK Retransmission	Counter that increases when a SYN-ACK message is present. It indicates that a SYN-ACK message has been sent but a SYN-ACK message has not been received. The retransmission of SYN-ACK messages indicates that network packet loss is occurring. To determine whether wider packet loss problems might be occurring in the network, also examine the values of the TCP retransmission forward and reverse counters.

Network Metrics

Metric	Description
Network Response Time	<p>The network response time is determined based on the SYN to SYN-ACK (SSA) round-trip time (RTT) and SYN-ACK to ACK (SAA) RTT measurements. For more information, see the figure about application response times, below.</p> <p>VOS devices can measure network, server, and application response times for TCP sessions that are transiting the application directly or are proxied on the device by HTTP, SSL, or TCP. All response times are position independent; that is, the measurement is the same regardless of whether the VOS device is closer to the client or closer to the server.</p>
Versa Link Rank	<p>(For Releases 22.1.1 and later.) For TCP-based sessions, the Versa link rank (VLR) is a measure of application quality. The Versa link rank consolidates TCP (that is, network) metrics into a single value that represents that application's performance. The Versa link rank is a value from 0 (best performance) through 100 (worst performance).</p> <p>You can display the VLR on live monitoring views.</p>

Metric	Description
Versa App Rank	The Versa application rank is calculated using the same method as VLR, using TCP metrics for specific tenants, branches, applications, and users. The Versa application rank is a value from 0 (best performance) through 100 (worst performance).

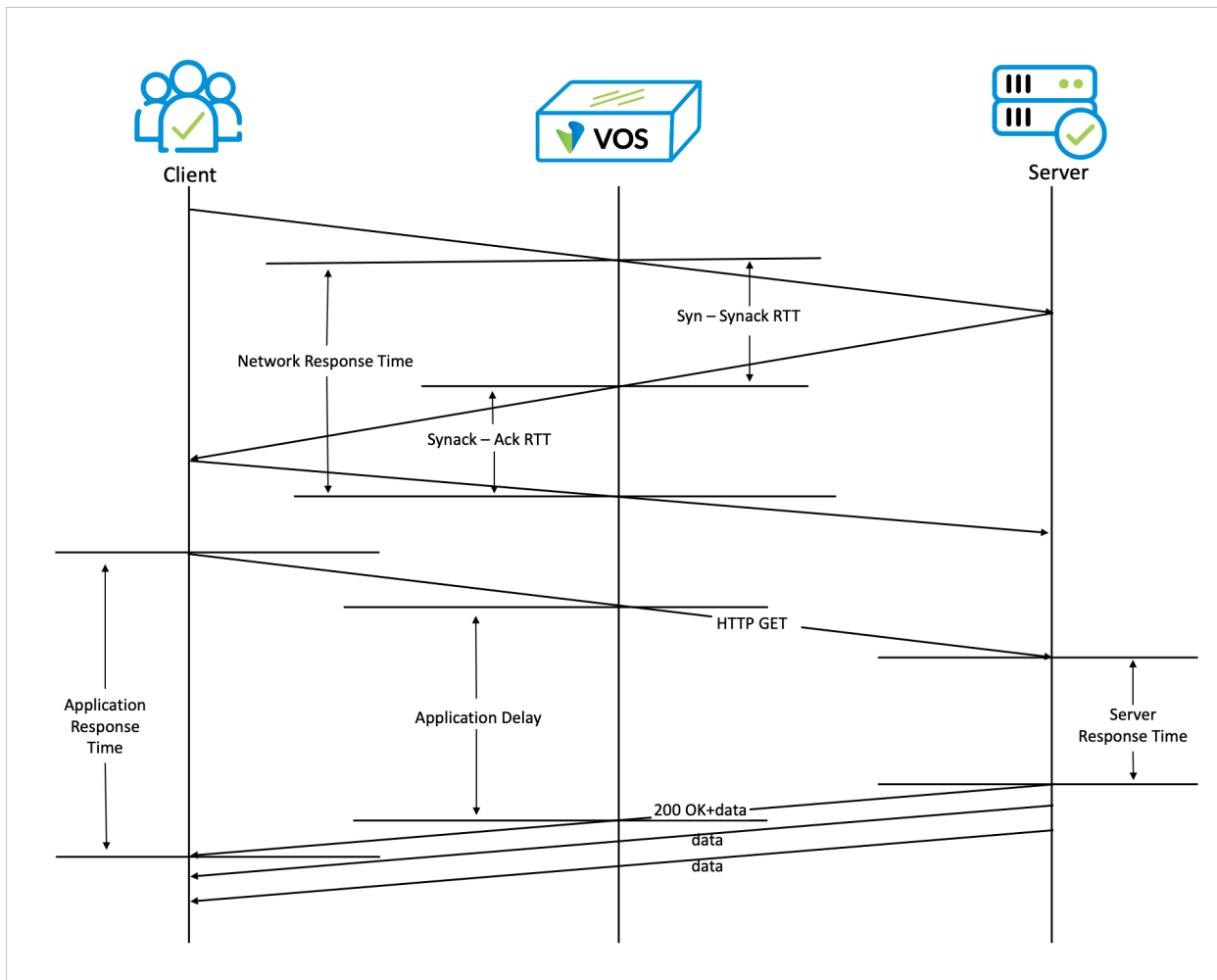
HTTP/HTTPS–Based Application Metrics

For Releases 22.1.1 and later.

Name	Description
Application Response Time	<p>The application response time is the time difference between an application-level request from a client to a server and the start of the response to the request. The application response time includes the network response time, server response time, and delays caused by network packet loss and the resulting retransmissions.</p> <p>For HTTP- and HTTPS-based applications, the application layer response time is derived from the first HTTP request to the start of the first HTTP response. For non-HTTP applications, it is calculated from the first client to the server data segment and the first server-to-client data segment.</p> <p>Application Response Time = Application Delay – SynAck-To-AckRTT</p>
Server Response Time	<p>The server response time is the processing delay on the server from the time when it receives the client request until it sends the response. A VOS device cannot directly measure the server response time, so it is estimated based on the network response time.</p> <p>Server Response Time = Application Delay – Syn-To-SynAck-RTT</p>

Name	Description
Successful Application Queries	Count of the successful HTTP/HTTPs requests.
Total Application Queries	Total number of HTTP/HTTPs requests.
Application Performance Score	<p>A VOS device derives an application performance score (APS) based on application response time samples. The VOS device sorts the response times into predefined response time ranges to determine a weighted average of acceptable responses. This weighted average is converted into a score in the range of 1 to 100, with a higher score indicating better performance.</p> <p>For Releases 22.1.1 and later, you can display this metric on live monitoring screens.</p>

The following figure illustrates how APM calculates network, server, and application response times.



Configure Historical APM

To configure historical APM for an organization on a VOS device, you configure a traffic-monitoring policy rule. In the rule, you define the applications and application groups to match, and then you enable TCP performance monitoring. With this configuration, the VOS device collects performance metrics for all applications and application groups matching the rule. Finally, you select a LEF profile that configures the VOS device to export the log metrics in logs to the destination specified in the LEF profile. For more information, see [Configure Log Export Functionality](#).

To use historical APM on a VOS device, you must enable either the SD-WAN or traffic detection function (TDF) functionality, or both.

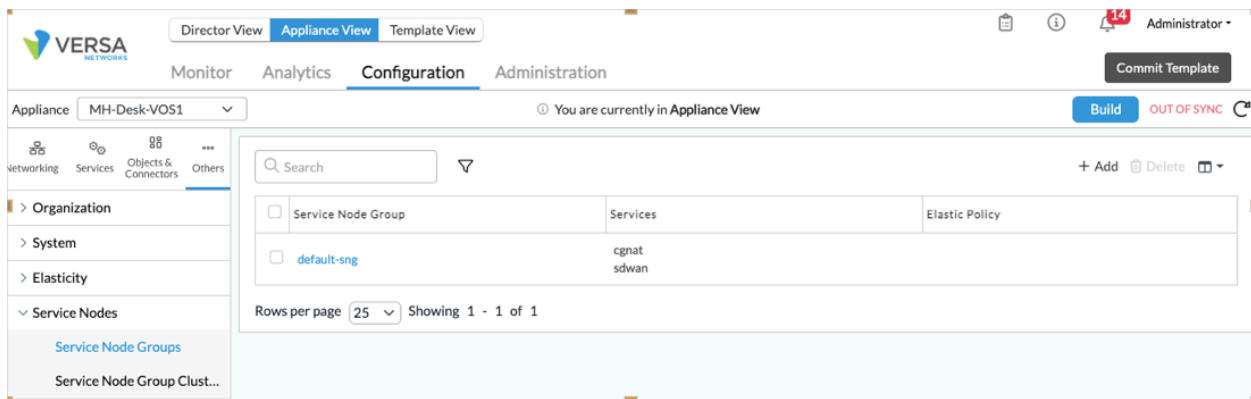
For Releases 22.1.1 and later, the TCP performance monitoring option enables both historical and live monitoring for any supporting applications, even if they are not TCP based.

To configure historical APM for an organization on a VOS device, you do the following:

- Verify that SD-WAN or TDF is enabled globally on the VOS device.
- Verify that SD-WAN or TDF is enabled for the organization.
- Configure traffic monitoring policy rules.

To verify that SD-WAN or TDF is enabled globally on the VOS device:

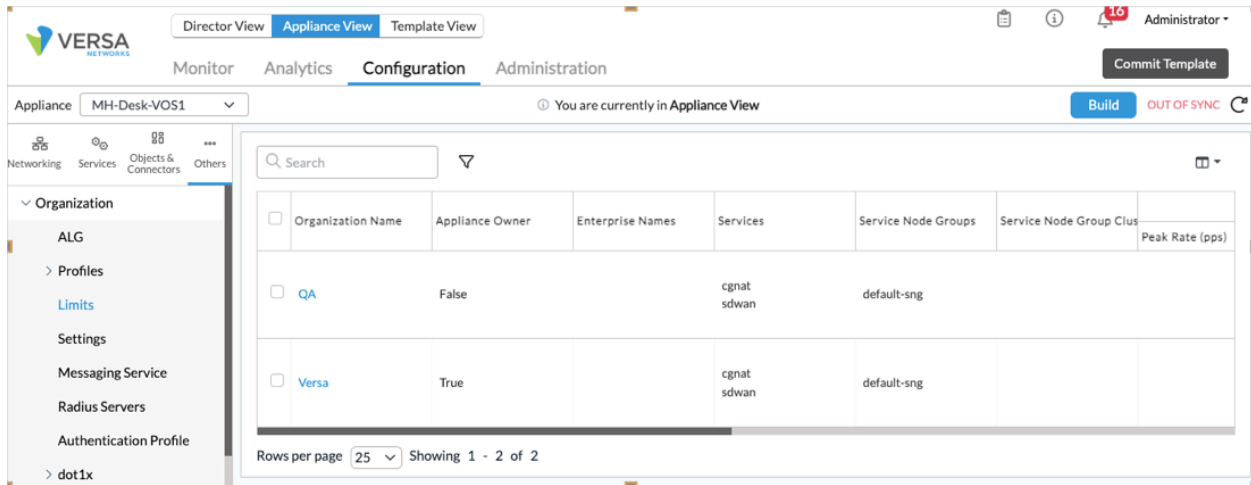
1. In Director view:
 - a. Click Appliance view. The Select Appliance popup window displays.
 - b. Select an organization in the Organization field.
 - c. Click an appliance name. The view changes to Appliance View.
2. Select the Configuration tab in the top menu bar.
3. Select Others > Service Nodes > Service Node Groups in the left menu bar. The main pane displays the service node groups that are already configured.



4. Ensure that SD-WAN or TDF, or both, is listed in the Services column for the service node group. If neither is listed, click the name of the service node group and then add one or both services. For more information, see [Configure Service Node Groups](#).
5. If you added a service in Step 4, refresh the browser window.

To verify that SD-WAN or TDF is enabled for the organization:

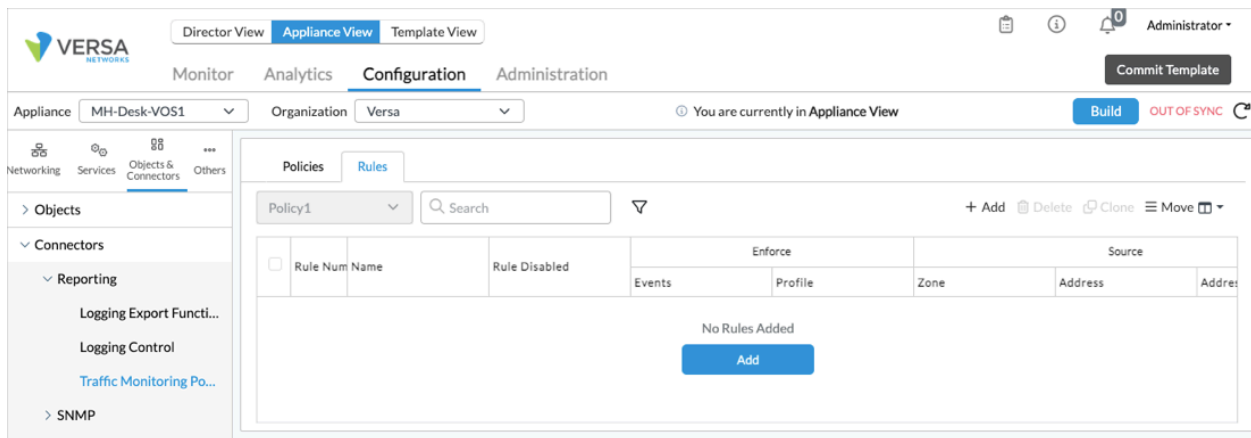
1. In Director view:
 - a. Click Appliance view. The Select Appliance popup window displays.
 - b. Select an organization in the Organization field.
 - c. Click an appliance name. The view changes to Appliance View.
2. Select the Configuration tab in the top menu bar.
3. Select Others > Organization > Limits in the left menu bar. The main pane displays the organizations that are already configured.



4. Ensure that SD-WAN or TDF, or both, is listed in the Services column for the organization. If neither is listed, click the name of the service node group and then add one or both services. For more information, see [Configure Organization Limits](#).
5. If you added a service in Step 4, refresh the browser window.

To enable TCP monitoring and configure historical APM:

1. In Director view:
 - a. Click Appliance view. The Select Appliance popup window displays.
 - b. Select an organization in the Organization field.
 - c. Click an appliance name. The view changes to Appliance View.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Connectors > Reporting > Traffic Monitoring Policy in the left menu bar.



4. Select the Rules tab in the horizontal menu bar.
5. Click an existing rule or click the Add icon. The Add/Edit Rules popup window displays.

Add Rules [Close]

General | Source | Destination | Headers/Schedule | Applications/URL | Enforce

Name *

Description

Tags

☐ Disable Rule

OK Cancel

6. Select the Application/URL tab.

Add Rules [Close]

General | Source | Destination | Headers/Schedule | Applications/URL | Enforce

Applications

<input type="checkbox"/>	Application List	+ New Application + New Filter + New Group +
Application List Not Configured		

URL Categories

<input type="checkbox"/>	URL Category List	+ New URL Category +
URL Category List Not Configured		

OK Cancel

7. In the Application List field, click the  Add icon, and then select an application.

8. Repeat Step 7 to add additional applications to the table.

9. Click OK.

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

Add Rules

General

Source

Destination

Headers/Schedule

Applications/URL

Enforce

Flow Logging Setting

☐ Start

☐ End

☐ Start and End

☐ Interim

☒ Never

LEF Profile

--Select--

▼

☐ Default Profile

+ LEF Profile

☐ Send to Netflow Collector

Web Monitoring

LEF Profile

--Select--

▼

☐ Default Profile

+ LEF Profile

☐ Send SASE Web Data

Performance Monitoring

LEF Profile

--Select--

▼

☐ Default Profile

+ LEF Profile

☐ 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

LEF Profile

--Select--

▼

☐ Default Profile

+ LEF Profile

☐ Send DNS Metadata

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/SD-WAN_Configuration/Advanced_SD-W...

Updated: Wed, 23 Oct 2024 08:11:33 GMT

Copyright © 2024, Versa Networks, Inc.

10

Field	Description
Performance Monitoring (Group of Fields)	
◦ LEF Profile	Select a LEF profile. APM logs are exported to the destination associated with the LEF profile.
◦ Default Profile	Click Default Profile to use the default LEF profile. APM logs are exported to the destination associated with the LEF profile.
◦ TCP Monitoring	<p>Click to configure the VOS device to report APM statistics for all applications and application groups matching the rule.</p> <p>For Releases 22.1.1 and later, selecting this option also enables monitoring of non-TCP based applications and is part of enabling live APM monitoring. For more information, see Configure Live APM, below.</p>

11. Click OK.

Configure Live APM

For Releases 22.1.1 and later.

To configure live APM reporting, enable TCP monitoring as described in [Configure Historical APM](#), above.

Configure MOS Monitoring

To include MOS monitoring for real-time transport protocol (RTP) and real-time transport control protocol (RTCP) in live APM metrics, ensure that you configure real-time flow quality and enable monitoring and that you set a reporting interval. The recommended interval is 2 through 5 seconds. For more information, see [Configure MOS Score Monitoring](#).

APM can provide live monitoring for applications that report a MOS score, even if they are not TCP based, including Webex, Zoom, and generic RTP- or RTCP-based applications.

View Historical APM Metrics

For logs exported to Analytics clusters, you view historical APM metrics on Analytics dashboards.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/SD-WAN_Configuration/Advanced_SD-W...

Updated: Wed, 23 Oct 2024 08:11:33 GMT

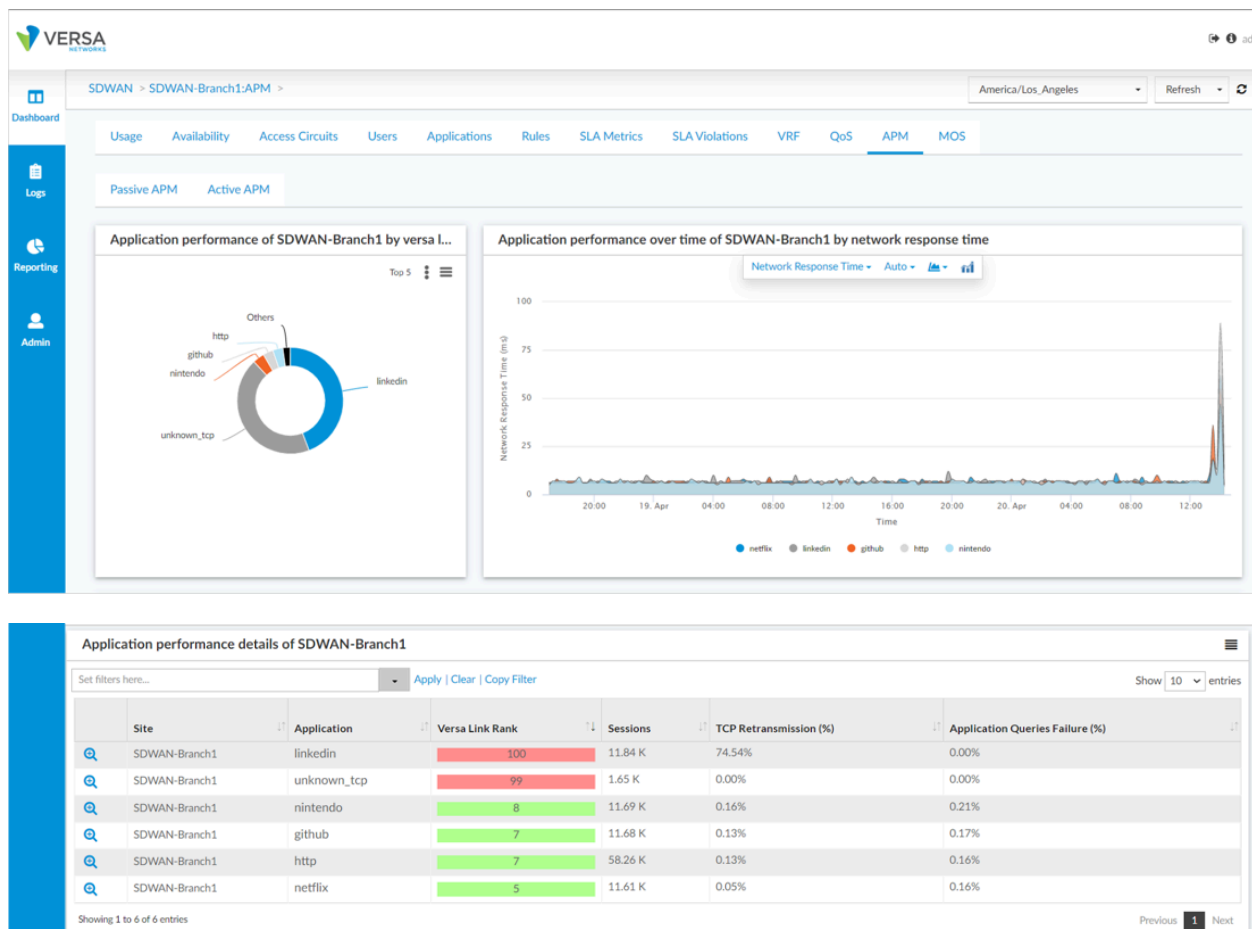
Copyright © 2024, Versa Networks, Inc.


For Releases 22.1.1 and later, to view the passive APM dashboard:

1. In Director view, select the Analytics tab.
2. Select Dashboard > SD-WAN, and then from the third drop-down menu select an individual VOS device.
3. Select APM > Passive APM to display the following items. Note that passive APM refers to historical APM and active APM refers to SaaS application monitoring. For information about configuring SaaS application performance monitoring, see [Configure SaaS Application Monitoring](#).

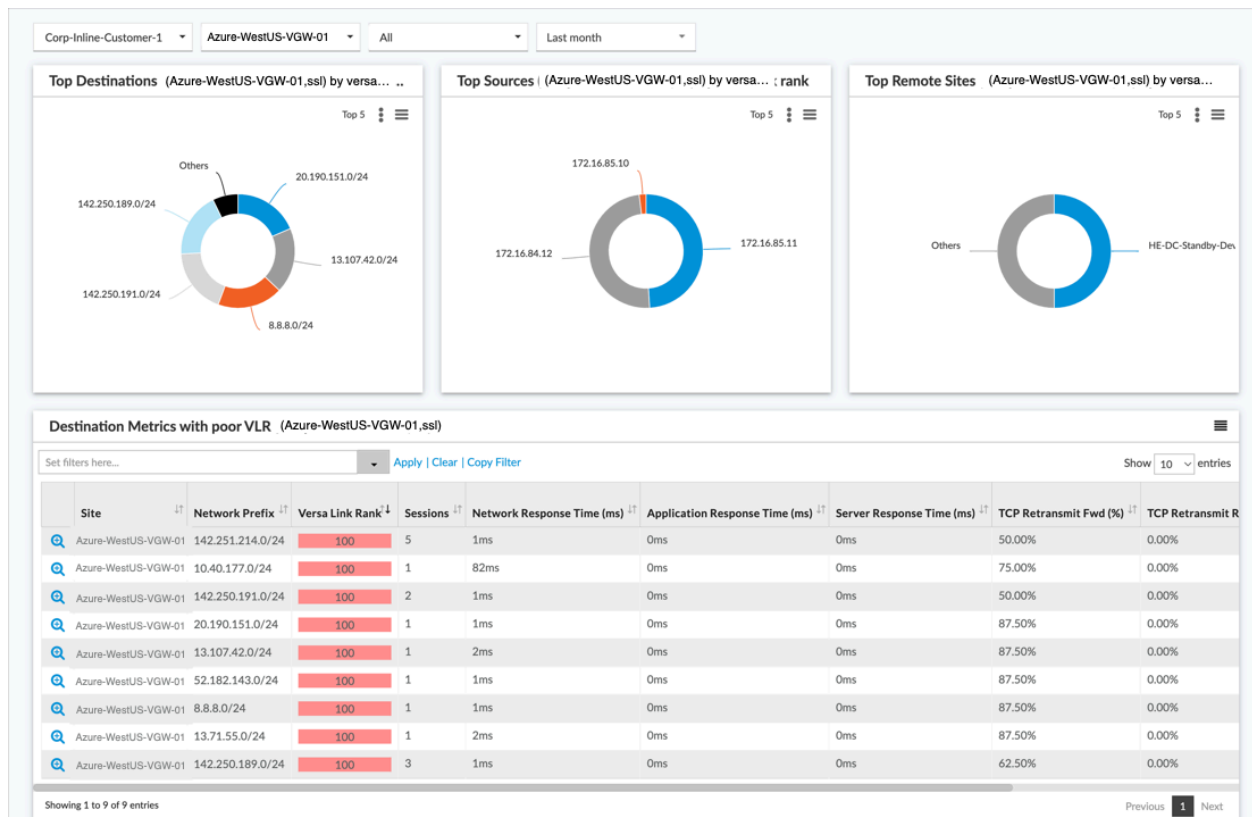
- Application Performance of *device* (chart)
- Application Performance Over Time of *device* (chart)
- Application Performance Details of *device* (table)

For example, the following screen displays passive APM items for device SDWAN-Branch1. The Application Performance of SDWAN-Branch1 chart displays the top five applications with poor VLR, the Application Performance Over Time of SDWAN-Branch1 chart displays application performance by network response time, and the Application Performance Details of SDWAN-Branch1 table displays the VLR and other statistics for each application.



4. In the Application Performance Details of *device* table, click the  Zoom icon to display an application's performance by source, destination, and remote site as well as detailed metrics. The screen displays the following items:
- Top Destination (*device, application*) (chart)
 - Top Sources (*device, application*) (chart)
 - Top Remote Sites (*device, application*) (chart)
 - Destination Metrics With Poor VLR (*device, application*) (table)
 - Remote Site Metrics With Poor VLR (*device, application*) (table)
 - Performance Monitoring (*device, application*) (table)

For example, the following screen displays passive APM details for the ssl application for device Azure-WestUS-VGW-01.



Remote Sites Metrics With Poor VLR (Azure-WestUS-VGW-01,ssl)

Set filters here...

▼ Apply | Clear | Copy Filter

Show 10 ▼ entries

Site	Remote Site	Versa Link Rank	Sessions	Network Response Time (ms)	Application Response Time (ms)	Server Response Time (ms)	SDWAN Delay (ms)	SDWAN Loss (%)
Azure-WestUS-VGW-01		100	29	4ms	0ms	0ms	0ms	0.00%
Azure-WestUS-VGW-01	HE-DC-Standby-Device	100	1	82ms	0ms	0ms	0ms	0.00%

Showing 1 to 2 of 2 entries

Previous 1 Next

Performance Monitoring (Azure-WestUS-VGW-01,ssl)

Set filters here...

▼ Apply | Clear | Copy Filter

Show 10 ▼ entries

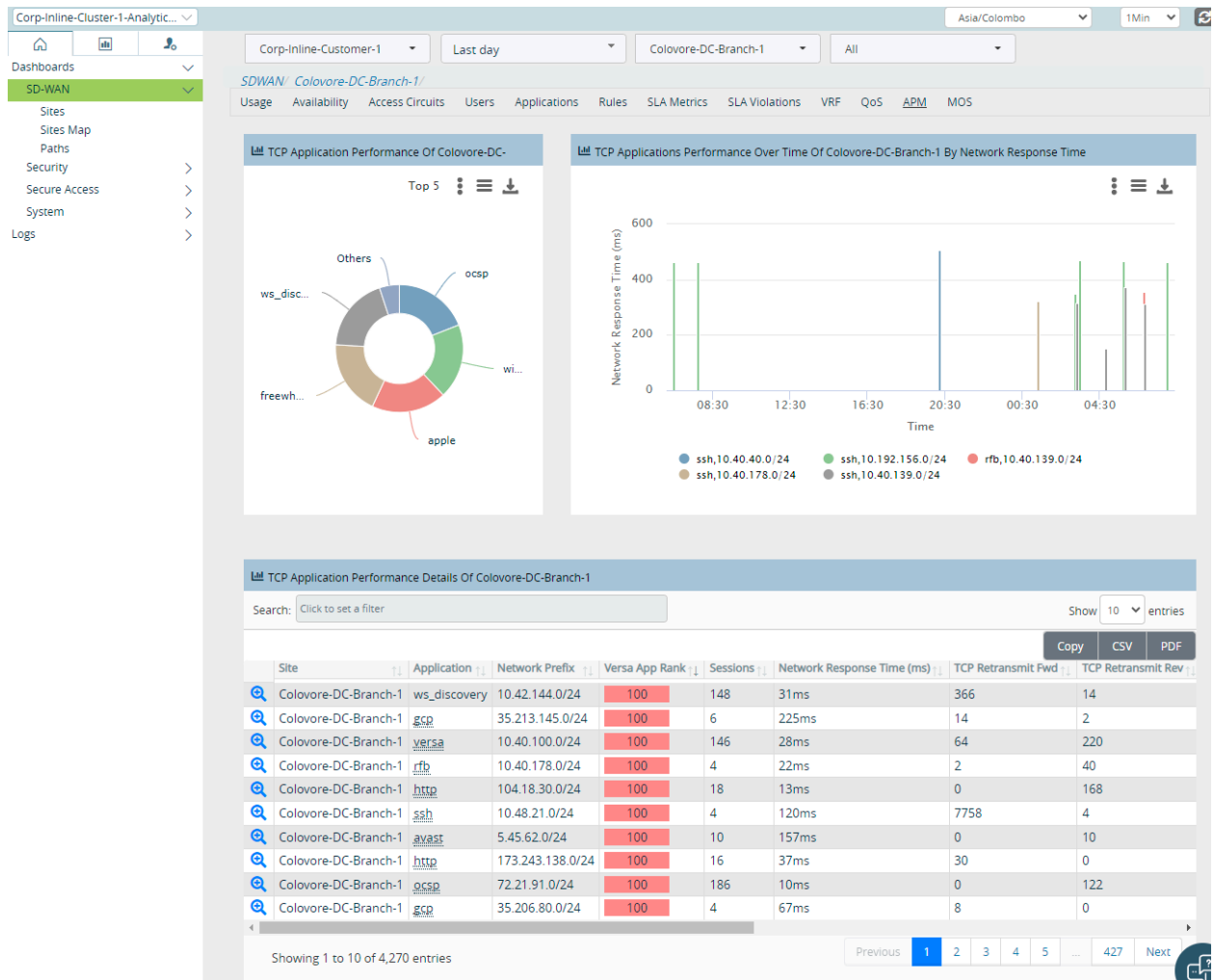
Site	Access circuit	Remote Site	Application	Network Prefix	Users	Versa Link Rank	Sessions	Network Response Time (ms)	Application Response Time (ms)	Server Response Time (ms)
Azure-WestUS-VGW-01	Internet-1		ssl	13.71.55.0/24	172.16.84.12	100	1	2ms	0ms	0ms
Azure-WestUS-VGW-01	Internet-1		ssl	20.190.151.0/24	172.16.84.12	100	1	1ms	0ms	0ms
Azure-WestUS-VGW-01	Internet-1		ssl	52.182.143.0/24	172.16.84.12	100	1	1ms	0ms	0ms
Azure-WestUS-VGW-01	Internet-1		ssl	8.8.8.0/24	172.16.84.12	100	1	1ms	0ms	0ms
Azure-WestUS-VGW-01	Internet-1		ssl	13.107.42.0/24	172.16.84.12	100	1	2ms	0ms	0ms
Azure-WestUS-VGW-01	Internet-1		ssl	142.251.214.0/24	172.16.84.12	100	5	1ms	0ms	0ms
Azure-WestUS-VGW-01	Internet-1		ssl	142.250.191.0/24	172.16.84.12	100	2	1ms	0ms	0ms
Azure-WestUS-VGW-01	Internet-1	HE-DC-Standby-Device	ssl	10.40.177.0/24	172.16.85.11	100	1	82ms	0ms	0ms
Azure-WestUS-VGW-01	Internet-1		ssl	142.250.189.0/24	172.16.84.12	100	3	1ms	0ms	0ms
Azure-WestUS-VGW-01	Internet-1		ssl	52.115.63.0/24	172.16.85.10	4	4	14ms	0ms	0ms

Showing 1 to 10 of 16 entries

Previous 1 2 Next

For Releases 20.3.x and 21.x.x., to view the APM dashboard:

1. In Director view, select the Analytics tab.
2. Select Dashboard (Home) > Dashboards > SD-WAN, and then from the third drop-down menu select an individual VOS device.
3. Select the APM tab to display the following items:
 - TCP Application Performance of *device* (chart)
 - TCP Application Performance Over Time of *device* (chart)
 - TCP Application Performance Details of *device* (table)



In the TCP Application Performance Details of *device* table, the Versa Application Rank column indicates the application's performance with a unitless numeric ranking and a color:

- Green
 - Rank—0 through 33.3
 - Performance—Good
- Yellow
 - Rank—33.3 through 66.3
 - Performance—Medium
- Red
 - Rank—66.3 and higher
 - Performance—Poor

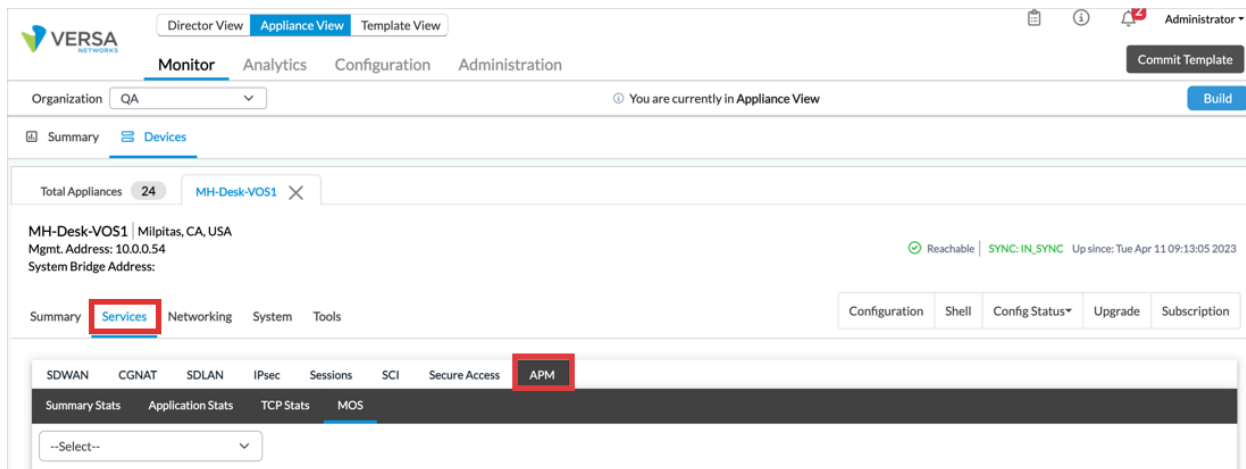
View Live APM Metrics

For Releases 22.1.1 and later.

You view the live APM metrics for a VOS device from the Monitor tab on the Director node. The values displayed represent the APM metrics for the last two minutes.

To display live APM metrics:

1. In Director view:
 - a. Click Appliance view. The Select Appliance popup window displays.
 - b. Select an organization in the Organization field.
 - c. Click an appliance name. The view changes to Appliance View.
2. Select the Monitor tab. The following screen displays.



3. Select Services > APM.
4. Select an application from the drop-down menu in the main pane.
5. Select an APM-related tab to display the live APM metrics for the application.
 - Summary Statistics tab
 - Application Statistics tab
 - TCP Statistics tab
 - MOS tab

Supported Software Information

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

- Releases 20.2.3 adds the ability to view the Versa application rank.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/SD-WAN_Configuration/Advanced_SD-W...

Updated: Wed, 23 Oct 2024 08:11:33 GMT

Copyright © 2024, Versa Networks, Inc.

- Release 22.1.1 supports APM monitoring of non-TCP-based applications, live monitoring of APM metrics, application performance score, and HTTP/HTTPS metrics.

Additional Information

[Configure Log Export Functionality](#)

[Configure MOS Score Monitoring](#)

[Configure Organization Limits](#)

[Configure Real-Time Monitoring](#)

[Configure SaaS Application Monitoring](#)

[Configure SD-WAN Policy](#)

[Configure Service Node Groups](#)