# Analyze Degraded Services

This section explains how Service Health monitoring helps to deep dive into the degraded services and subservices, and drill down to the root cause of the service degradation.

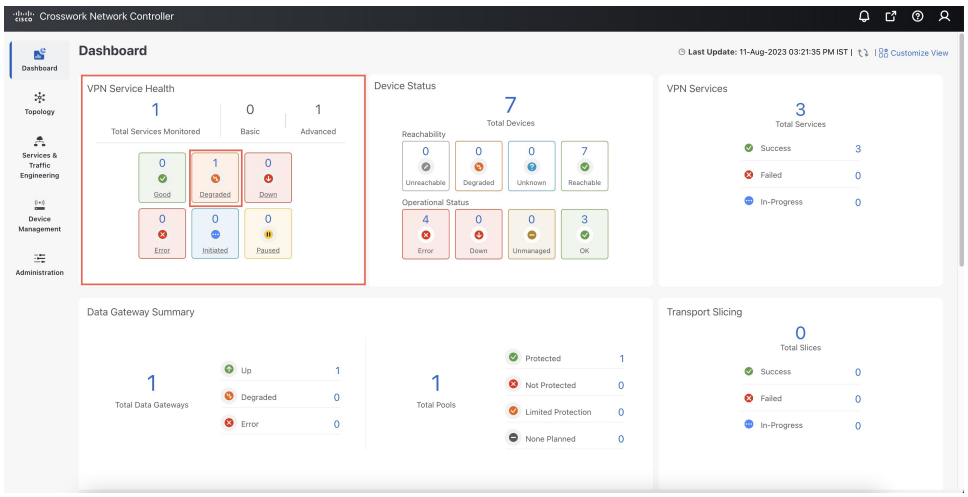


# View Monitored Services

You can view the monitored services in any of the following ways:

### From the Crosswork Home Page

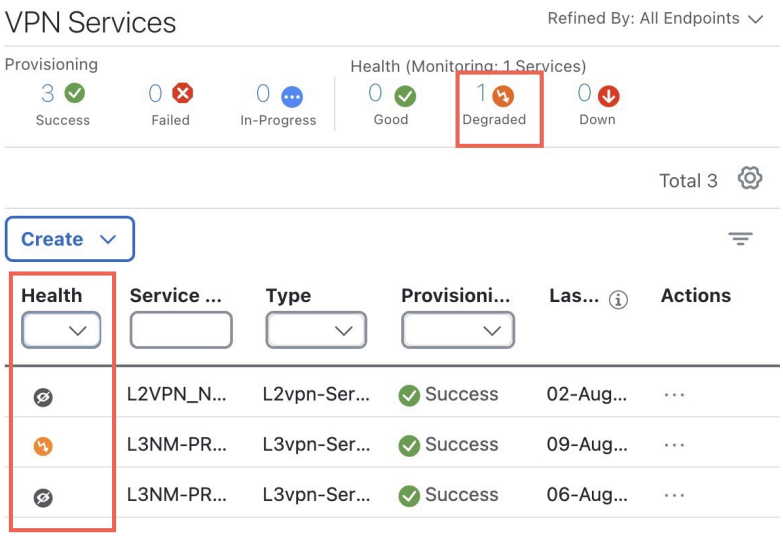
You will see the **VPN Service Health** dashlet on the Crosswork Home Page. This dashlet provides an overview of all the VPN services that are being monitored. From the dashlet you can click any of the status indicators to be taken to the **VPN Services** page with a filter set for the status you selected. To view the degraded services, click the **Degraded** box within the dashlet. This will take you to the VPN Services page, where only the degraded VPN services are displayed.




### From the VPN Services Page

From the main menu, choose **Services & Traffic Engineering** > **VPN Services**. All the VPN services are listed on this page. The degraded services show an orange icon in the **Health** column.

You can filter the services by their health (Down, Degraded, Good, Paused, Initiated, Error, Unmonitored). You can also click the Degraded tab in the Health tab in this page to filter and view only the Degraded services.



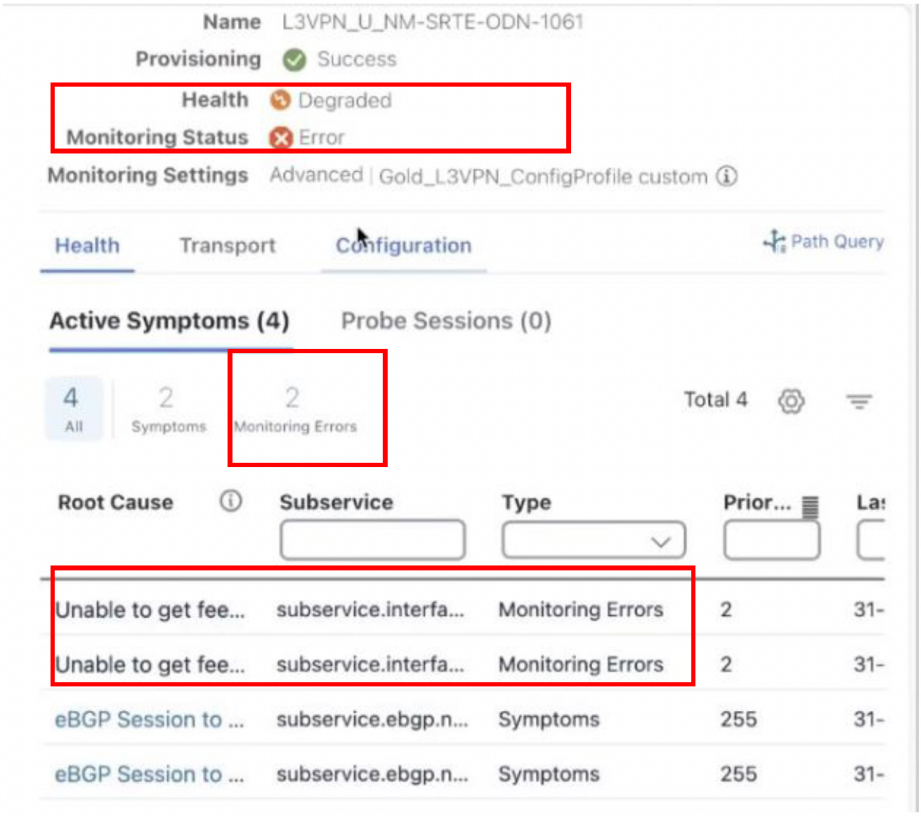

To clear the filter, click **X** next to the designated filter appearing in the space at the top of the column. To remove all the filters and to show all the VPN services, click the **X** icon in the Filters field above the table.

**Note** If a service is not yet being monitored, a gray icon is displayed in the Health column. To enable monitoring for such a service, click ⋯ and select **Start Monitoring**. For more information, see Start Service Health monitoring.

# View Monitoring Status of a Service

You can view the **Monitoring Status** of a service from its **Service Details** page.

From the main menu, choose **Services & Traffic Engineering** > **VPN Services**. Locate the service that you are interested in and under the **Actions** column, click **View Details**. This page displays the **Monitoring Status** and the **Health** status of the service.




Monitoring status for a service can be either **Healthy** or **Error**.

- **Healthy**: This means the end-to-end flow of monitoring the service is working as expected and Service Health is able to evaluate the health of the service successfully.
- **Error**: This means Service Health is unable to monitor the current health of the service due to component failures, operational errors or device errors, and the health status that is displayed is the last known health of the service. You can filter monitoring errors using the mini dashboard or the filters.

**Note** Monitoring errors reported on account of device health do not affect the overall health of the service.

In the Historical Graph, Events of Significance (EoS) are displayed for monitoring errors as well. If the service is healthy but there are monitoring errors, a green warning icon is displayed. However, if the service is degraded and there are monitoring errors, then an orange warning icon is displayed. Clicking these icons provides you with the details in the symptoms table with type as **Monitoring Errors**.

**Note** The Historical Graph displays monitoring errors only when the Monitoring Errors setting is enabled via API. There is no option to enable this setting from the UI in this release. Once this setting is enabled, the system starts to log these monitoring errors as Events of Significance and display them in the historical graph. Refer to the API documentation on Cisco Devnet for more information.

# Identify Active Symptoms and Root Causes of a Degraded Service

By analysing the root cause of reported active symptoms and impacted services, you can determine what issues must be addressed first to maintain a healthy setup and what requires further inspection and troubleshooting.

**Note** L3VPN service monitoring is supported on Cisco IOS XR devices and not on Cisco IOS XE devices. For an L3VPN service being monitored, if a provider and devices are deleted, and then added again, the monitoring status will remain in the degraded state with a monitoring status as Monitoring error. Stop and restart the service monitoring to recover from this error.

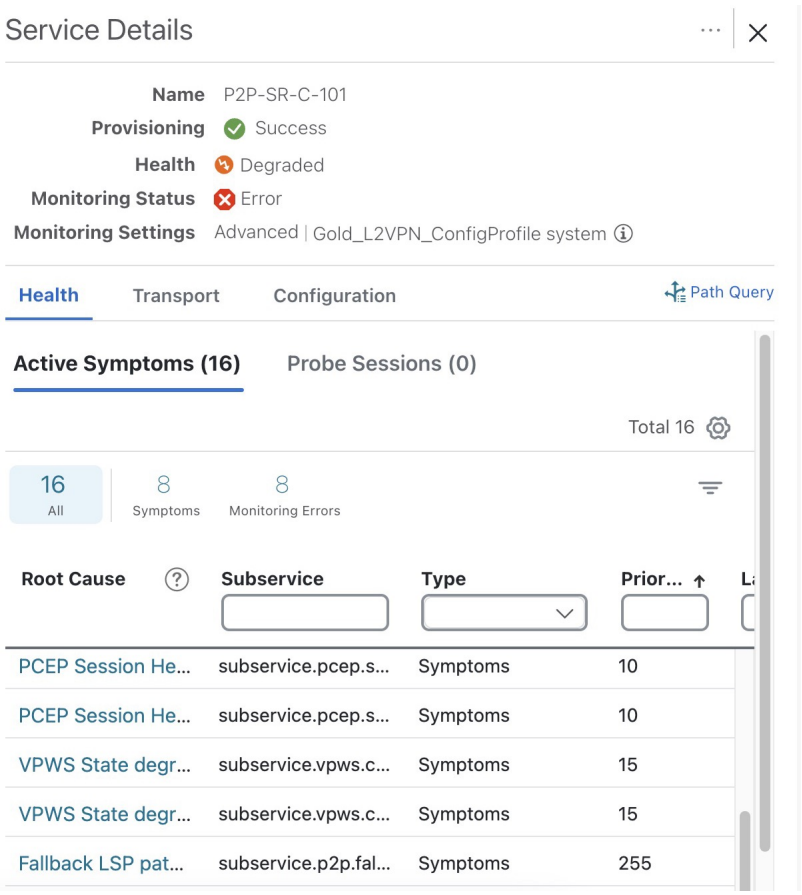
To view the active symptoms and root causes for a service degradation:

**Step 1** From the main menu, choose **Services & Traffic Engineering** > **VPN Services**. The service assurance dependency graph opens on the left side of the page and the table opens on the right side.

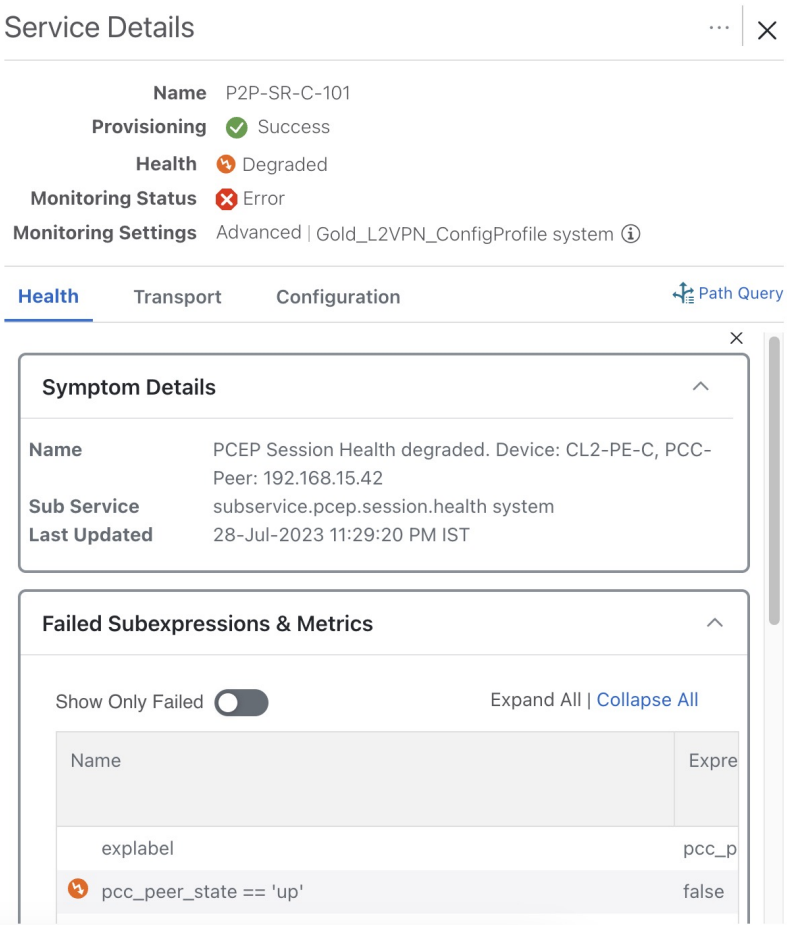
**Step 2** In the Actions column, click  and click **View Details**. The Service Details panel appears on the right side.

**Step 3** Select the Health tab and click the **Active Symptoms** tab. The Active Symptoms table displays **Active Symptoms** and **Monitoring Errors** by default. To filter the table to show only the Active Symptoms, either click the **Symptoms** tab in the mini dashboard above the table or select **Symptoms** from the filter box under the **Type**. The table now shows a filtered list containing only the Active Symptoms.

Review the Active Symptoms for the degraded service (including the Root Cause, Subservice, Type, Priority, and Last Updated details).




**Step 4** Click on a Root Cause and view both the **Symptom Details** and the **Failed Subexpressions & Metrics** information. You can expand or collapse all of the symptoms listed in the tree, as required. In addition, use the **Show Only Failed** toggle to focus only on the failed expression values.




**Step 5** Click the **Transport** and **Configuration** tabs and review the details provided.

**Step 6** Click **X** in the top-right corner to return to the VPN Services list.

### Related Information

- To monitor the VPN services using Assurance Graph capabilities and inspect any services or related nodes that are degraded, see Identify Root Causes Using Assurance Graph, on page 7.
- To identify the issues with the degraded services within a specific time range, use the Last 24Hr Metrics. For details, see Identify Root Causes Using Last 24Hr Metrics, on page 10.
- To identify a service health issue by examining the collection jobs, see View Collection Jobs, on page 14.

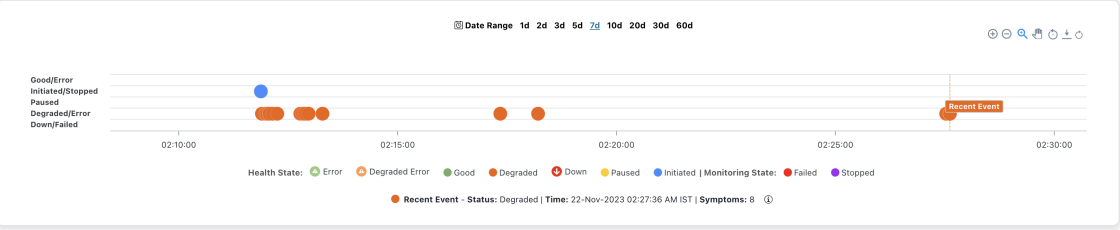
# About Assurance Graph

In Crosswork Service Health, a service instance is decomposed into subservices, which are then assured independently. Assurance Graph represents the service instances, and their dependent subservices in a graphical form. In this logical dependency tree, the topmost node represents the service instance that is being monitored and its child nodes represent the components identified as its subservices. Each subservice can have

dependencies as well. Assurance Graph helps to locate the problem area, and provides an indication of the possible symptoms and impacting metrics, which in turn helps in troubleshooting in case of degradation.

Crosswork Service Health updates the Assurance Graph automatically when the service instance is modified.

To view a service in the Assurance Graph, from the **Actions** column for the service, select **Assurance Graph**. Toggle the **Show History** button to view the historical data chart. Each dot on the history chart represents one Event Of Significance (EOS) for a service.




For each EOS, you can view the Assurance Graph and symptoms with 24 hours metrics collected based on the time of the EOS. For example, for a service for which monitoring was stopped, a dot appears indicating that the monitoring was stopped. Using your mouse, click and drag over a selected range over the EOS to zoom in on the time range. Hover your mouse over the service to view details about the event and any associated symptoms.

# Identify Root Causes Using Assurance Graph

You can monitor the VPN services using Assurance Graph capabilities and inspect any services or related nodes that are degraded.

### Before you begin

- Ensure that service health monitoring is enabled for the service you want to inspect. For details, see Start Service Health monitoring.
- Before using Service Health's Assurance Graph, ensure that topology map nodes have been fully configured and created with a profile associated to the service. If not, Subservice Details metrics will show that no value has yet to be reported.

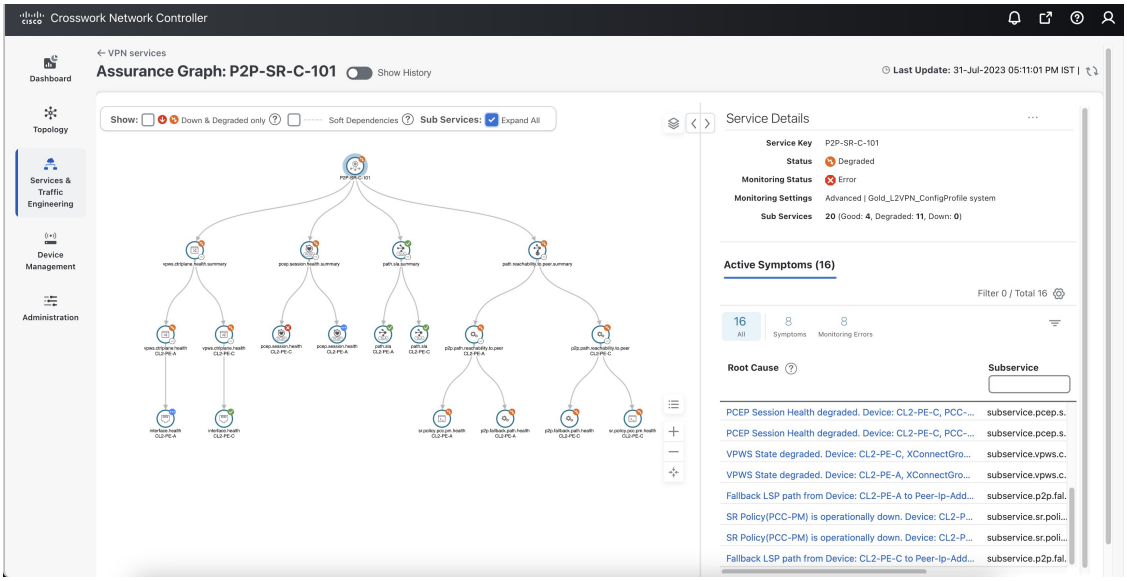
**Note** L3VPN service monitoring is supported on Cisco IOS XR devices and not on Cisco IOS XE devices. For an L3VPN service being monitored, if a provider and devices are deleted, and then added again, the monitoring status will remain in the degraded state with a monitoring status as Monitoring error. Stop and restart the service monitoring to recover from this error.

To identify the root causes using Assurance Graph, do the following:

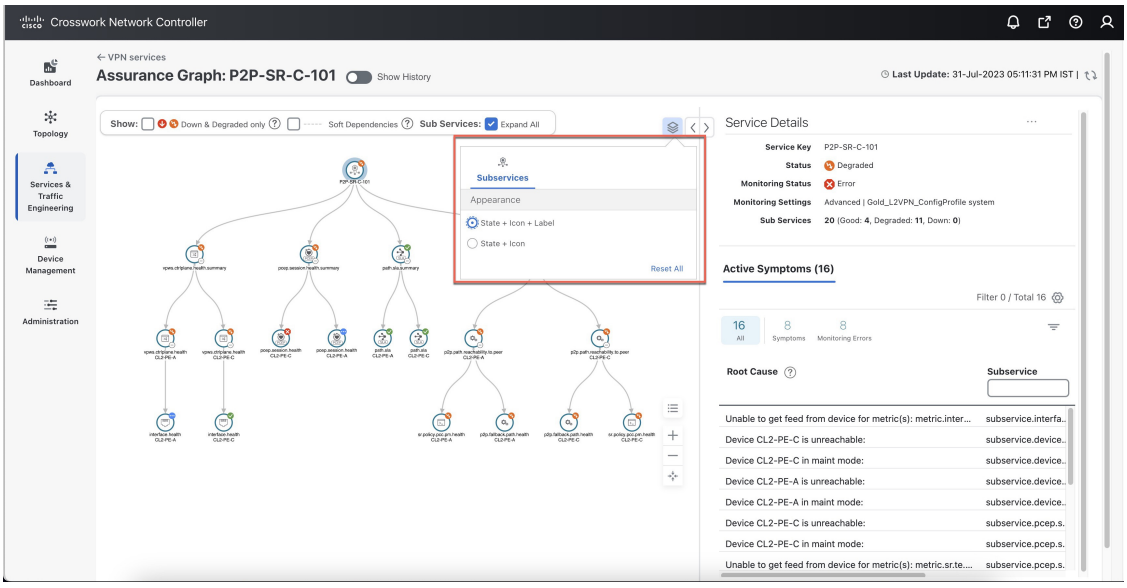
**Step 1** From the main menu, choose **Services & Traffic Engineering** > **VPN Services**. The service assurance dependency graph view opens on the left side of the page and the table opens on the right side.

**Step 2** In the Actions column, click ⋯ for the required degraded service and click **Assurance Graph**. The service assurance dependency graph view of services and subservices appear with the Service Details panel showing Service Key, Status, Monitoring Status, Monitoring Settings, Sub Services, and Active Symptoms details.

This may take up to 5-10 minutes to update after a service has been enabled for monitoring.



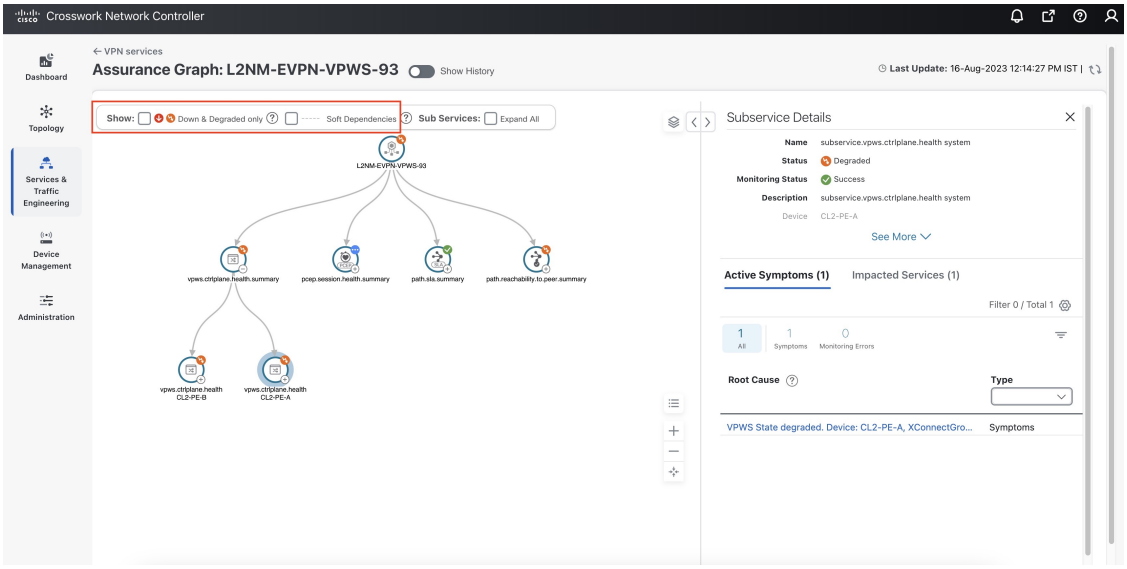

At the top-right of the service assurance dependency graph, select the stack icon to select the appearance option for the Subservices: **State + Icon + Label** or **State + Icon**.




**Step 3** By default, the Assurance Graph displays a concise view with only the service and the top level subservices (aggregator nodes). Click the + icon in the nodes to expand the graph and to view the dependent details. To expand all the nodes at once, click the **Subservices: Expand All** check box at the top.

**Step 4** Select a degraded subservice in the Assurance Graph. The Subservice Details panel appears with subservice metrics, as well as subservice specific Active Symptoms and Impacted Services details.

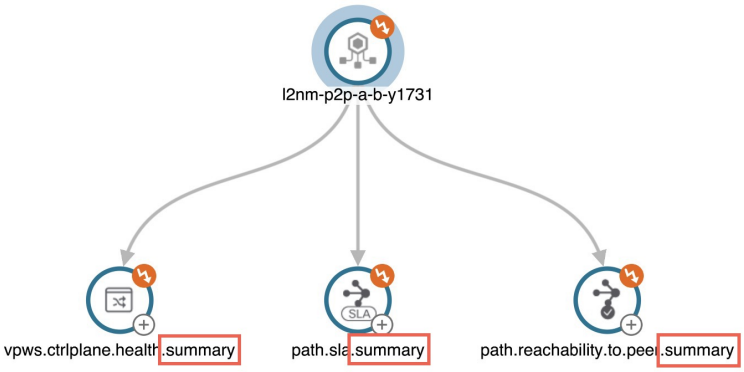
- **Active Symptoms**: Provides symptom details for nodes actively being monitored.
- **Impacted Services**: Provides information for services that are impacted by issues based on historical monitoring of health status.




**Note** At the top left of the service assurance dependency graph, check the **Down & Degraded only** or **Soft Dependencies** check boxes to further isolate the subservices. Soft Dependencies implies that a child subservice's health has a weak correlation to its parent's health. As a result, the degraded health of the child will not result in the parent's health degradation.

**Note** In some cases, the Summary node feature is available and summarizes the aggregated health status of child subservices and reports a consolidated health status to a service node. The Summary node feature is available in both L2VPN multipoint Basic and Advanced monitoring models.

- Basic monitoring subservices:
  - Device—Summarizes the health status of all underlying Devices participating in the given L2VPN service.
  - Bridge Domain—Summarizes the L2VPN service's Bridge Domain health status across all participating devices.
- Advanced monitoring subservices (in addition to what is also available with Basic monitoring):
  - EVPN—Summarizes the health status of all underlying subservices—BGP Neighbor Health and MacLearning Health across all participating PE endpoints and provides a consolidated overall EVPN health summary status.
  - Transport—Summarizes the health status of all underlying subservices—SR-ODN (dynamic), SR Policy (statically configured), and RSVP TE Tunnel, across all participating PE endpoints and provides a consolidated overall Transport health summary status.
  - SR-PCEP—Summarizes the health status of all the underlying subservices that are monitoring the PCEP sessions. Each underlying subservice monitors the PCEP session health on a particular device participating in the given VPN service.




**Step 5** Inspect the Active Symptoms and Impacted Services information, and the root causes associated with the degraded service to determine what issues may need to be addressed to maintain a healthy setup.

### Related Information

- To view the Active Symptoms and Root Causes, see Identify Active Symptoms and Root Causes of a Degraded Service, on page 4.
- To identify the issues with the degraded services within a specific time range, use the Last 24Hr Metrics. For details, see Identify Root Causes Using Last 24Hr Metrics, on page 10.
- To identify a service health issue by examining the collection jobs, see View Collection Jobs, on page 14.

# Identify Root Causes Using Last 24Hr Metrics

You can utilize the Last 24Hr Metrics to identify the issues with the degraded services within a specific time range. By isolating the issues within a specific time range, you can drill down on the details that may have caused the degraded (or down) service that can lead to troubleshooting the service or the node to address detailed symptoms.

### Before you begin

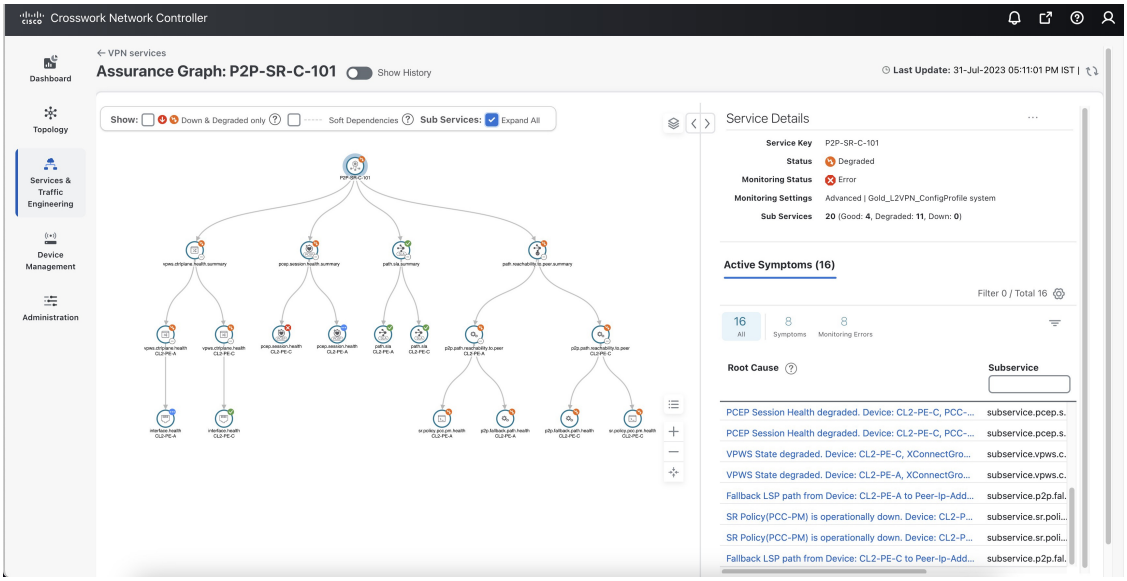
- Ensure that service health monitoring is enabled for the service you want to analyze. For details, see Start Service Health monitoring.
- Before using Service Health's Assurance Graph feature, ensure that topology map nodes have been fully configured and created with a profile associated with the service. If not, Subservice Details metrics will show that no value has yet to be reported.

**Note** L3VPN service monitoring is supported on Cisco IOS XR devices and not on Cisco IOS XE devices. For an L3VPN service being monitored, if a provider and devices are deleted, and then added again, the monitoring status will remain in the degraded state with a monitoring status as Monitoring error. Stop and restart the service monitoring to recover from this error.

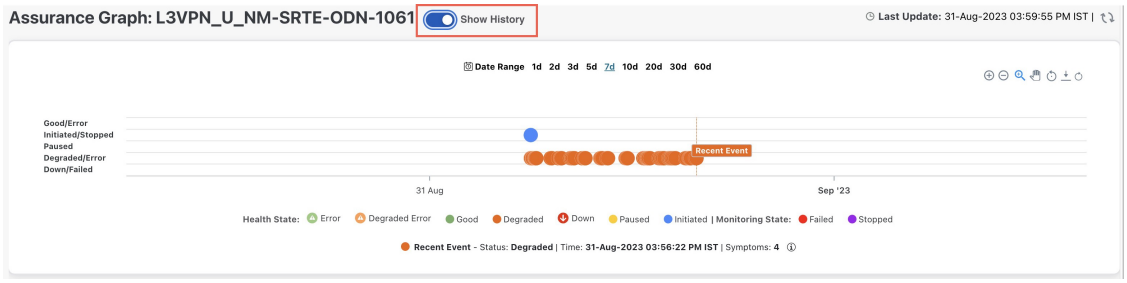
**Step 1** From the main menu, choose **Services & Traffic Engineering** > **VPN Services**. The service assurance dependency graph opens on the left side of the page and the table opens on the right side.

**Step 2** In the Actions column, click ... for the degraded service and click **Assurance Graph**. The service assurance dependency graph of services and subservices appear with the Service Details panel showing Service Key, Status, Monitoring Status, Monitoring Settings, Sub Services, and Active Symptoms details.

**Note** This may take up to 5-10 minutes to update after a service has been enabled for monitoring.

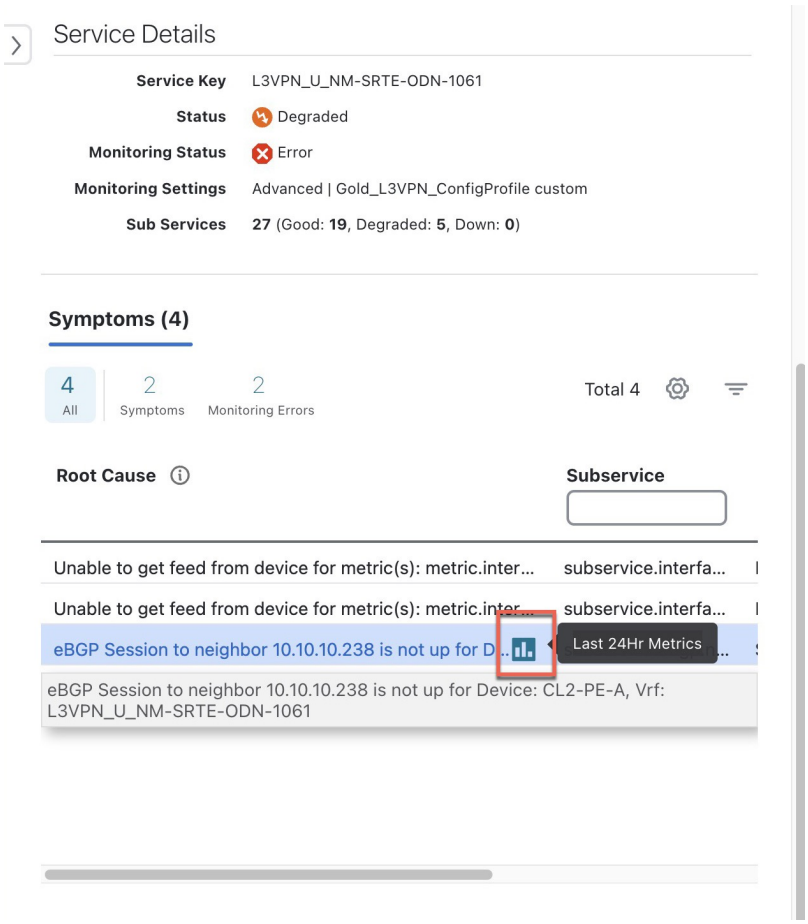



**Step 3** At the top of the page, click the **Show History** mode toggle. The historical Date Range graph appears. This graph shows different ranges of historical health service monitoring details from one day (1d) up to sixty days (60d). When you hover over an event on the Date Range graph, a tool tip with information about that event appears (such as date and time of the event, and number of symptoms).




**Step 4** Review the Root Cause information by clicking a particular event in the graph. The Service Details panel reloads, showing the active symptoms and the root causes associated with the event. Columns can be resized using your mouse or you can select the gear icon to deselect or select columns you want to appear.

**Note** Once you enable **Show History** mode, Root Cause information in the Active Symptoms table will start to show the blue Last 24Hr Metrics icon. Data from the device will be initially delayed, however, and may take some time before **Last 24Hr Metrics** begins to populate with data. Until then, the value of zero is reported.




**Step 5** To further isolate the possible issues and to utilize the **Last 24Hr Metrics**, perform the following steps:

a) In the Date Range graph, use your mouse to select the range of historical health service monitoring details from one day (1d) up to sixty days (60d).

**Note** At the top-right of the Date Range graph, select the appropriate icons to either zoom in or out, horizontally scroll through the date ranges, or refresh the graph to go back to the most recent event, for example. You can also use your mouse to draw a rectangle over events to further zoom in on the degraded devices. Events that are consecutive may appear as a line of white space.

b) Click on a degraded event in the graph. The Service Details panel reloads, showing any active symptoms and the root causes to be inspected. Expand the table and information as necessary for further details.

**Step 6** Check the **Down & Degraded Only** check box at the top-left corner of the Assurance graph to show only the Subservices which are degraded, along with other dependent but healthy subservices. Inspect the Service Details panel showing the active symptoms and their root cause. Uncheck the **Down & Degraded Only** check box and check the **Soft Dependencies** check box in the top-left corner of the Assurance graph. Soft Dependencies implies that a child subservice's health has a weak correlation to its parent's health. As a result, the degraded health of the child will not result in the parent's health degradation.

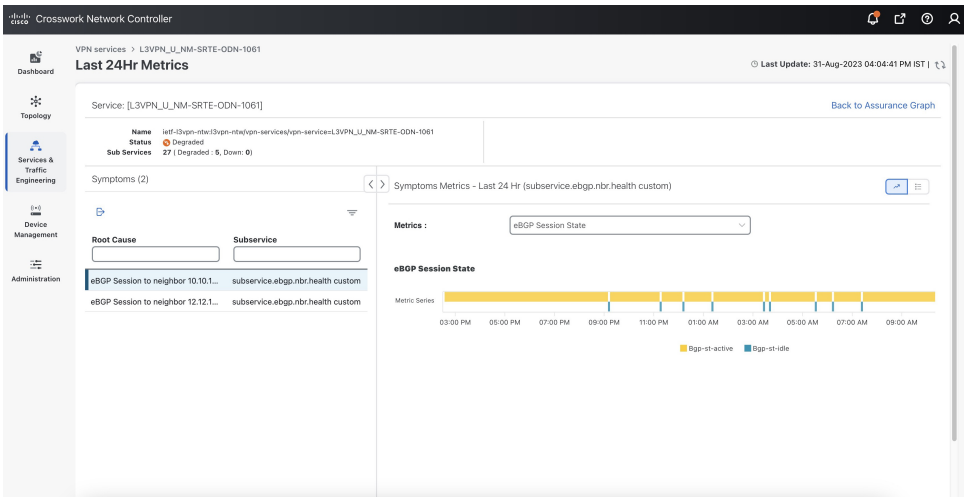
Use the + or – symbols in the bottom-right corner of the Assurance graph to zoom in or out on sub-services mapped. Select the **?** to view the Link Color Legend that explains all of the icons, symbols, badges, and colors and their definitions.

**Step 7** Select the degraded subservice in the Assurance graph to show the subservice details.

**Step 8** Click the **Symptoms** tab to show any root causes for the service health details that are displayed and then click the **Impacted Services** tab to view the impacted services.

**Step 9** Click **X** in the top-right corner to return to the VPN Services list and in the Actions column, click ⋯ for the degraded service in the list and click **Assurance Graph** to show the Service Details panel.

**Step 10** Again, select the **Show History** toggle in the top-right corner of the Service Details panel before selecting the blue metrics icon in one of the Root Cause rows. The Symptoms Metrics – Last 24 Hr bar chart appears. This chart provides details of the metric patterns for different sessions states (such as active, idle, failed) for individual root cause symptoms with Status, Session, Start Time, and Duration information to assist in troubleshooting prevailing issues. Use your mouse to hover over the chart to view the different details.




### Related Information

- To view the Active Symptoms and Root Causes, see Identify Active Symptoms and Root Causes of a Degraded Service, on page 4.
- To monitor the VPN services using Assurance Graph capabilities and inspect any services or related nodes that are degraded, see Identify Root Causes Using Assurance Graph, on page 7.
- To identify a service health issue by examining the collection jobs, see View Collection Jobs, on page 14.

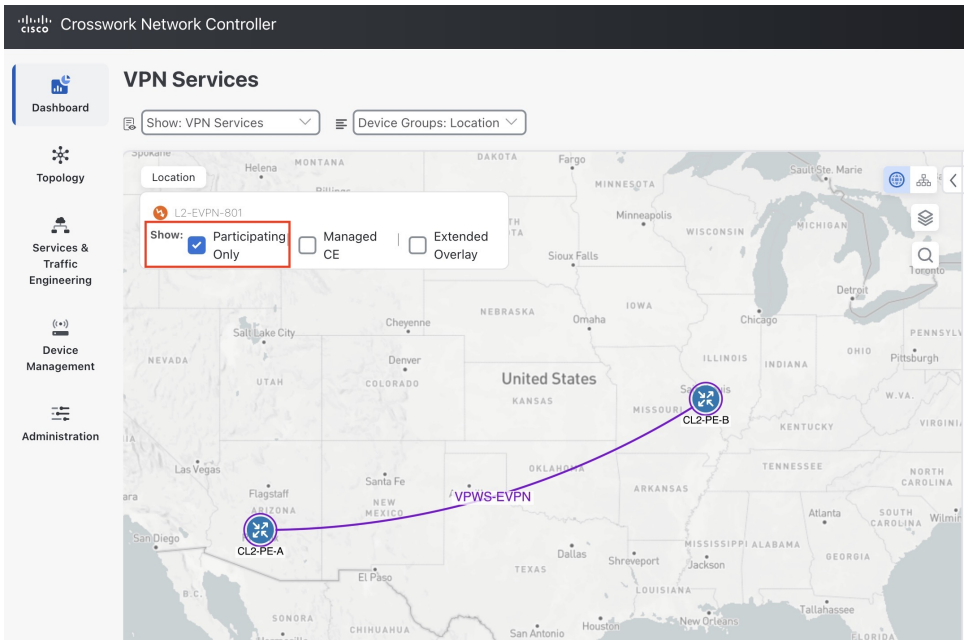
# View the Devices Participating in the Service

When a device or interface related subservice degrades, the corresponding devices display an orange icon in the topology view. To view the devices participating in the services, do the following:

**Step 1** From the main menu, choose **Services & Traffic Engineering** > **VPN Services**. The service assurance dependency graph view opens on the left side of the page and the table opens on the right side.

**Step 2** Click on the name of a service that shows as being degraded. The service assurance dependency graph view is updated, isolating the corresponding devices participating in that service.

**Step 3** At the top-left of the service assurance dependency graph view, select the **Show Participating Only** check box so that the service assurance dependency graph only shows the devices participating in the service.




**Step 4** Hover your mouse over the device icons and review the popup information relating to its Reachability State, Host Name, Node IP, and Type.

The devices that are healthy may show an orange badge to indicate that there are device or interface related subservices underneath that are not healthy. This ensures that unhealthy subservices are easily visible and can be identified from the topological view even if the device itself is healthy. After examining the Service Details for a device, for example, a condition, such as the CPU is low on a subservice node, helps to take the necessary steps to address the unhealthy subservice.

# View Collection Jobs

Crosswork Service Health provides the capability to view Parameterized Jobs (template-based collection jobs) that supports a greater number of jobs, adding the ability to view CLI collection jobs. This is useful when troubleshooting collection job issues by examining details of individual devices. Devices are identified by their Context ID (protocol) to determine if the jobs are gNMI, SNMP, or CLI-based jobs.

The **Parameterized Jobs** tab on the Collection Jobs page lists all active jobs created by the Cisco Crosswork Service Health application. If Crosswork Service Health is not deployed, this page will have no data.

**Step 1** From the main menu, choose **Administration** > **Collection Jobs**.

The Collection Jobs page appears.

**Step 2** Click the **Parameterized Jobs** tab.

**Step 3** Review the Parameterized Jobs list to identify the devices that may have service health degradation issues. By reviewing Parameterized Jobs, you can identify and focus on gNMI, SNMP, and CLI-based jobs by their Context ID (protocol) for further troubleshooting purposes.

**Step 4** In the Job Details panel, select the collection job you want to export and click to download the status of collection jobs for further examination. The information provided is collected in a .csv file when the export is initiated.

**Note** When exporting the collection status, you must fill in the information each time an export is executed. In addition, make sure to review the **Steps to Decrypt Exported File** content available on the Export Collection Status dialog box to ensure you can access and view the exported information.

**Step 5** Click **Export**.

**Step 6** To check the status of the exported collection job data, click **View Export Status** at the top right of the Job Details panel. The Export Status Jobs panel appears providing the status of the export request.

**Step 7** Review the exported .csv file for collection job details and the possible cause of the degraded device.