Cisco Nexus Dashboard Insights Traffic Analytics, Release 6.4.1 - For Cisco NDFC or Standalone NX-OS

Table of Contents

First Published: 2024-03-04

Last Modified: 2024-03-13

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

New and Changed Information

The following table provides an overview of the significant changes up to the current release. The table does not provide an exhaustive list of all changes or the new features up to this release.

Table 1. New Features and Changed Behavior in the Cisco Nexus Dashboard Insights

Feature	Description	Release	Where Documented
Traffic Analytics	Traffic Analytics enables to monitor your network's latency, congestion, and drops.	6.4.1	Traffic Analytics

This document is available from your Cisco Nexus Dashboard Insights GUI as well as online at www.cisco.com. For the latest version of this document, visit Cisco Nexus Dashboard Insights Documentation.

Traffic Analytics

Traffic Analytics

Traffic Analytics enables to monitor your network's latency, congestion, and drops.

Traffic Analytics automatically discovers services running in your network by matching well-know Layer 4 ports to their corresponding service endpoint categories. Nexus Dashboard Insights then assess service performance based on thresholds you define for the following metrics:

- Latency: Measures the overall time in microseconds it takes a packet to go from one place to another.
- Congestion: Measures network bandwidth utilization and quality of service (QoS) activation mechanisms to determine if a service is experiencing network congestion.
- Drops: Measures the percentage of dropped versus transmitted packets considering factors such as CRC errors, faulty cables and other devices.

An anomaly is raised if there is any deviation in the performance metrics such as latency, congestion, and drops. Performance score is calculated for each conversation and aggregated to Service Endpoint or Endpoint level to raise anomalies.

Performance score is calculated based on the following:

- Congestion - Consistent congestion avoidance active between endpoints is calculated.
- Latency - Deviation from measured baseline is calculated.
- Drops - Directly correspond to an issue with the conversation or service.

Using Traffic Analytics you can

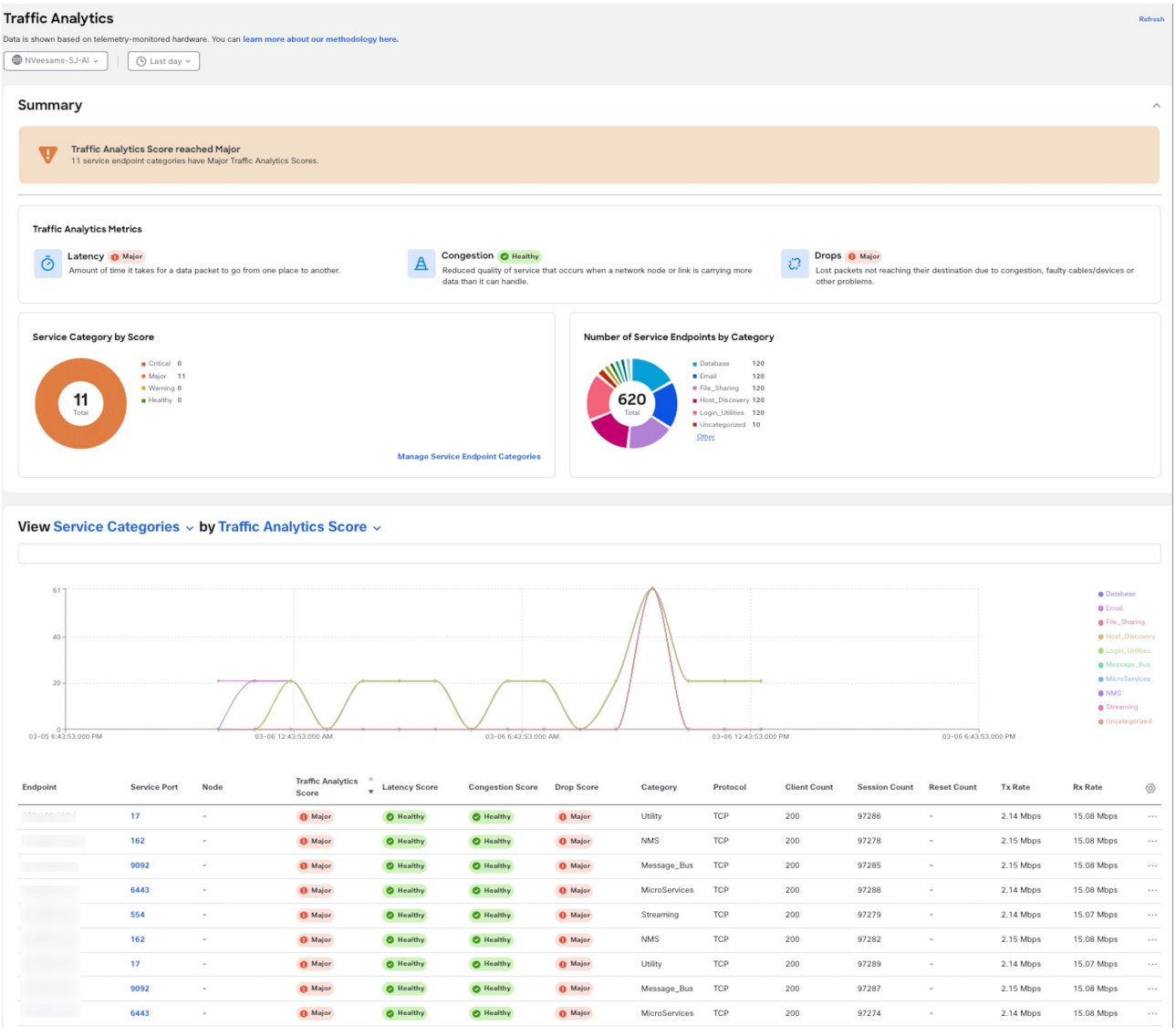
- Monitor traffic pervasively.
- Report performance issues using anomalies raised for performance metrics.
- Sort top talking services and clients and determine the top talkers in the system.
- Determine the SYN or RST counts per service.
- Troubleshoot conversations or flows on-demand.

A conversation is defined as a 4-tuple including source IP address, destination IP address, destination port, and protocol. In case a single client establishes multiple communication flows initiated by multiple source ports towards a service endpoint, all related statistics would be aggregated as a single entry in the Traffic Analytics table. A service endpoint is defined by an IP address, a port, and a protocol.

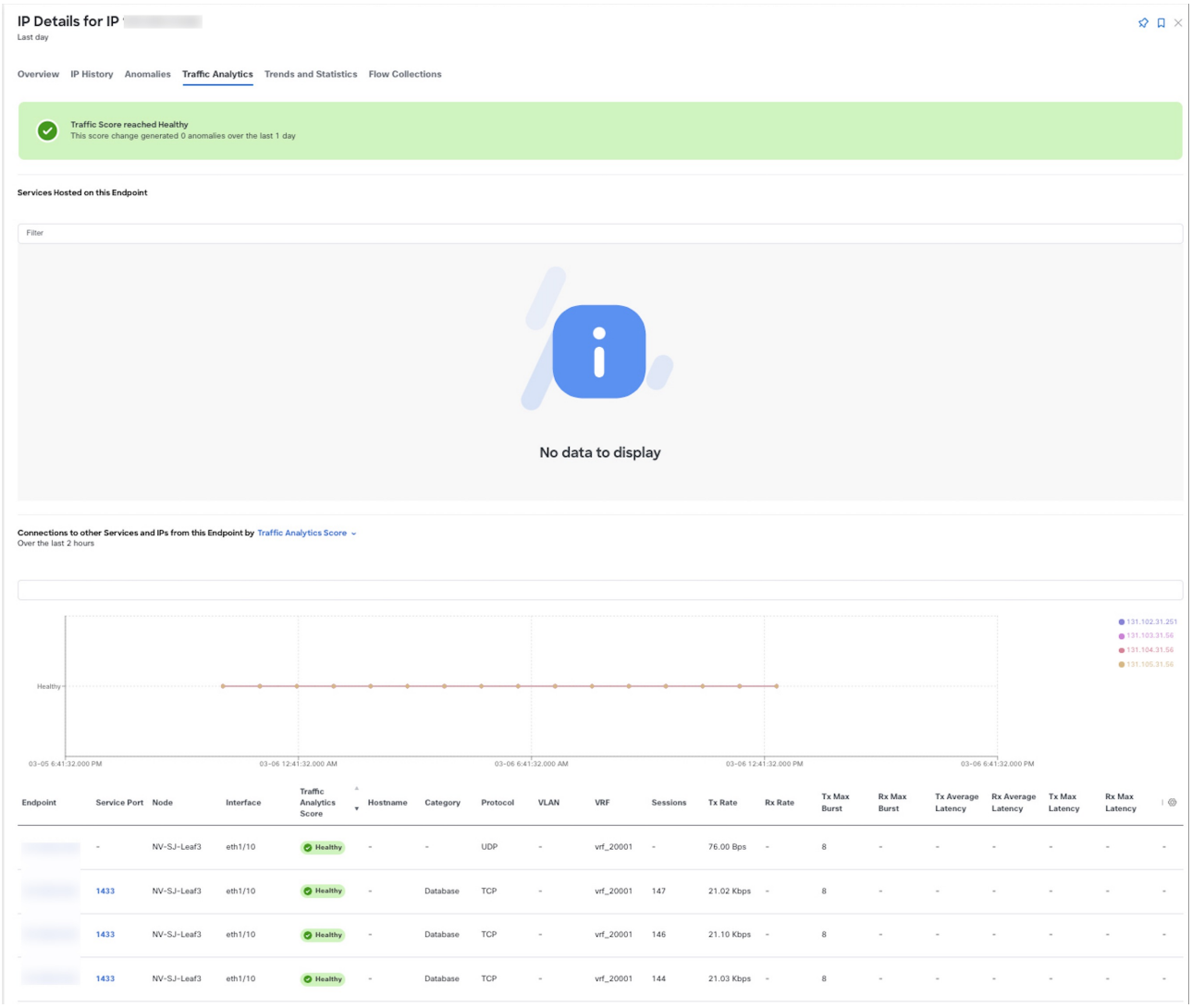
An anomaly is raised once conversation limit is exceeded. Navigate to **Admin** > **System Settings** > **Flow Collection**. In the Traffic Analytics status for the last hour area, you can view if the conversation rate approaches or exceeds the limits. You can also view if there are any Traffic Analytics record drops.

Guidelines and Limitations

- Traffic Analytics is supported on Cisco NX-OS release 10.4(2)F and later.
- Traffic Analytics is not supported for Layer 4 to Layer 7 Services.
- Traffic Analytics is not supported for Multi-Site.
- Before enabling Traffic Analytics on NDFC sites with Netflow configuration, you must add a freeform policy to the leaf switches. This ensures that if Traffic Analytics is disabled from Nexus Dashboard Insights, Netflow configuration is not removed.
- Multicast is not supported for Traffic Analytics.
- Traffic Analytics is only available for traffic flows between IPv4/IPv6 endpoints that are contained within the fabric. These endpoints should be visible in the **Manage** > **Sites** > **Connectivity** > **Endpoints** page. If the source or destination endpoint exists outside the fabric, then the Traffic Analytics flow will not be displayed in the Traffic Analytics table.
- Traffic Analytics configurations or export is not supported on Cisco Nexus 9500 modular chassis, however flow troubleshoot jobs is supported for FX platform switches and Cisco Nexus 9500 modular chassis.
- Traffic Analytics Report only displays TCP services and TCP clients/conversations. Navigate to **Analyze** > **Analysis Hub** > **Traffic Analytics** to view this information.



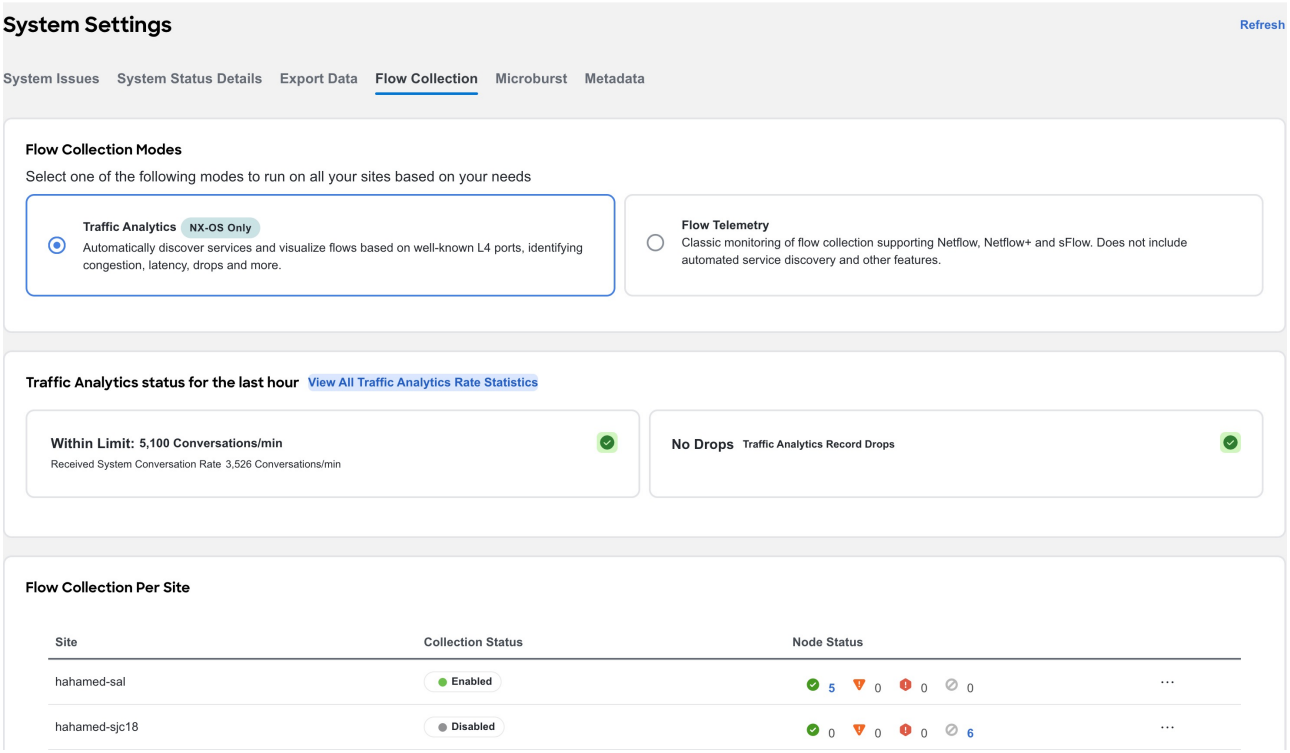
- UDP and ICMP flow/conversation reports will be only shown at the endpoint level. Navigate to **Manage** > **Sites**. Select a site. Click **Connectivity** > **Endpoints** > **Endpoint** > **Traffic Analytics** to view this information.



- Traffic Analytics may display partial data when the VRF instance is configured with the new L3VNI mode. For more information about the new L3VNI mode, see the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide.

Configure Traffic Analytics

1. Navigate to **Admin** > **System Settings** > **Flow Collection**.
2. In the **Flow Collection Mode** area, select **Traffic Analytics**.



3. In the **Flow Collection per Site** table, select the site.
4. Click the ellipse icon and then click **Enable** to enable Traffic Analytics.

> If flow telemetry is already enabled on the site, you must first disable flow telemetry for all the sites before enabling Traffic Analytics.

5. You can view the Flow Collection status for each node in the Node Status column.
   - Green – Flow collection is successfully enabled.
   - Red – Flow collection is not enabled.
   - Orange – Flow collection is partially enabled.
   - Grey – Flow collection is not supported or data cannot be found. If a switch is in disabled state, it will included in the Grey category.
6. In the Traffic Analytics Status For The Last Hour area you can see the number of conversations that are over limit and Traffic Analytics drops. You must make sure that you do not exceed the maximum conversation limit. If you exceed the maximum conversation limit you will see drops in flows records and it will impact the visibility.
7. Click **View All Traffic Analytics Rate Statistics** to view the statistics for each node in a site.

Apply Traffic Analytics Configuration

For NDFC fabric in Monitored mode, Nexus Dashboard Insights will not deploy Traffic Analytics configuration to all switches in the fabric. You must apply the Traffic Analytics configuration to every switch.

1. Navigate to **Admin** > **System Settings** > **System Status Details**.
2. Select a site.
3. Click the ellipse icon and then click **Expected Configuration**.

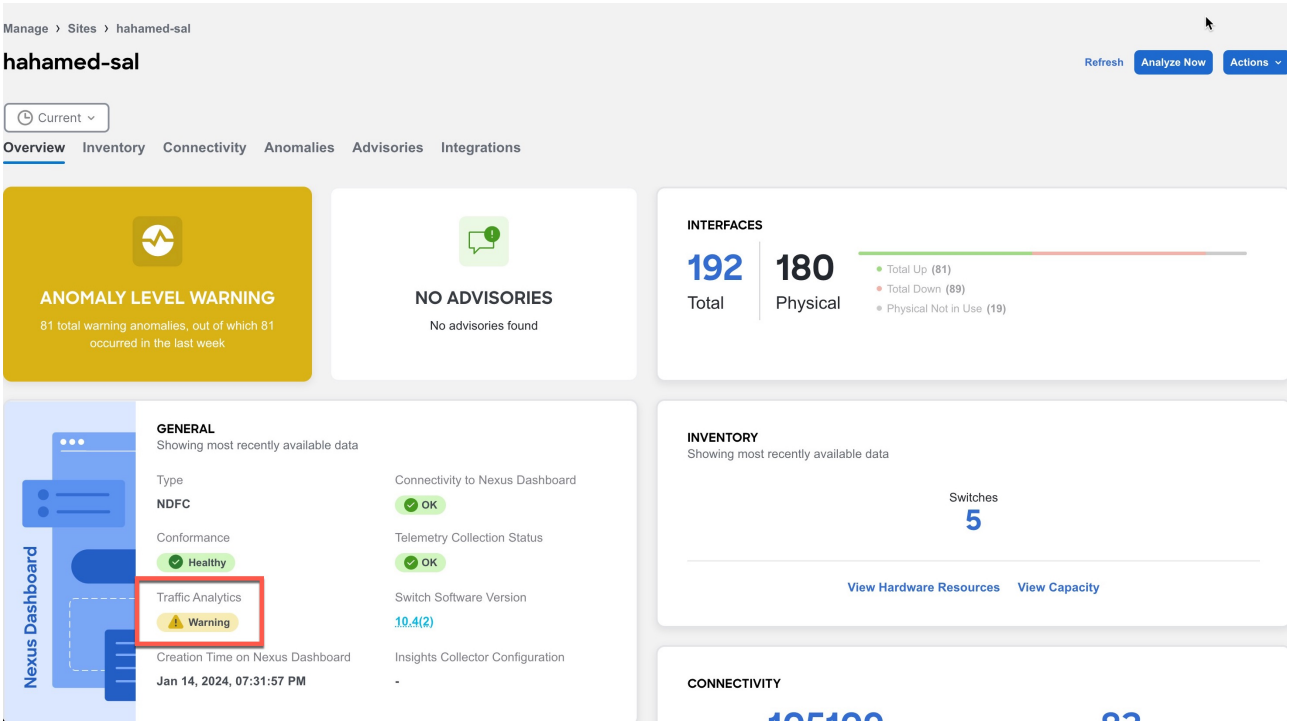
4. From the **Expected Configuration** area, you can view and copy configurations under **Software Telemetry** and **Flow Telemetry**.
5. Using the command line, log in to the switch.
6. Enter the following commands:

```
switch# configure terminal
switch(config)# copy running-config startup-config
```

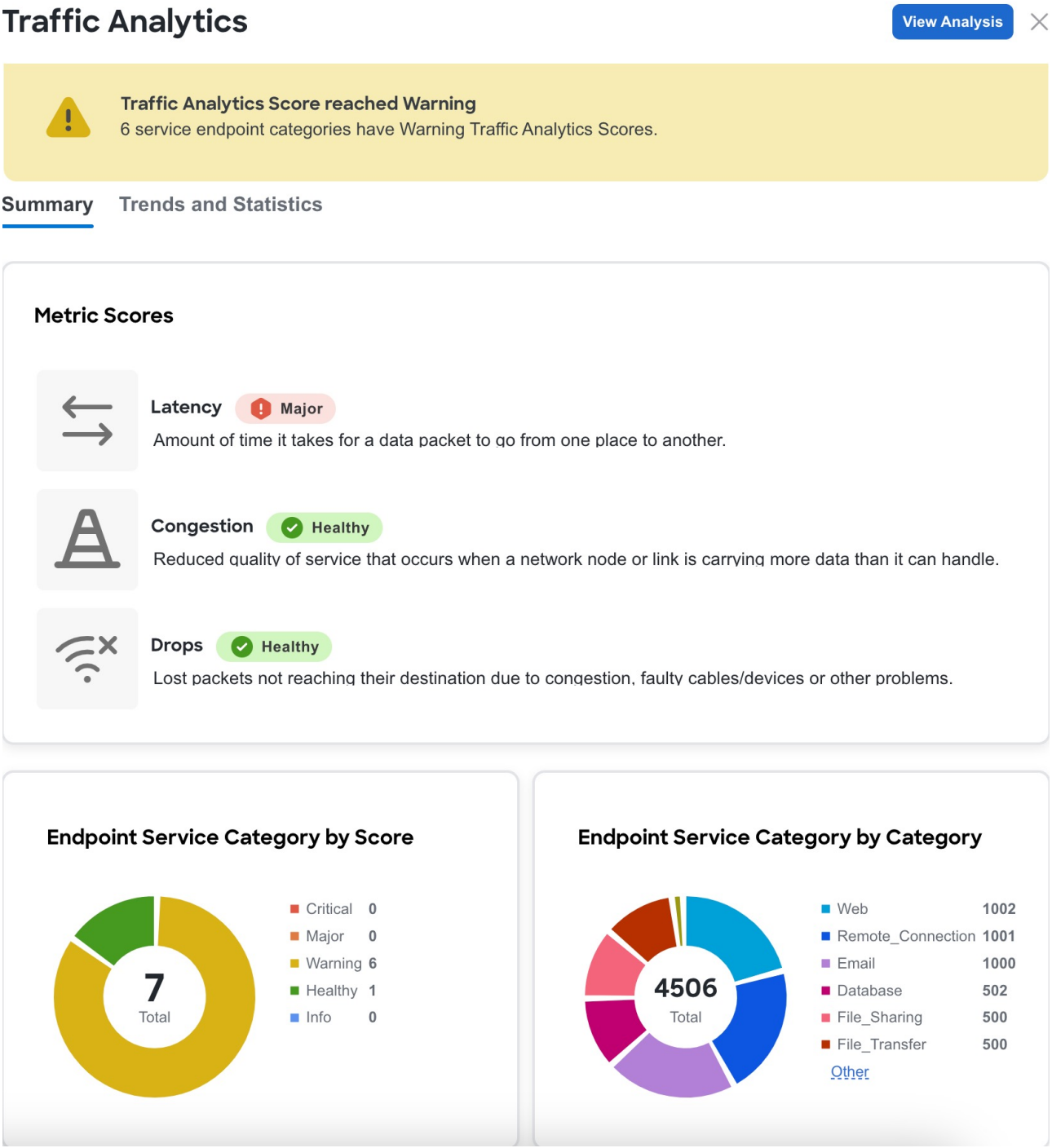
View Traffic Analytics

View Traffic Analytics for an Individual Site

1. Navigate to **Manage** > **Sites**.
2. Click site name.



3. Select a time range from the dropdown menu. By default the Current time (last 2 hours) is selected.
4. In the General area, click **Traffic Analytics** to view Traffic Analytics details for that site. In the Traffic Analytics page all the information is grouped as service categories for that site.



5. The Summary area displays the Traffic Analytics Score and how the metrics is determined. You can view the traffic profile for endpoint service category by score and category.
6. Click **Trends and Statistics** to view Traffic profile, Top Endpoint Service Score Changes, and Top Endpoint Categories.

Traffic Analytics

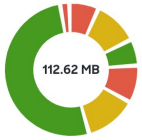
View Analysis

Traffic Analytics Score reached Warning
6 service endpoint categories have Warning Traffic Analytics Scores.

Summary | Trends and Statistics

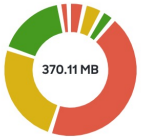
Traffic Profile

Tx



- Database 6.85 MB
- Email 11.69 MB
- File_Sharing 5.91 MB
- File_Transfer 9.36 MB
- Other

Rx



- Database 8.69 MB
- Email 11.70 MB
- File_Sharing 5.91 MB
- File_Transfer 177.97 MB
- Other

Top Endpoint Service Score Changes

Categories	Score Change	Affecting Metric
Database	Warning → Healthy	Latency ↘
File_Transfer	Warning → Healthy	Latency ↘
Remote_Connection	Warning → Healthy	Latency ↘
Email	Warning → Warning	Latency →
File_Sharing	Warning → Warning	Latency →
RoCE	Unknown → Healthy	-
Web	Warning → Warning	Latency →

7 items found

Rows per page 10 | 1

Top Endpoint Categories by Rx Latency

Categories	Average	Trend
File_Transfer	2.01 us	↗ 3%
Remote_Connection	2 us	↗ 1%
Database	2 us	↘ 0%
Email	2 us	↘ 0%
File_Sharing	2 us	→
RoCE	0 us	→
Web	2 us	↘ 0%

a. In the Traffic Profile area you can view the traffic amount for the endpoint service category.

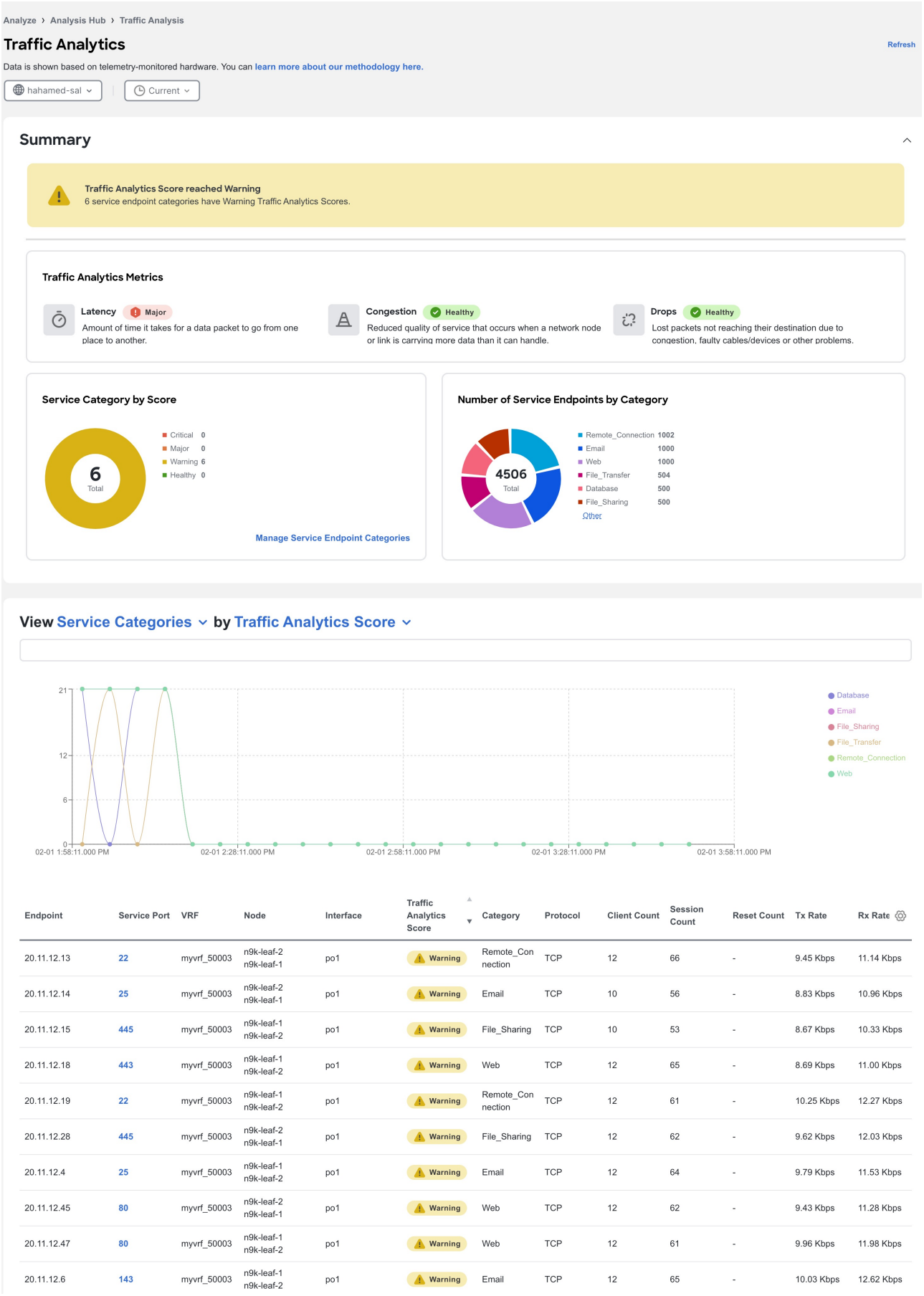
b. In the Top Endpoint Service Score Changes area, you can view the anomaly score change across 2 hours and the metrics (such as latency, congestion, drops) affecting the score change.

c. In the Top Endpoint Categories by area you can see the top categories by Rx and Tx Latency, Congestion Score, and Drop Score.

7. Click **View Analysis** to view Traffic Analytics for all the sites.

View Traffic Analytics for all Sites

1. Navigate to **Analyze** > **Analyze Hub** > **Traffic Analytics**.
2. Select a site from the drop-down menu.
3. Select a time range from the dropdown menu. By default the Current time (last 2 hours) is selected. When you select the Current time, any issues observed in the Traffic Analytics score over the last 2 hours is displayed.

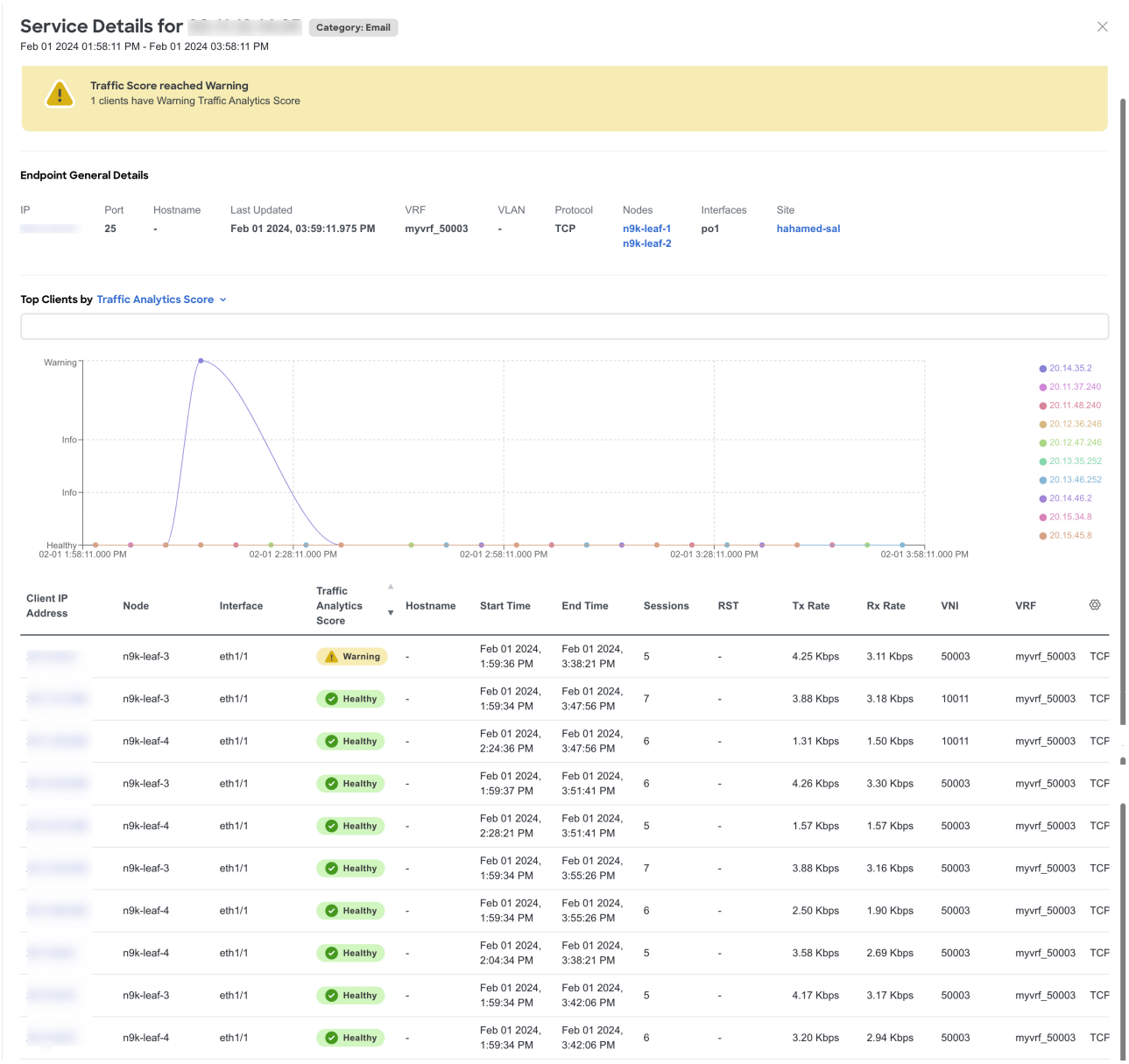


Endpoint	Service Port	VRF	Node	Interface	Traffic Analytics Score	Category	Protocol	Client Count	Session Count	Reset Count	Tx Rate	Rx Rate
20.11.12.13	22	myvrf_50003	n9k-leaf-2 n9k-leaf-1	po1	Warning	Remote_Connection	TCP	12	66	-	9.45 Kbps	11.14 Kbps
20.11.12.14	25	myvrf_50003	n9k-leaf-2 n9k-leaf-1	po1	Warning	Email	TCP	10	56	-	8.83 Kbps	10.96 Kbps
20.11.12.15	445	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	File_Sharing	TCP	10	53	-	8.67 Kbps	10.33 Kbps
20.11.12.18	443	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	Web	TCP	12	65	-	8.69 Kbps	11.00 Kbps
20.11.12.19	22	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	Remote_Connection	TCP	12	61	-	10.25 Kbps	12.27 Kbps
20.11.12.28	445	myvrf_50003	n9k-leaf-2 n9k-leaf-1	po1	Warning	File_Sharing	TCP	12	62	-	9.62 Kbps	12.03 Kbps
20.11.12.4	25	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	Email	TCP	12	64	-	9.79 Kbps	11.53 Kbps
20.11.12.45	80	myvrf_50003	n9k-leaf-2 n9k-leaf-1	po1	Warning	Web	TCP	12	62	-	9.43 Kbps	11.28 Kbps
20.11.12.47	80	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	Web	TCP	12	61	-	9.96 Kbps	11.98 Kbps
20.11.12.6	143	myvrf_50003	n9k-leaf-1 n9k-leaf-2	po1	Warning	Email	TCP	12	65	-	10.03 Kbps	12.62 Kbps

4. The Summary area displays the Traffic Analytics Score and how the metrics are determined. Next you can view the information for a Service Endpoint Category by Score and Category. Service endpoint categories consists of ports that have been assigned to categories based on standard networking defaults and any categories you may have created. These categories are dynamic and

can be updated any time. See Manage Service Endpoint Categories.

5. Next use the drop-down list to view the Service Categories or Service Endpoints information for attributes such as Traffic Score, Congestion Score, Latency Score, Drop Score, and others in a graphical format. When you select Service Endpoints, you can also view the top 10 endpoints for various attributes such as Traffic Analytic Score, Latency Score, Congestion Score, Drop Score, Session Count, Reset Count, TX Rate, and Rx Rate. For Current Time, when you select view **Service Categories** for **Traffic Analytics Score**, you can use the graph to view the transition between healthy and unhealthy score.
6. In the Traffic Analytics table, you can view the Service Categories or Service Endpoints information. The Traffic Score information for service categories or endpoints is a combination of congestion score, latency score, and drop score. When the score is calculated, congestion score has the lowest weighage, and drop score has the highest weighage.
   a. You can hover on the Traffic Analytics Score column to view the Traffic Analytics Score breakdown for the service.
   b. Use the search bar to filter by Service Categories or Service Endpoints values.
   c. Click the gear icon to configure the columns in the Traffic Analytics table.
7. Click **Service Port** to view additional details for the particular service.



a. In the Overview area you can view the endpoint details and client details such as top clients and conversation between a client and service.

   i. In the Endpoint General Details, click Client IP Address to view endpoint details. You can view all the services hosted on that endpoint and connections to other services and IP addresses from this endpoint.

   ii. Use the drop-down list to view the information for Top Clients by Traffic Analytics Score, Latency Score, Drop Score and others.

   iii. In the Clients table, hover on the Traffic Analytics Score to view the Traffic Analytics Score breakdown for that service.

b. In the Trends and Statistics area you the view the trends for values such clients, service, latency and others for that service.

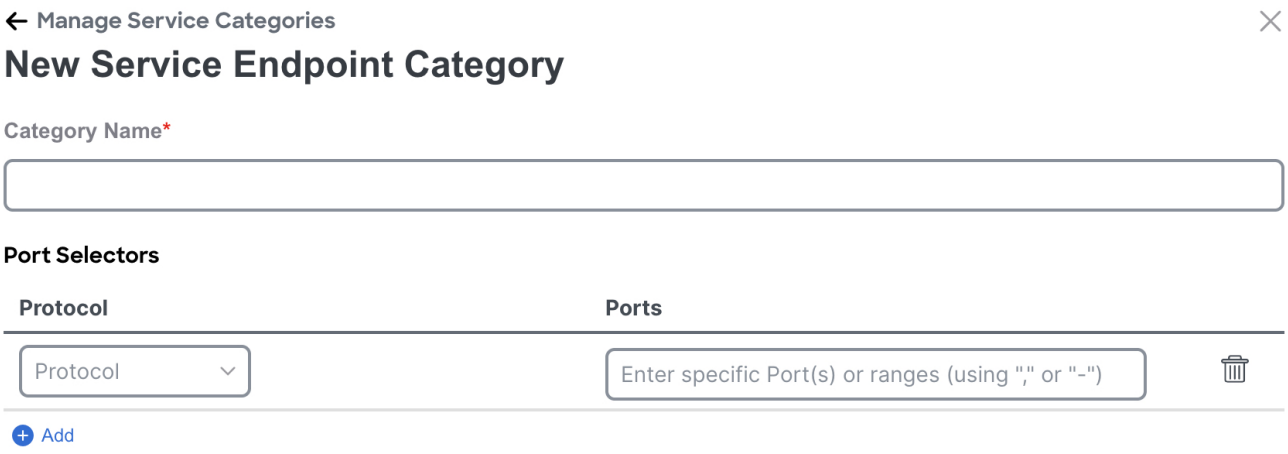
c. In the Anomalies area, you can view the anomalies for the particular service endpoint based on traffic score.

d. In the Flow Collections area, you can view the flow collections for that service.

Manage Service Endpoint Categories

In the Manage Service Endpoint Categories area you can view the ports that have been assigned to categories based on standard networking defaults and any categories you may have created. If a port has not been assigned to a category, you can assign it to one of the existing categories or create a new category. This helps you to organize and manage your network ports more efficiently.

1. Navigate to **Analyze** > **Analyze Hub** > **Traffic Analytics**.
2. Select a site from the drop-down menu.
3. Select a time range from the dropdown menu. By default the Current time (past 2 hours) is selected.
4. In the Service Category by Score area click **Manage Service Endpoint Categories**.
5. To create a new category, click **New Categories**.

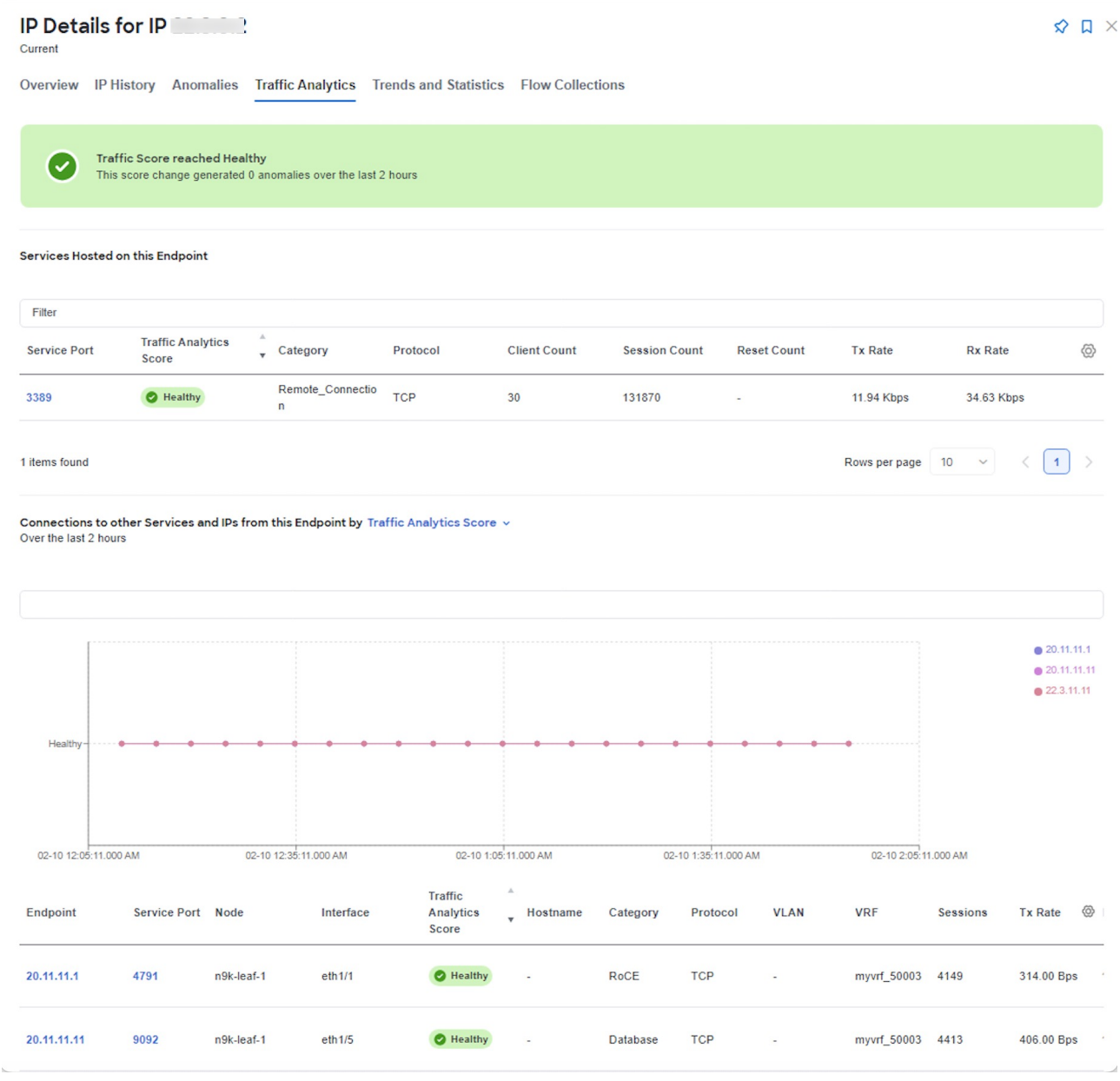


6. Enter the name of the category.
7. From the Protocol drop-down list, select the protocol.
8. In the Ports field, enter the ports or port range.

9. Click **Add** to add additional protocols.
10. Click **Save**.
11. To edit a category, click the ellipse icon and select edit.
    a. Edit the values and click **Save**.
12. To delete a category, click the ellipse icon and select delete.
    a. Click **Confirm**.

View Traffic Analytics for Endpoints

1. Navigate to **Manage** > **Sites**.
2. Click site name.
3. Navigate to **Connectivity** > **Endpoints**.
4. In the Endpoint table click an IP address.
5. In the IP Details page, click **Traffic Analytics** to display the Traffic Analytics view for endpoints.



Flow Troubleshoot Workflow

The Flow Troubleshoot workflow enables you to collect all the flow records between two endpoints when the Traffic Analytics score is unhealthy for a service endpoint. Nexus Dashboard Insights allows you to specify the duration for flow collection and then collect records between specific endpoints for the specified duration. As a result you can view the path visualization, 5-tuple flow information, and any issues seen on individual flows.

1. Navigate to **Analyze** > **Analyze Hub** > **Traffic Analytics**.
2. Select a site from the drop-down menu.
3. Select a time range from the dropdown menu. By default the Current time (last 2 hours) is selected.
4. In the Service Endpoint table, select the endpoint with an unhealthy Traffic Analytics score and click **Service Port**.
5. In the Service Details page, select the Client IP address with an unhealthy Traffic Analytics score. Click the ellipse icon and choose **Start Flow Collection**.
6. Select the duration to collect flow records for a specific time period. Click **Start**.
7. Click **Flow Collections** to view the status.
8. After the Collection Status displays Completed, click **View Records** to view the flow record details for that specific service endpoint.

To view the Flow Collection for all the service endpoints for a site, navigate to **Manage** > **Sites**. Select a site. Click **Connectivity** > **Flow Collections**.

Flow troubleshoot may not show all the nodes through which packet traverses for each record in the following scenarios:

- When there are flow drops in Nexus Dashboard Insights
- When there are table collisions in the hardware

Copyright