



Traces

- [Feature history of traces, on page 1](#)
- [Exporting traces, on page 1](#)
- [SD-WAN Analytics triggered NWPI Trace, on page 3](#)
- [View Trace Instances, on page 3](#)
- [View and Manage Trace Information, on page 3](#)
- [Flow Path and Metrics, on page 4](#)
- [Insight, on page 5](#)

Feature history of traces

Table 1: Feature History

Feature Name	Release Information	Feature Description
Export and import traces	Cisco Catalyst SD-WAN Control Components Release 20.18.1	If you perform a trace and find a network issue, you can export the trace information to analyze externally. For example, the information may be useful for troubleshooting as part of a Cisco Technical Assistance Center (TAC) case. You can import a saved trace to view the details in Cisco SD-WAN Manager.

Exporting traces

If you perform a trace and find a network issue, you can export the trace information to analyze externally. For example, you can send the exported information to the Cisco Technical Assistance Center (TAC) for analysis. Similarly, you can save trace information for internal use.

File format

Exporting a trace creates a .tar.gz archive containing a set of JSON files. While you can view these in any desired tool, it is most useful to import a saved trace into Cisco SD-WAN Manager to view the trace details.

Export a trace

Procedure

- Step 1** From the Cisco SD-WAN Manager menu, choose **Tools > Network-wide Path Insights**.
- Step 2** In the table of traces, adjacent to a trace, click **...**
- Step 3** Choose any one action:
- **Download:** SD-WAN Manager downloads the trace as a .tar.gz file containing a set of JSON files.
 - **Attach to TAC Case:** Upload the trace to open a Cisco service case for troubleshooting, using the SR number of the case.
-

Import a trace

Procedure

- Step 1** From the Cisco SD-WAN Manager menu, choose **Tools > Network-wide Path Insights**.
- Step 2** Click **Imported Traces** to view a list of imported traces.
- Step 3** Click **Import Trace**.
- Step 4** Follow the instructions to upload a trace file.
- The uploaded trace file appears in the table on the **Imported Traces** page.
-

View an imported trace

Procedure

- Step 1** From the Cisco SD-WAN Manager menu, choose **Tools > Network-wide Path Insights**.
- Step 2** Click **Imported Traces** to view a list of imported traces.
- Step 3** Choose an action available in the table.
- **Insight Summary:** View a summary of the trace.
 - **View Insights:** View the details of the trace.
 - Delete a trace from the table.
-

SD-WAN Analytics triggered NWPI Trace

From Cisco Catalyst SD-WAN Manager Release 20.18.1, NWPI Traces can be automatically triggered using SD-WAN Analytics.

Prerequisites to enable SD-WAN Analytics triggered NWPI Trace

1. In Cisco SD-WAN Manager, go to **Settings > Data Collection & Statistics** and enable **Cloud Services**.
2. In Cisco SD-WAN Manager, go to **Monitor > Network-Wide Path Insight > Administration Settings** and click **Allow Analytics to create traces and tasks via API**.

SD-WAN Analytics-triggered traces are typically named in a `[trigger reason] Auto Triage - [timestamp]` format.



Note Enable **Upload Traces and Tasks to the Cloud** to upload the NWPI trace to the SD-WAN Analytics cloud. You can see the trace's storage location in the trace table. The location can be local stored, cloud stored, or both local and cloud stored.

View Trace Instances

The path trace instances appear with unique trace IDs in the **Trace History** area (in releases before Cisco vManage Release 20.6.1) or in the **Trace** area (in Cisco vManage Release 20.6.1 and later releases). Information about each instance is also displayed, including its state and the actions that you can perform.

From Cisco Catalyst SD-WAN Manager Release 20.12.1, the **Trace** area includes the following tabs:

- **All Trace**: Provides information about the traces that you start manually.
- **Auto-On Task**: Provides information about the traces that are generated by an auto-on task.

View and Manage Trace Information

You can perform the following actions in the **Trace History** area or **Trace** area:

- In releases before Cisco vManage Release 20.6.1:
 - To stop an active trace, click **Stop**. If you have specified the trace duration, the trace stops automatically when the timer expires.
 - To navigate to the **Flow Path and Metrics** section, click **Detail**.
- From Cisco vManage Release 20.6.1:

Action	Procedure	Tab (from Cisco Catalyst SD-WAN Manager Release 20.12.1)
Stop a trace that is in progress.	Click Stop in the Action column for the trace, and then click Confirm in the Stop Trace dialog box.	All Trace and Auto-On Task
Delete a trace that is completed.	Click Delete in the Action column for the trace, and then click Confirm in the Delete Trace dialog box.	All Trace and Auto-On Task
Display trace-level insight summary information (from Cisco vManage Release 20.9.1).	See Insight Summary .	All Trace and Auto-On Task
Display detailed information about the flows in a trace in the Insight area.	Click Insight Summary for the trace in the Trace Name column.	All Trace
View the filters and settings for a trace.	Click the name of the trace in the Trace Name column.	All Trace
View information about the source of a trace.	Click the corresponding value in the Src Site column.	All Trace
View information about the applications or application groups that a trace monitors.	Click the corresponding value in the Application/App Group column.	All Trace
View the status of a trace and error messages, if any, that have been generated.	Click the corresponding value in the Trace State column.	All Trace
View statistics for a task (from Cisco Catalyst SD-WAN Manager Release 20.12.1).	Click the name of the corresponding task.	Auto-On Task
View the filters and settings for a trace in a task (from Cisco Catalyst SD-WAN Manager Release 20.12.1).	Expand the task that you want, and then click the name of the trace in the Trace Name column.	Auto-On Task

Flow Path and Metrics

This section applies to releases before Cisco vManage Release 20.6.1.

In the **Flow Path and Metrics** section, view bidirectional flow path table with hop-by-hop metrics. You can expand any trace instance in the log to view the following details:

Column	Description
Last Update Time	The flow path instances in running state are refreshed every 10 seconds and the time of the update is displayed.
Flow ID	Flow IDs differentiate two identical flow path instances occurring at different times.
State	This state helps you visualize potential issues with the flow. Only SLA state of the flow is supported.
Direction	Directions could be upstream or downstream. The direction in which the first packet flow is identified is considered as upstream.
Local Color, Remote Color	Local edge (source) and the remote edge (destination) colors indicate different WAN interfaces.
Local Drop(%)	Packet drop on hop's local edge routers.
Remote Drop(%)	Packet drop on hop's remote edge routers (WAN underlay drop on remote edge router excluded)
WAN Drop(%)	Packet loss on WAN from hop's local edge router to remote edge router (includes WAN underlay drop on remote edge router, eg.IPsec Anti-Replay drop.)
Jitter(ms), Latency(ms)	Jitter and latency metrics of the flow. These metrics help with evaluating the application performance in real time.
Total Packets, Total Bytes	For each direction of the flow, total number of packets and total byte count are displayed.

Insight

This section applies to Cisco vManage Release 20.6.1 and later.

Click **View Insight** in the **Actions** column in the list of traces to display detailed information about the flows in the corresponding trace. This detailed information appears in the **Insight** area. The following information is displayed in this area:

- The **DNS Domains** tab is available only when DNS domain discovery is enabled and displays information about each domain that the trace discovers. You can expand any row in the list to display detailed information about the application.

From Cisco vManage Release 20.9.1, click **Discovered Domains** to display information for every domain that the trace discovered but that are not yet traced. Click **Monitored Domains** to display information only for domains that the trace monitored.



Note In Cisco vManage Release 20.6.1 through Cisco vManage Release 20.8.x, the **DNS Domains** tab is called the **Applications** tab.

- (From Cisco vManage Release 20.9.1) The **Applications** tab displays information about applications that were traced. You can expand any row in this list to display bidirectional path information with hop-by-hop metrics for each application.
- The **Active Flows** tab displays information about the flows that are in the Running state. You can expand a flow instance to display bidirectional flow path information with hop-by-hop metrics.
- The **Completed Flows** tab shows information about the flows that are in the Stopped state. You can expand a flow instance to display bidirectional flow path information with hop-by-hop metrics.
- In the **DNS Domains** tab, start or stop flow monitoring of the applications in the selected domain for an active trace. Starting flow monitoring also deploys an HTTP probe (through Cisco vManage Release 20.8.x) or an HTTPS probe (from Cisco vManage Release 20.9.1) for the domain on the WAN. A dialog box indicates that monitoring has started. Monitoring information is displayed in the **Active Flows** and **Completed Flows** tabs.
 - In Cisco vManage Release 20.6.1 through Cisco vManage Release 20.8.x, click **Start Flow Monitor** and **Stop Flow Monitor**, as needed, to start or stop monitoring for the selected domains.
 - From Cisco vManage Release 20.9.1, to start flow monitoring, click **Discovered Domains**, check the corresponding check box for one or more domains to start monitoring, and click **Start Flow Monitor**. In the confirmation dialog box that appears, click **Confirm**. You can change the domain selections in this dialog box before you click **Confirm**.

From Cisco vManage Release 20.9.1, to stop flow monitoring, click **Monitored Domains**, check the check box for each domain for which you want to stop monitoring, and click **Stop Flow Monitor**. In the confirmation dialog box that appears, click **Confirm**.
- Use the **Search** option to find specific flow instances.

From Cisco vManage Release 20.6.1, you also can cut and paste the following keywords to search for flows that include corresponding the events:

- **Local Drop**
- **WAN Loss**
- **TCP Reset**
- **NAT Translation**
- **DPI First Packet Unclassified**
- **SLA Violation**
- **QoS Congestion**
- **WAN Color Inconsistency**
- **Flow Asymmetry**
- **Policy Bypass**

- **Server No Response**
- **AppQoE Diverted**
- **UTD Diverted**

- For completed flows, use the **Filter** option to display only flow instances that meet specified criteria.
- For completed flows, you can limit the display to flows that occurred within a specified period.

In releases through Cisco vManage Release 20.8.x, you can choose a period of 1, 10, or 30 minutes, or 1, 2, or 5 hours. You also can click **Custom** and enter a date and time range.

From Cisco vManage Release 20.9.1, you can drag the ends of the time bar to designate the start and end dates and times for a certain period.

The following sections describe the information that appears for each application and each instance in a flow, and, if DNS domain discovery is enabled, for each domain:

- [DNS Domains Tab, on page 7](#)
- [Applications Tab, on page 8](#)
- [Active Flows and Completed Flows Tabs, on page 10](#)
- [Expanded DNS Domains Information, on page 14](#)
- [Expanded Application Information, on page 15](#)
- [Expanded Flow Instance Information, on page 15](#)



Note The **DNS domains** tab (called **Applications** tab in Cisco vManage Release 20.6.1 through Cisco Manage 20.8.x) is available only when DNS Domain Discovery is enabled for a trace.

DNS Domains Tab

Table 2: DNS Domains Tab (Called Applications Tab in Cisco vManage Release 20.6.1 Through Cisco Manage 20.8.x)

Column	Description
Check box	Check the check box for the domains for which you want monitoring to be enabled or disabled and click Start Flow Monitor or Stop Flow Monitor .
Domain	Name of the domain that the trace discovered.
Update Time	Date and time at which the information was last refreshed. Instances are refreshed every 30 seconds by default.
Application	Name of the application that the trace discovered in the domain.

Column	Description
Insights	From Cisco Catalyst SD-WAN Manager Release 20.18.1, you can click on View in this column to get details about this domain in a side frame.
Application Group or App Group	Name of the application group that the trace discovered in the domain.
VPN Id	Available from Cisco Catalyst SD-WAN Manager Release 20.12.1. Identifier of the VPN in which the application flow was traced.
DNS Server	Destination of DNS packets sent from clients.
DNS Redirect	DNS resolver to which a device redirects DNS traffic if a resolver is configured by a centralized policy or by Cisco Umbrella.
Resolved IP	DNS-resolved IP address for the application.
DNS Transport	Transport type used by the domain.
DNS Egress	Egress interface and type used by the domain.
TTL (sec)	DNS time to live, in seconds.
Request	Number of DNS packets sent.
Monitor State	Status of flow monitoring for the domain.

Applications Tab

Table 3: Applications Tabs (Available from Cisco vManage Release 20.9.1)

Column	Description
Columns Displayed in Cisco vManage Release 20.9.1 through Cisco vManage Release 20.11.x	
Last Update Time	Date and time at which the information was last refreshed. Instances are refreshed every 10 seconds by default.
App Name	Name of the application.
App Group	Application group to which the application belongs.
Upstream Flow Count	Number of upstream flows that were counted for the application.
Downstream Flow Count	Number of downstream flows that were counted for the application.

Column	Description
Upstream Bytes (K)	Number of KBs in the upstream traffic of this application.
Downstream Bytes (K)	Number of KBs in the downstream traffic of this application.
Columns Displayed From Cisco Catalyst SD-WAN Manager Release 20.12.1	
Last Update Time	Date and time at which the information was last refreshed. Instances are refreshed every 10 seconds by default.
App Name	Name of the application.
App Group	Application group to which the application belongs.
VPN Id	Identifier of the VPN in which the application flow was traced.
Total Bytes (K)	Number of KBs in the upstream and downstream flows of this application.
Total packets	Number of packets in the upstream and downstream flows of this application.
KBPS	Number of KBs per second in the upstream and downstream flows of this application during the past minute.
PPS	Number of packets per second in the upstream and downstream flows of this application during the past minute.
Total Flows	Number of flows that were counted for the application.
Active Flows	Flows that had activity during the past 1 minute.
Flow Setup Rate	Average number of new flows per second during the past 1 minute.
Flow Live Time (ms) Max/Min/Avg	Maximum, minimum, and average number of milliseconds of detectable flow activity during the duration of the trace.
Sampled Flows	Number of flows that were sampled in the upstream or downstream traffic of this application. Click the up arrow icon next to the column name to display information for upstream traffic. Click the down arrow icon to display information for downstream traffic.

Column	Description
Sampled Bytes (K)	Number of KBs in the upstream or downstream traffic of this application. Click the up arrow icon next to the column name to display information for upstream traffic. Click the down arrow icon to display information for downstream traffic.

Active Flows and Completed Flows Tabs

Table 4: Active Flows and Completed Flows Tabs

Column	Description
Last Update Time or Start - Update Time	In releases through Cisco vManage 17.8.x: Date and time at which the information was last refreshed. In releases from Cisco vManage 20.9.1: Date and time at which the flow started, and date and time at which the information was last refreshed. Instances are refreshed every 10 seconds by default.
Flow ID	System-assigned identifier of the flow.

Column	Description
Readout	

Column	Description
	<p>Information that the flow contains (error, warning, or information). Click an icon to display detailed information about the flow in a dialog box (in releases before Cisco vManage Release 20.9.1) or a slide-in pane (in releases from Cisco vManage Release 20.9.1). If the flow identifies an application issue, you can use this information to assist with a root-cause analysis.</p> <p>From Cisco Catalyst SD-WAN Manager Release 20.14.1, a Cisco ThousandEyes icon indicates that the flow comes from a Cisco ThousandEyes test.</p> <p>The dialog box or slide-in pane includes the following information:</p> <ul style="list-style-type: none"> • Overview: Includes details about flow asymmetry, bidirectional WAN color inconsistency, QoS congestion, LAN or WAN packet drops, SLA violation, path change, flow reset, SAIE packet classification status, TCP server response, and so on. <p>Note From Cisco Catalyst SD-WAN Manager Release 20.15.1, when the WAN packet drops in a flow, the Cisco SD-WAN Manager displays the percentage of IPsec failures on the hop.</p> <ul style="list-style-type: none"> • Path Insight (available from Cisco vManage Release 20.9.1): Provides information about how a forwarding path was determined for a flow. This information includes the edge router name; destination IP address; IP address lookup and matched route information; route-receiving source protocol, preference, and metrics; flow path-routing candidates; method for deciding the flow path; NAT translation detail; and the flow path used. (You may have to scroll to the bottom of the Path Insight tab to access the horizontal scroll bar.) • Underlay Insight (available from Cisco Catalyst SD-WAN Manager Release 20.14.1): Provides underlay hop information about each overlay hop in the flow. <p>Note In Cisco vManage Release 20.7.x and earlier releases, the SD-WAN Application Intelligence Engine (SAIE) flow is called the deep packet inspection (DPI) flow.</p>

Column	Description
	At the beginning of a trace in a network using Multi-Region Fabric, some Path Insight or Routing Insight information might be missing in the second or subsequent hops for the first few flows.
VPN Id	From Cisco Catalyst SD-WAN Manager Release 20.12.1, identifier of the VPN in which the application flow was traced.
Source IP	Source IP address of the traffic that the trace monitors.
Source Port or Src Port	Source port of the traffic that the trace monitors.
Destination IP	Destination IP address of the traffic that the trace monitors.
Destination Port or Dest Port	Destination port of the traffic that the trace monitors.
Protocol	Protocol of the traffic that the trace monitors.
DSCP Upstream/Downstream	DSCP type that the trace monitors for upstream traffic and downstream traffic.
Application	Application that the trace monitors.
Application Group	Application group that the trace monitors.
Domain	<p>Domain that the flow belongs to.</p> <p>Click a domain name to display the protocol from which the domain was recognized.</p> <p>Note This field shows information only for DNS and HTTPS protocol flows. For other flow types, this field displays Unknown.</p>
ART CND (ms)/SND (ms)	Application response time, in milliseconds, for client network delay (CND) and server network delay (SND).
User	<p>From Cisco Catalyst SD-WAN Manager Release 20.13.1, the username of the user who sends or receives traffic that the trace monitors.</p> <ul style="list-style-type: none"> • A username does not include a domain. For example, if a username is aduser@add.com, the name appears as aduser. • A username appears only if Cisco ISE is integrated with Cisco Catalyst SD-WAN. If Cisco ISE is not integrated, this field displays "Unknown."

Column	Description
User Group	From Cisco Catalyst SD-WAN Manager Release 20.13.1, the name of the Cisco ISE user group to which the user who sends or receives traffic belongs. Note A user group name appears only if Cisco ISE is integrated with Cisco Catalyst SD-WAN. If Cisco ISE is not integrated, this field displays "Unknown."
Security Group Tag	From Cisco Catalyst SD-WAN Manager Release 20.12.1, security group tag that is assigned to the flow.

Expanded DNS Domains Information

Table 5: Expanded DNS Domains Information (Called Expanded Application Information in Cisco vManage Release 20.6.1 Through Cisco vManage 20.8.x)

Column	Description
Egress Interface	Egress interface type used by the domain.
Local Edge, Remote Edge	Names of the local edge (source) and the remote edge (destination) of the flow.
Local Color	Color of the local edge (source) of the flow, which indicates the egress WAN interface.
Remote Color	Color of the remote edge (destination) of the flow, which indicates the ingress WAN interface.
App CND (ms)/App SND (ms)	Application response time, in milliseconds, for client network delay (CND) and server network delay (SND).
HTTP Probe Response Time (ms)	Response time, in milliseconds, of an HTTP probe ping from the device to the application server.
HTTP Probe Loss (%)	Packet loss percentage of an HTTP probe ping from the device to the application server.
Path Score	Path score of an HTTP probe ping from the device to the application server.

Expanded Application Information

Table 6: Expanded Application Information (Available from Cisco vManage Release 20.9.1)

Column	Description
Direction	Direction of the application flow (upstream or downstream). The first packet that the flow identifies is shown as a flow in the upstream direction.
HopIndex	Hop index number for each direction of the application.
Local Edge	Name of the local edge device (source) of the application.
Remote Edge	Name of the remote edge device (destination) of the application.
Local Color	Color of the local edge device (source) of the application, which indicates the egress WAN interface.
Remote Color	Color of the remote edge device (destination) of the application, which indicates the ingress WAN interface.
Local Drop (%), WAN Drop (%), Remote Drop (%) or Local Drop (%), WAN Loss (%), Remote Drop (%)	Packet drop, as measured in the local and remote edge routers. Packet drop is also measured in the complete WAN network.
Jitter (ms), Latency (ms)	Jitter and latency metrics of the application during the past minute. These values help with evaluating the application performance in real time.
ART CND (ms)/SND (ms)	Application response time, in milliseconds, for client network delay (CND) and server network delay (SND) during the past minute.
Total Packets, Total Bytes, or Sampled Total Packets and Sampled Total Bytes	For each direction of the application flow, the total number of packets and the total byte count of packets.

Expanded Flow Instance Information

Table 7: Expanded Flow Instance Information

Column	Description
Direction	Direction of the flow (upstream or downstream). The first packet that the flow identifies is considered to flow in the upstream direction.

Column	Description
HopIndex	Hop index number for each direction of the flow.
Local Edge	Name of the local edge (source) of the flow.
Remote Edge	Name of the remote edge (destination) of the flow.
Local Color	Color of the local edge (source) of the flow, which indicates the egress WAN interface.
Remote Color	Color of the remote edge (destination) of the flow, which indicates the ingress WAN interface.
Local Drop (%), WAN Drop (%), Remote Drop (%) or Local Drop (%), WAN Loss (%), Remote Drop (%)	Packet drop, as measured in the local and remote edge routers. The packet drop is also measured in the complete WAN network.
Jitter (ms), Latency (ms)	Jitter and latency metrics of the flow. These values help with evaluating the application performance in real time.
ART CND (ms)/SND (ms)	Application response time, in milliseconds, for client network delay (CND) and server network delay (SND).
Total Packets, Total Bytes	For each direction of the flow, the total number of packets and the total byte count of packets.
Queue Id	Identifier of the QoS queue for the flow.
QDepthLimit/Max/Min/Avg	Limit, maximum, minimum, and average values of the QoS queue depth for the flow.