Activity maps concepts

Published: 2018-02-06

An activity map is a dynamic visual representation of the L4-L7 protocol activity between devices in your network. With activity maps, you can view real-time information about which devices and services are talking to each other across your network.

When you generate an activity map for a single device, device group, or activity group, you can view traffic from the origin device to any server or client over a specific protocol. Hover portions of the map to find details about devices and their connections. Interact with map data to investigate related metrics and export your map as an image or PDF file.

Activity maps can help you with the following scenarios:

Complete a data center or cloud migration

As part of your migration strategy, you must determine which services can be turned off and when. An activity map helps you identify which devices are still connected so you can prevent unexpected service disruptions during the migration process.

Identify the root cause behind a slow application

Applications often depend on multiple tiers of services within a network. An activity map can help you identify the delivery chain of traffic to your slow application server. Click a device to investigate related metrics, which can shed more light onto the root cause of the slow-down.

Track suspicious devices or unexpected connections

During a security event, an activity map can help you identify affected devices by tracking the real-time east-west traffic associated with a suspicious device. As part of a daily security monitoring strategy, you can generate an activity map to confirm that devices are not making unexpected connections with other devices.

Here are some important considerations about activity maps:

- You cannot view custom devices in an activity map.
- You cannot select a device in limited analysis to be the origin of an activity map because these devices do not have L4-L7 protocol metrics associated with them. You can view connections from an origin device in full analysis to devices in limited analysis. For more information about limited analysis, see View the device limit and device counts.
- You cannot view a device without any protocol activity in an activity map. Change the time interval or your device selections and try again.
- You can create an activity map in a Command appliance to view device connections across all of your Discover appliances. However, connected Discover appliances must be upgraded to firmware version 7.0.

View a 2D or 3D map

By default, activity maps are displayed in a 2D layout. Click-and-drag your mouse to pan across the map. Click the controls in the bottom right corner of the page, or scroll with your mouse, to zoom in and out to view map data.

If you would like to view your map on a large screen, for example in a network operations center, we recommend that you display your map in a 3D layout. In the upper right corner of the activity map, click the command menu ⋮ and select **View 3D layout**. Maps that are displayed in a 3D layout automatically rotate. Click-and-drag your mouse to rotate the map to a specific location or scroll with your mouse to zoom to view map data.

You can export an entire map to an PNG, SVG, or PDF file.

View map labels

Devices are represented by circles and protocol activity is represented by lines that connect the circles.

To optimize the amount of information you can view in a large map, the map displays a small number of map labels by default. Zoom or hover over circles or lines in the map to view their label.

Circle labels contain details such as the device hostname, IP address, or MAC address. Line labels contain protocol names associated with the device connection and the direction of traffic flowing between the devices, which is displayed as animated pulses.

Interpret map data

The layout, color, and size of map elements are optimized to show you the dynamic device connections displayed on a map. Larger circles, wider lines, and darker colors highlight areas of more protocol activity. You can also learn about the direction of traffic between devices by viewing the animated pulse in the center of a line.

The map layout changes as data about device activity is updated in real-time. For example, the layout is updated as new connections are observed or devices become inactive. When the time interval in the upper left corner of the page is set to an interval such as Last 30 minutes, Last 6 hours, or Last day, activity map data will continuously update every minute with real-time data.

Tip: Set a custom time interval with a specific start and end time to stop real-time layout updates.

The size of the circles and the width of the lines in a map correspond to a metric, such as bytes, connections, or TCP turns. By default, the circles and lines sizes correspond to bytes, or volume of traffic. For example, larger circles highlight which devices are associated with more traffic. Wider lines highlight which device connections are associated with more traffic that was sent or received over a protocol.

At the bottom of the left pane, you can select a different metric for map elements:

• **Bytes:** See all of the devices sending or receiving data during the time interval.

• **Connections:** See only the devices that have established a new connection at least once during the time interval.

• **TCP Turns:** See only the devices that have switched between sending and receiving data at least once during the time interval.

Investigate device connection metrics and records

If you find a device on your map that is worth investigating, you have several options to gather more information about that device.

Change the time interval to view differences in connections

Click the time interval in the top left corner of the page and select a time interval. You can see how metric activity and device connections changed over time.

For more information, see Change the time interval.

Navigate to protocol pages to find related metric activity

Click a circle or line to access a drop-down menu as shown in the following figure.

Select the device name from the menu to navigate to the Overview protocol page for that device. The protocol page contains a summary of important protocol metrics that were observed and associated with the device. From a protocol page, you can find related metrics such as errors, requests, responses, and server processing time. You can also drill down on a metric from a protocol page to view metric details, such as server IP address, client IP address, status codes, methods, and URIs.

Search for transaction records associated with a connection (Explore appliance only)

Click a circle or line to access the drop-down menu. Click **Records**. A records query page opens and displays all the records from each connected device, including all record types associated with the device connection protocols.

Related topics

Check out the following resources that are designed to familiarize new users with activity maps.

- Generate an activity map
- Activity Maps FAQ