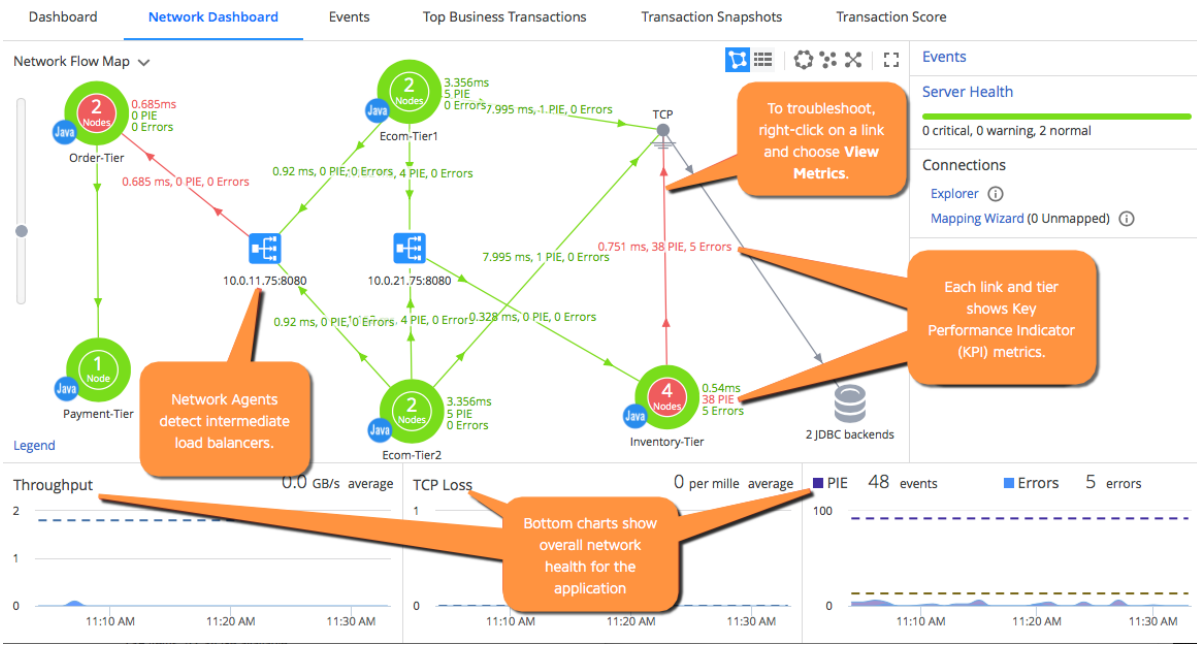
Network Dashboard

On this page:

The Network Dashboard provides a network-layer view of your application. Here you can quickly see if any part of the network is impacting application performance. The bottom charts show the overall network health. Each tier and link shows network KPI (Key Performance Indicator) metrics. Network Agents detect intermediate load balancers and TCP endpoints. You can do the following:

- Enable baselining to visualize network elements with performance issues (red/yellow links and tiers).
- View network metric charts in tier/link popups.
- Find root causes in a specific network link: right-click and choose View Metrics. This opens a context-sensitive dashboard for the element.
  - The tier dashboard shows correlations between outlier (Slow/Very Slow/Stalled/Error) transactions and network-performance metrics.
  - The link dashboard shows network-performance issues on the client tier, server tier, and network path.
- Find root causes in a specific connection: when you narrow the issue down to a specific network link, you can
  - Configure the Network Agents to collect detailed metrics for the individual Connections used on that link.
  - Drill down to find the root cause in an individual Connection.
- You can copy IPs and ports for individual connections from the Network Dashboard. This makes it easy to forward this information to operations and other personnel when troubleshooting an issue. To copy IPs and ports:
  1. Click on a link to open the link popup and go to the Connections tab.
  2. Select the connections of interest (use ctrl-click to select multiple connections).
  3. Right-click on the selection and choose Copy IP addresses to clipboard.

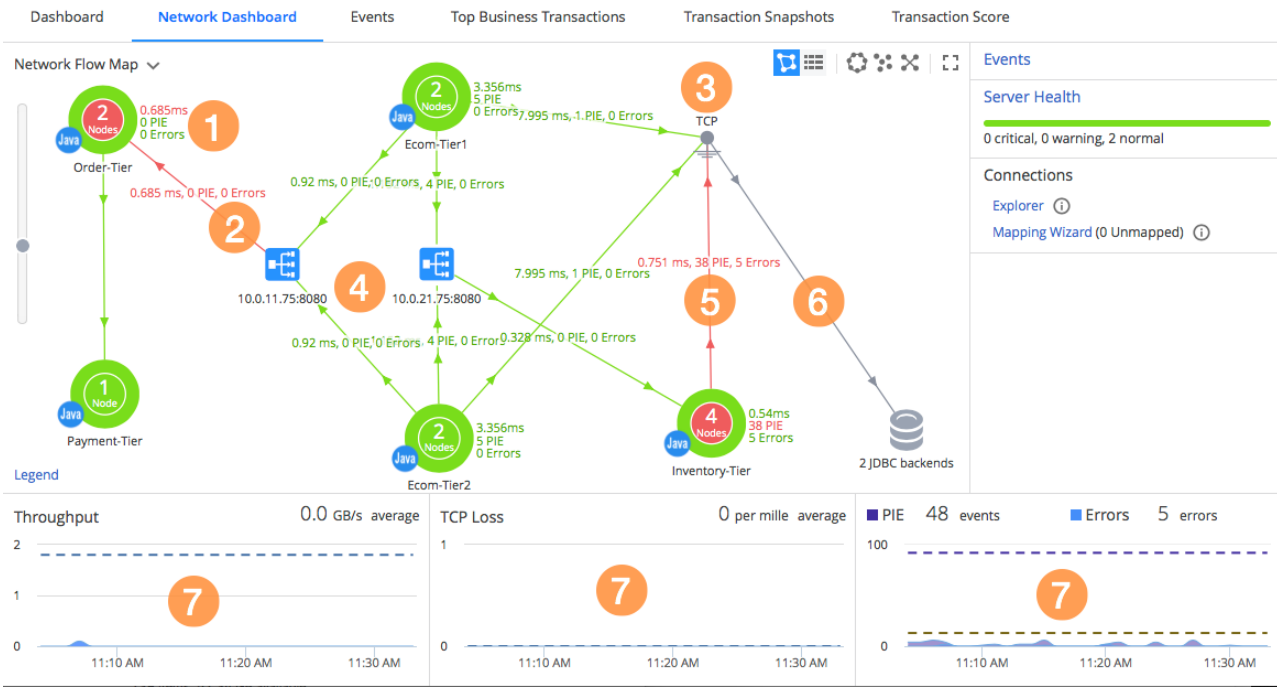


Important Notes

Note the following:

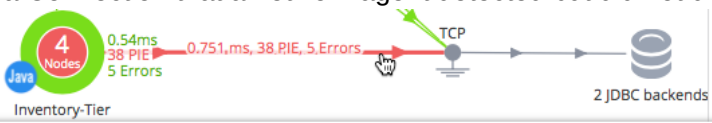
- In many cases, the Application Dashboard and Network Dashboard might show different topologies for the same application. This is expected behavior. Unlike app server agents, network agents detect intermediate network devices between nodes and considers these devices when collecting metrics. The two dashboards show the same application but from different perspectives: an application perspective and a multi-layer, network/application perspective.
- This release does not support the following Network Flow Map features:
  - Federated Flow Maps
  - Visualization of flows between web servers and APM entry tiers
  - The Network Flow Map does not filter out connections based on the selected time range.
- In some cases, the KPIs for a tier or link might be different in the Network tab vs. the Flow Map. The popup window shows the latest data; the Flow Map updates data every two minutes. Any discrepancy between KPI values is due to this difference in reporting times.
- If you open the Network Flow Map for an individual node, the KPI metrics for node-to-load-balancer and node-to-tcp-endpoint links show KPIs for all nodes in the parent tier (instead of KPIs the individual node only). To view KPIs for the individual node, open the link popup and look at the Connection KPIs.

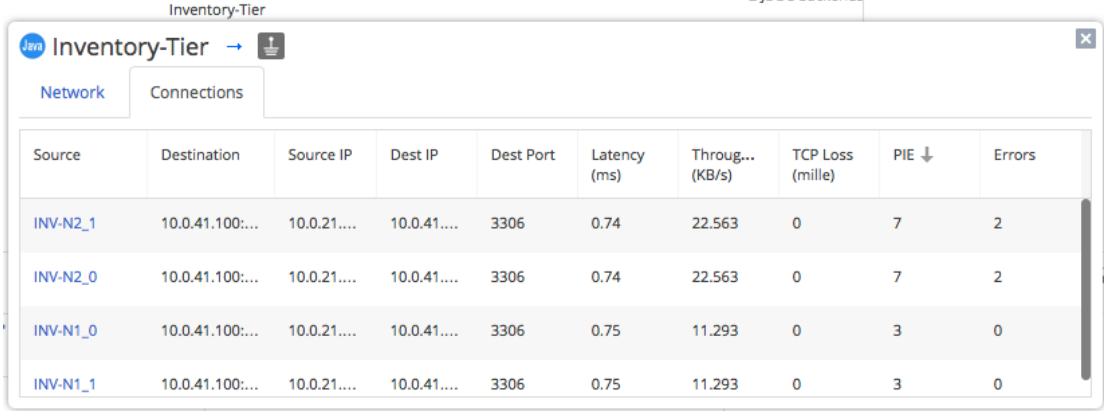
Network Dashboard Reference



The Network Dashboard shows:

- Network-based key performance Indicators (KPIs) 1 for the monitored nodes in each tier:
  - The average Latency (#ms) for individual packets
  - The number of Performance Impacting Events (PIE)
  - The number of Errors
- KPIs for all network links 2. Click a tier or link to see the set of all associated Connections. (A gray link indicates a Connection that a network agent detected but did not directly monitor.)





- The Network Dashboard shows a TCP endpoint 3 icon when a network agent observes traffic between a monitored node and an endpoint (IP address & TCP port & protocol), but cannot determine if the endpoint represents
  - An application node that sends/receives traffic for the application, or
  - An intermediate device (proxy or load balancer) that transfers traffic to/from another node over a separate Connection
- Network agents automatically detect load balancers 4, which often mask internal IP addresses and have the effect of splittin g an in-flight application message into two separate TCP connections. The auto-detection of TCP endpoints and load balancers between application nodes make it easy to identify the exact locations where network issues are occurring.

- Note how links are colored in the Network Dashboard:
  - Green/yellow/red, to visualize the network performance compared to the overall performance baseline for that link 5
  - Blue, if baselining is disabled
  - Gray, for connections between application nodes and TCP endpoints. 6 In this case, the gray link means "The connected node and endpoint are either the same device, or two devices exchanging traffic over a separate, unmonitored Connection."

- The Network Dashboard also shows KPIs 7 for the entire application. Here you can see the overall throughput that the application places on the network; the rate of network packet loss (packets sent but never received); the number of Performance Impacting Events (PIE), which indicate potential problems on one or more nodes or Connections; and the number of errors for the entire application.