Cisco Nexus Insights 5.0 Whitepaper

Introduction

Troubleshooting, root-cause analysis, and remediation of network issues are common challenges for day to day operations. With the legacy networking operation tools, these tasks are manual, time consuming, and reactive.

They require network operators to have years of experience, extensive domain expertise, and the ability to correlate complex IT environments to prevent or fix issues while upholding the infrastructure uptime with minimum disruption. Cisco Nexus Insights, a modern networking operation application, aims to simplify and automate these operation tasks. By ingesting real-time streamed network telemetries from all devices, it provides pervasive infrastructure visibility. With its powerful analytics and engine, it can proactively detect different types of anomalies throughout the network, root cause the anomalies, and identify remediation methods. It is a tool to modernize the operation of networks, helping the network team to reduce troubleshooting efforts, increase operation efficiency, and proactively prevent network outages.

Note: The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Background

Modern data centers are managed through controllers such as Cisco ACI™ or Cisco DCNM which capture the intents of network to deliver an automated, consistent policy framework across the data center. The same intent-based policies can be extended to multiple data center sites, branches, and the public cloud, to provide centralized control. Cisco Nexus Insights helps with Day 2 Operations of these fabrics to provide visibility, proactively detecting anomalies with correlated network and application view. This helps accelerate troubleshooting, thereafter remediating issues in these fabrics. Cisco Nexus Insights was designed with the following network characteristics and architecture in mind.

Inbuilt automation: The network configuration is centrally managed by a controller, therefore the network operators no longer need to manage the device configuration on a box-by-box basis. With the centralized controller method, it is easier to maintain feature and configuration consistency across the network.

Scalable architecture: Driven by different reasons, such as scale, disaster avoidance or disaster recovery, modern data centers often expand beyond a single site to multiple geographically dispersed locations, sometimes even to the public cloud. As data centers scale out, the complexity of collecting and analyzing data to understand the operation state of the networks increases. At the same time, with the increasingly distributed application workload, a data center infrastructure can be running anywhere between a few thousands to a few millions of flows at a time. In addition, at times there may be a few hundred messages or events being logged every second. Manually correlating these flows, logs, switch by switch in order to troubleshoot issues can be very challenging and time consuming.

Operations test: The challenge faced by operators is to comprehend and correlate the data collected from each switch in the fabric to a particular problem, such as slowness in a web application. This implies a stringent expectation that an operator has the required knowledge and expertise (which usually takes time to build) about most if not everything happening in the infrastructure.

Cisco Nexus Insights addresses these challenges to bring about the following benefits

- Increase operation efficiency and network availability with proactive monitoring and alerts: Cisco Nexus Insights learns and analyzes the network behaviors to recognize anomalies before the end users do, then generates proactive alerts useful in preventing outages. Cisco Nexus Insights also proactively identifies vulnerability exposure of the networks to known defaults, PSIRTs or field notices and recommend the best course for proactive remediation.
- Shorten time to resolution for troubleshooting: Cisco Nexus Insights minimizes critical troubleshooting time through automated root-cause analysis of data-plane anomalies, such as packet drops, latency, workload movements, routing issues, ACL drops, etc. Additionally, Cisco Nexus Insights provides assisted auditing and compliance checks using searchable historical data presented in time-series format.
- Increase speed and agility for capacity planning: Cisco Nexus Insights detects and highlights components exceeding capacity thresholds through fabric-wide visibility of resource utilization and historical trends. The captured resource utilization shows time-series-based trends of capacity utilization so that the network operation team can plan for resizing, restructuring, and repurposing.

Cisco Nexus Insights Components

Cisco Nexus Insights is a micro-services-based modern application for network operation. It is hosted on Cisco Nexus Dashboard where Cisco ACI and Cisco DCNM* sites are onboarded and respective data from these sites is ingested and correlated by Cisco Nexus Insights.

*In Cisco Nexus Dashboard 2.0 release, Cisco DCNM managed NX-OS datacenter network sites are not managed by Cisco Nexus Dashboard. Cisco Nexus Insights application for NX-OS networks need to run on the DCNM compute nodes.

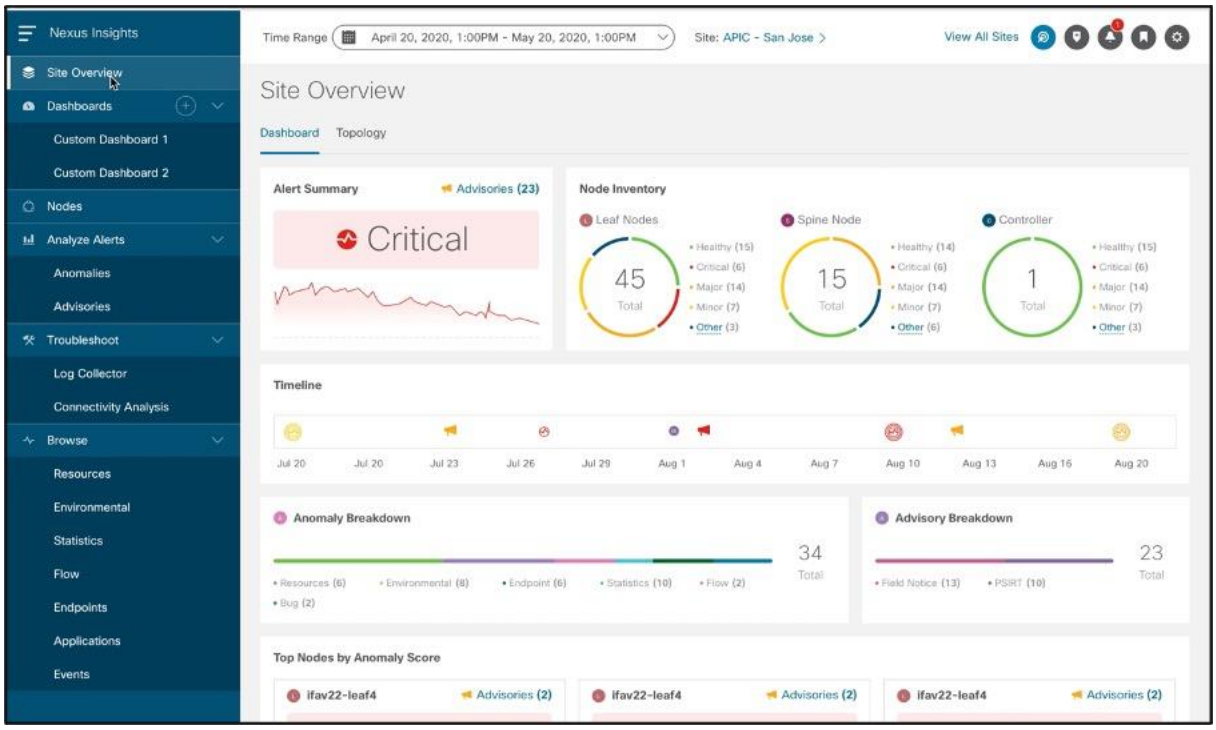
Cisco Nexus Insights directs operators' attention to the significant matters that are relevant to the task at hand, such as troubleshooting, monitoring, auditing, planning, vulnerabilities, etc. All anomalies and analytics results in Cisco Nexus Insights can be accessed by an external system via its REST-APIs, or exported using Kafka where users can subscribe to relevant topics. Users can also choose to receive email notifications on anomalies with the option to customize what anomaly types they want to see along with severity and cadence.

The sections below introduces the key components of Cisco Nexus Insights. These options (with sub categories) are available on the left panel of the application.

- **Cisco Nexus Insights Dashboard**

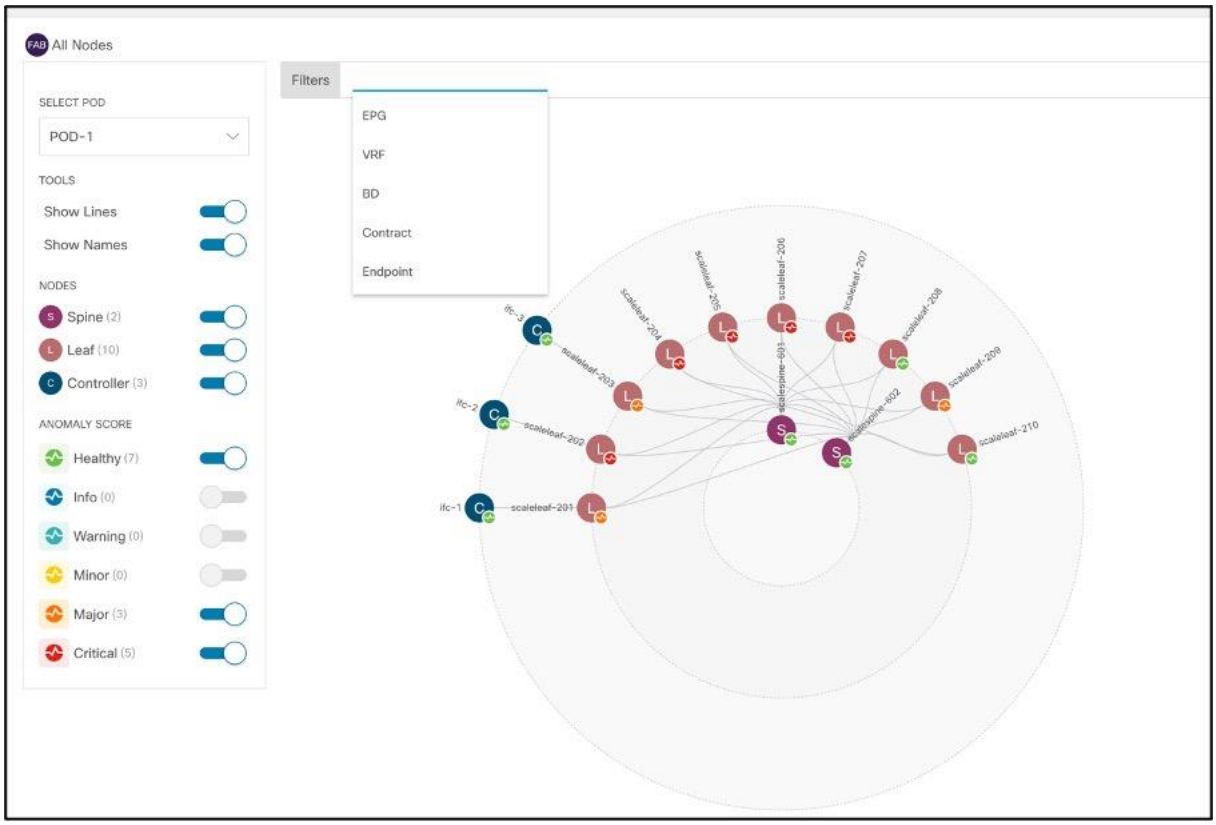
  Provides a view into site level issues that need attention, all which are calculated by Cisco Nexus Insights and rolled up into one place which is the Dashboard – an easy drill down into issues sorted by severity and categories, Top Nodes that are experiencing anomalies, Timeline view of issues based on the time range selected, Site health score, Advisories generated by the app, Node inventory by roles and corresponding health score of each node providing a single click option to Node 360 which gives all details on the nodes including trends of anomalies as observed.

  Cisco Nexus Insights also allows user to create custom Dashboards for any charts as seen in the app



- **Topology**

  Provides a graphical representation of the fabric and how nodes are connected. Allows user to select filters based on switch role, score of the node, VRF,EPG,BD etc. to locate issues in a topological view.



- **Alerts**

  Provides a view into Anomalies and Advisories generated by the app.

  Anomalies –

  Consists of threshold violations and sudden rate of change for

  - Resource utilization
  - Environmental issues like power failure, memory leaks, process crashes, node reloads, CPU, memory spikes
  - Interface and Routing protocol issues like CRC errors, DOM anomalies, interface drops, BGP issues like lost connectivity with an existing neighbor, PIM, IGMP flaps, LLDP flaps, CDP issues etc. Also provides a view into microbursts with offending and victim flows
  - Flow drop with location and reason of drop, Abnormal latency spikes of flows using hardware Telemetry and direct hardware export. Flows impacted due to events in a switch like buffer, policer, forwarding drops, ACL drops, policer drops etc. using Flow Table Events (FTE) which is another form of hardware Telemetry
  - Endpoint duplicates, rapid endpoint movement, rouge endpoints
  - Application issues a calculated by AppDynamics and Cisco Nexus Insights (AppD Integration required)

  Also consists of indication of being affected by known Cisco caveats and best practice violations at a node level.

  Advisories –

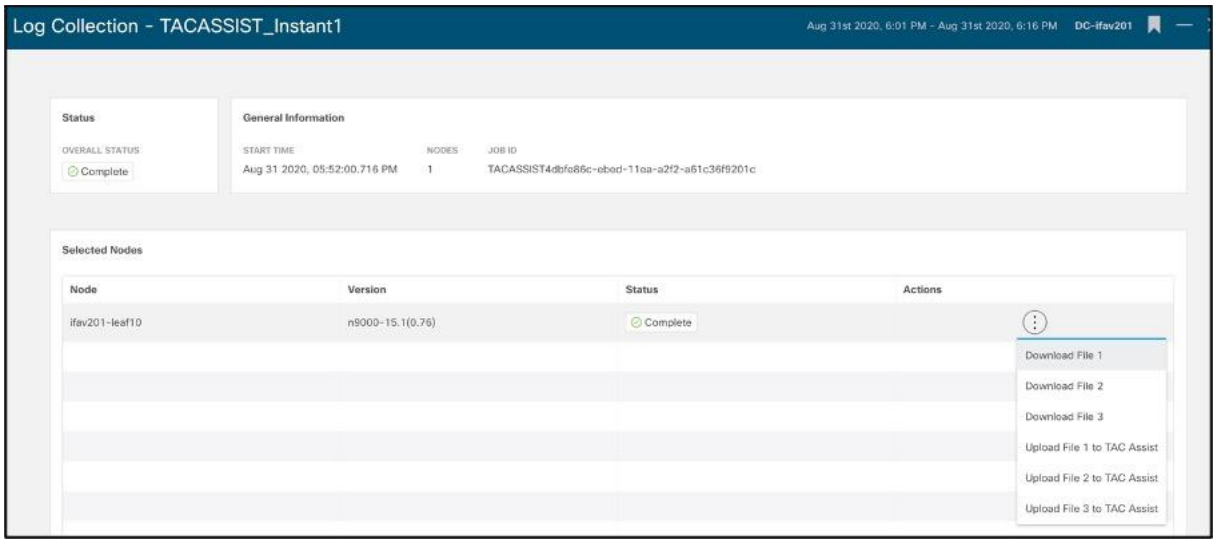
  Consists of relevant impact due to Field Notice, EOL/EOS of Software and Hardware and PSIRTs at a node level.

- **Troubleshoot**

  Allows users to collect logs and run analysis at a flow level to find offending nodes in the fabric.

  Log Collector

  Allows user to collect tech-support logs per node. These logs can be downloaded locally and optionally uploaded to Cisco Cloud to make them available for Cisco Support when opening a Service Request (SR).

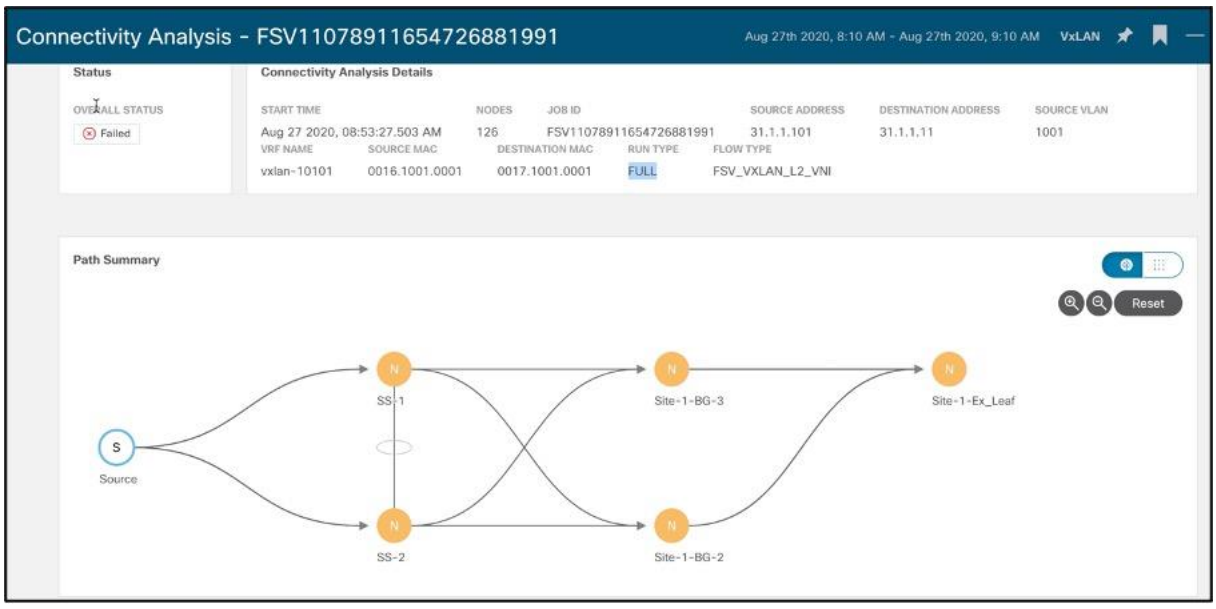


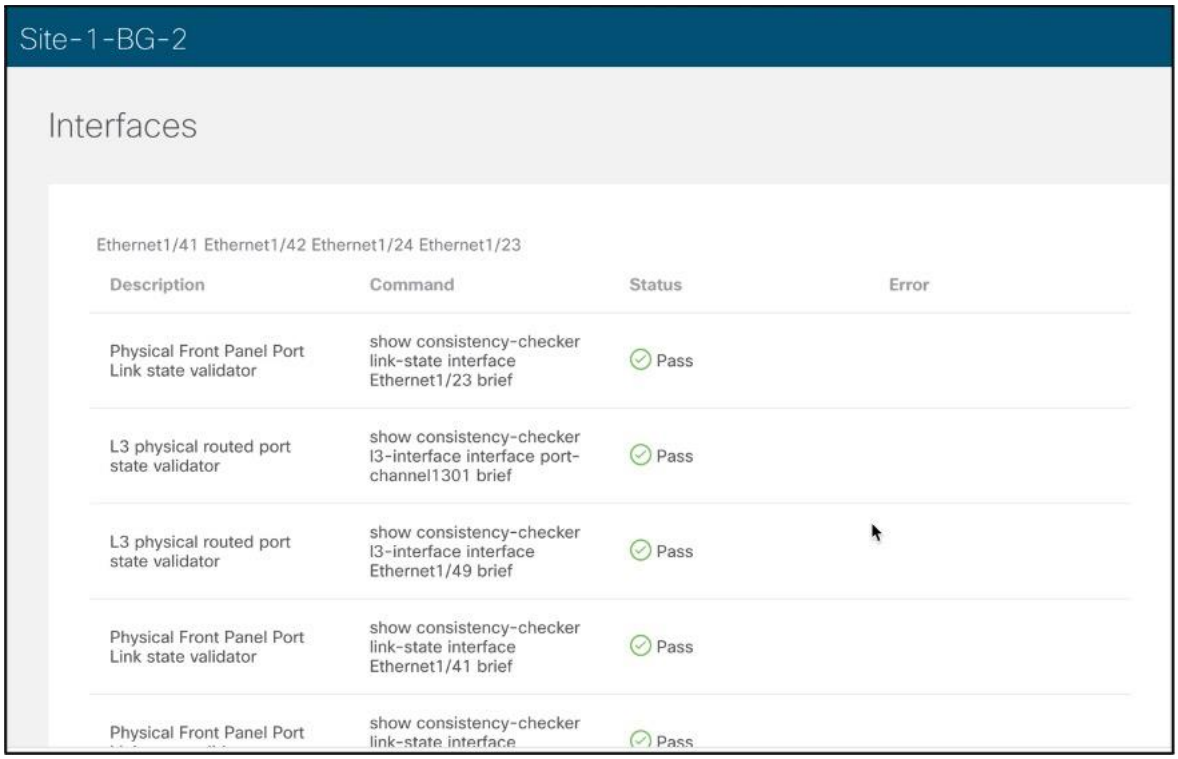
Connectivity Analysis

Allows user to run a quick or full analysis for a flow within a fabric or spanning multiple fabrics to -

- Trace all possible forwarding paths for a given flow across source to destination endpoints
- Identify the offending device with issue, resulting in the flow drop
- Help narrow down the root cause of the issue, including running forwarding path checks, software and hardware states programming consistencies through consistency-checkers, and further details related to packets walkthrough and lookup results through packet capture

Below screenshot shows an example of what are the possible paths a flow can traverse, while running thorough consistency checks with respective errors if any. These issues are time consuming to debug and connectivity analysis provides a quick analysis of these issues in a user driven way.





- **Browse**

  Browse options allow users to look at specific data sets ingested and correlated by Cisco Nexus Insights.

  - Resources - Useful for capacity planning because it offers early detection of resources that are exceeding capacity thresholds
  - Environmental - Identifies anomalies by observing parameters such as CPU, memory, temperature, power draw, fan speed, etc.
  - Statistics – Provides a thorough view into interface counters such as utilization, CRC, stomped CRC, FCS errors and into protocols such as CDP, LACP, LLDP, BGP, PIM, IGMP and IGMP snoop
  - Flow – Shows all flows as ingested and correlated by Cisco Nexus Insights. Helps identify, locate, and root-cause data path issues such as latency and packet drop for specific flows based on correlation done by the app
  - Endpoints – Provides a list of all endpoints and how they are attached, history of endpoint moves, duplicate endpoints and uses this database to correlate how network issues affect endpoints in the fabric
  - Applications – This enables AppDynamics integration with Cisco Nexus Insights allowing user to get a single pane of glass for apps and network issues and map an application link to a flow in the ACI and NXOS fabric thereby allowing quicker RCA of app slowness
  - Events - This is Software telemetry that leverages audit logs and events and faults data from the Cisco ACI fabric

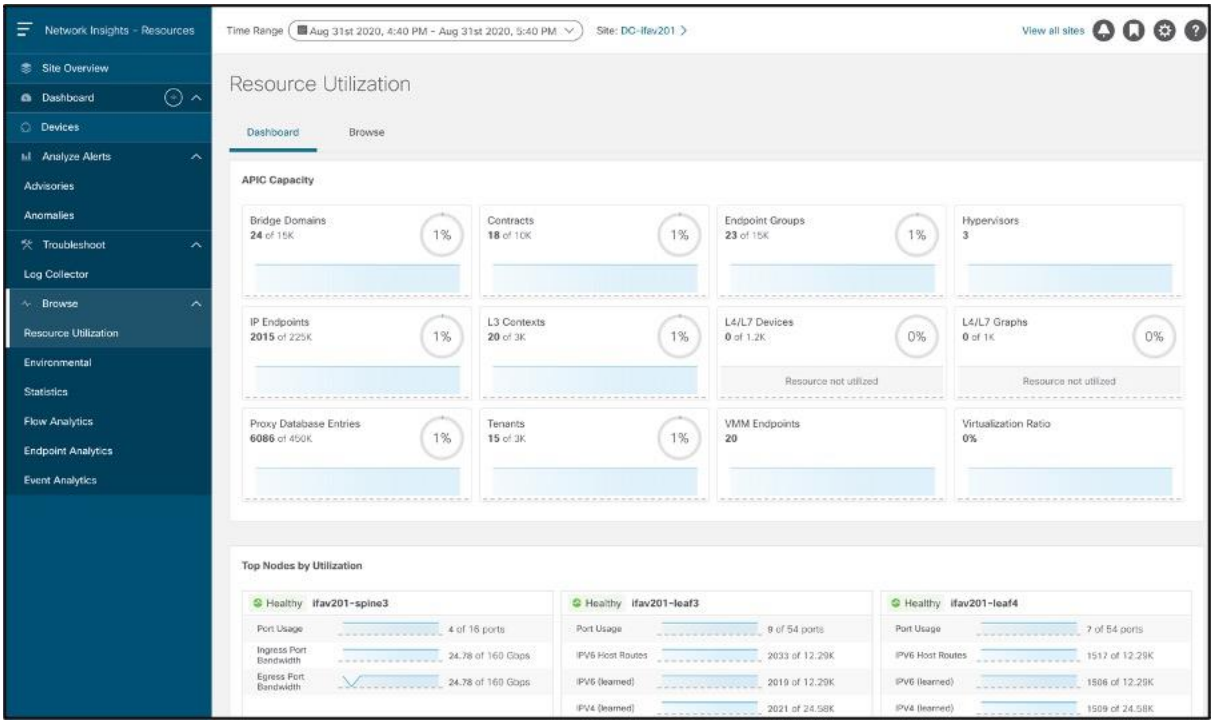
Browsing Cisco Nexus Insights

Let's delve into the browse data available in Cisco Nexus Insights. All anomalies observed for any of the below data sets are rolled into the Dashboard view of the respective site to draw your attention.

Resources

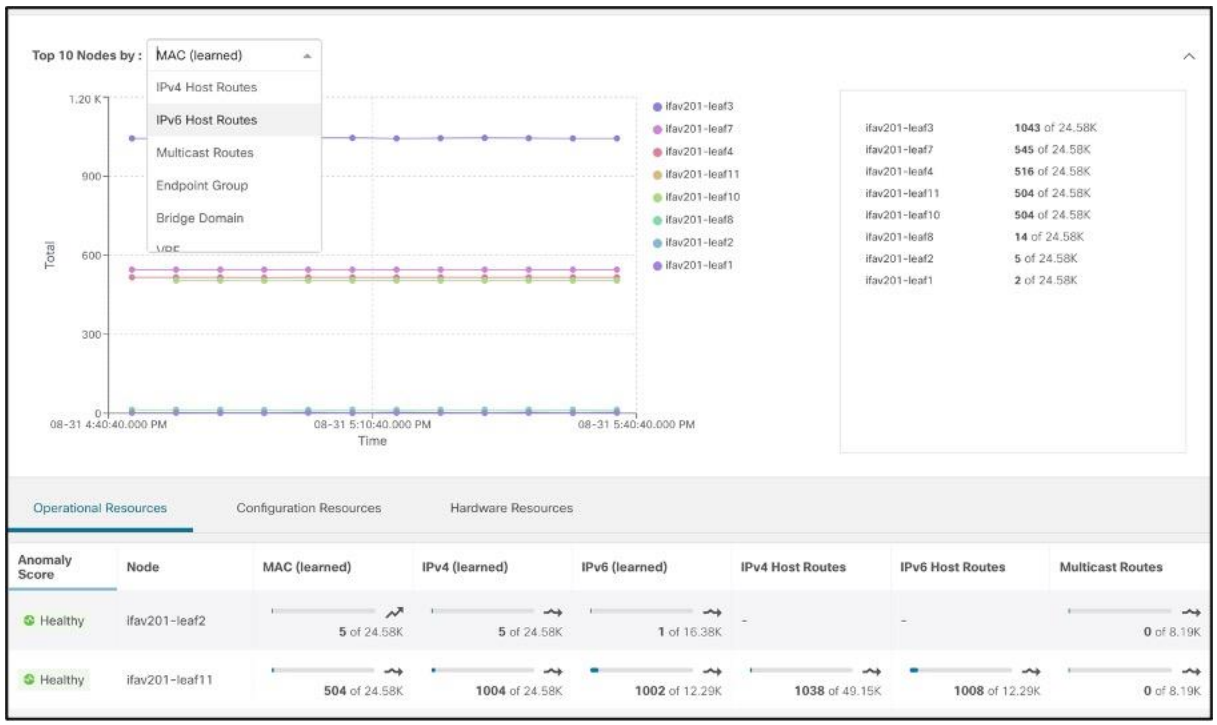
It is tedious to keep track of software verified scale per release, per resource and what scale the hardware in your network supports. Moreover, keeping track of utilization of resources per node over time, setting static thresholds for these resources to be notified on violation does not scale for dynamically growing networks. To resolve for these, Cisco Nexus Insights baselines utilization of resources, monitors trends, and generates anomalies on abnormal usage of resources across nodes so as to help user plan for capacity in their networks.

Resource utilization shows time-series based trends of capacity utilization by correlating Software Telemetry data collected from nodes in each site. Persistent trends help identify burdened pieces of infrastructure and plan for resizing, restructuring, and repurposing.

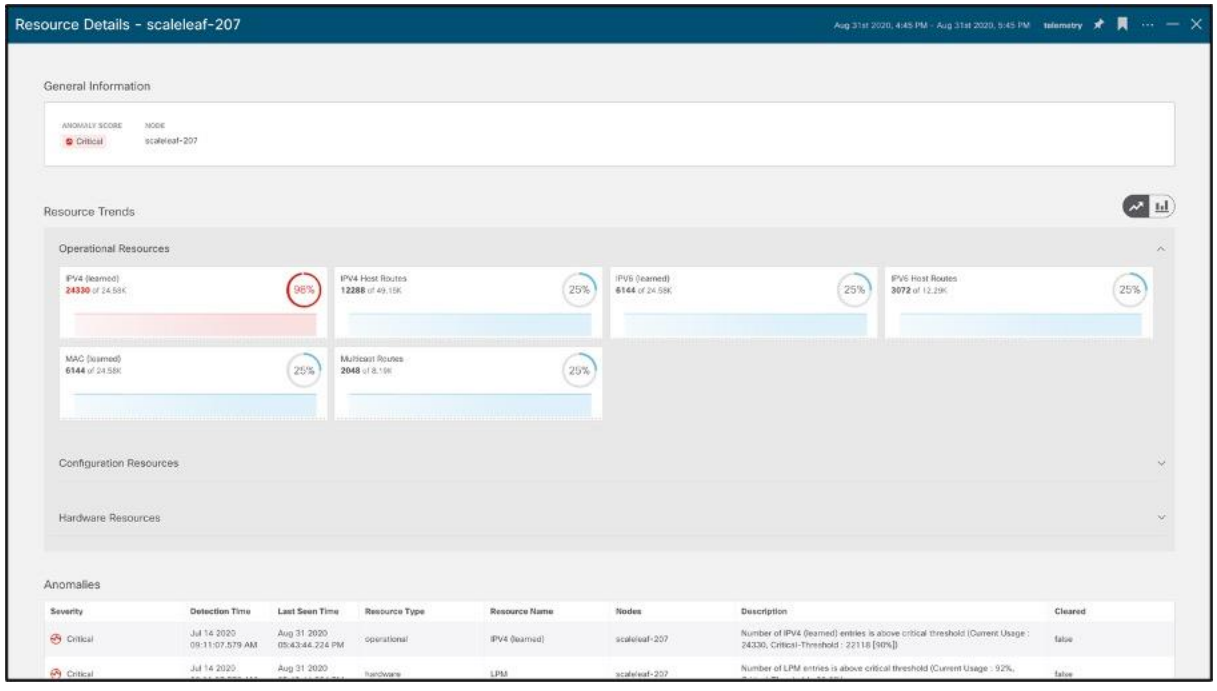


Resource utilization categorizes capacity utilization as follows:

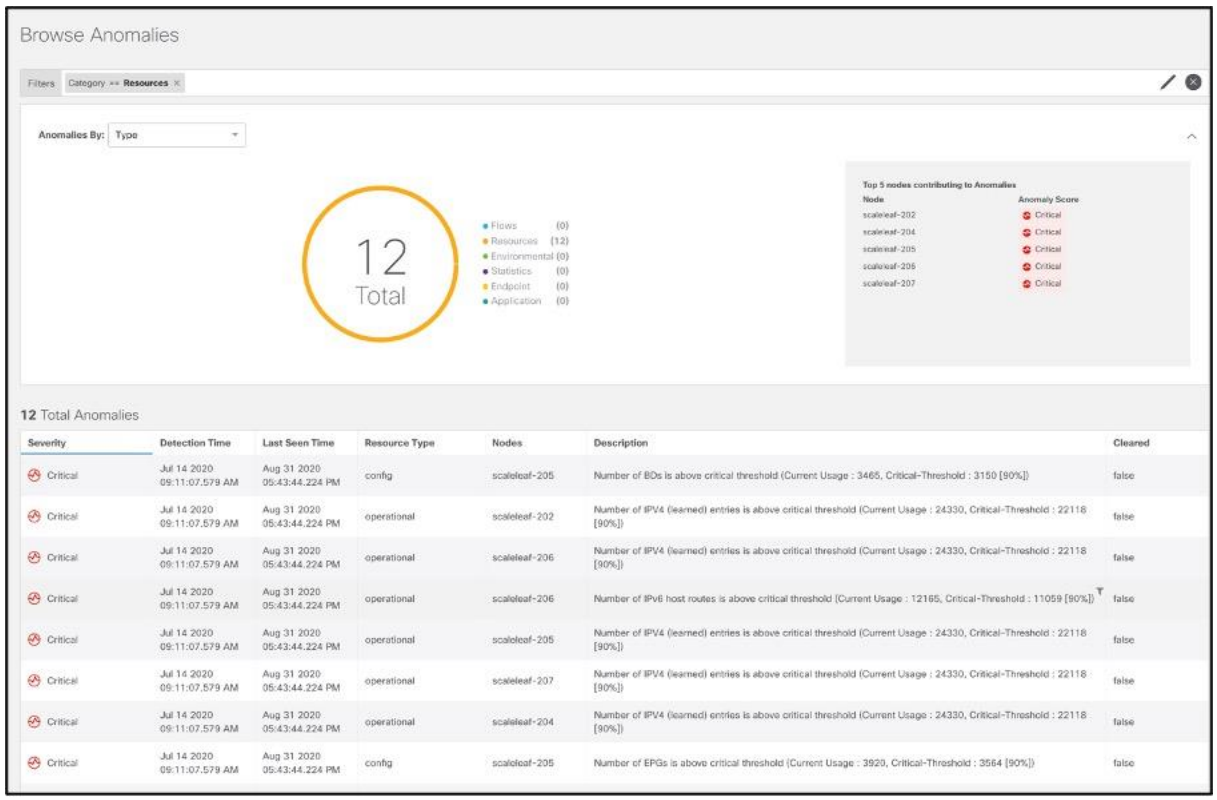
- Operational resources: Displays the capacity of transient resources that are dynamic in nature and expected to change over short intervals. Examples are routes, MAC addresses, security TCAM, etc
- Configuration resources: Displays the capacity utilization of resources that are dependent on configurations, such as the number of VRFs, bridge domains, VLANs, EPGs, etc
- Hardware resources: Displays port and bandwidth-capacity utilization



Drilling down on any device shows the details of processes that are high consumers of resources. Once. resource utilization crosses a 70 percent capacity threshold, it is color-coded yellow; beyond 80 percent, it is color-coded orange, beyond 90 percent, it is color-coded red. This proactively alerts the network operators about the specific resources that need their attention.



This also helps predicts anomalies based on historical trends and rates of change and forecasts resource shortages; see the screenshot below for an example.

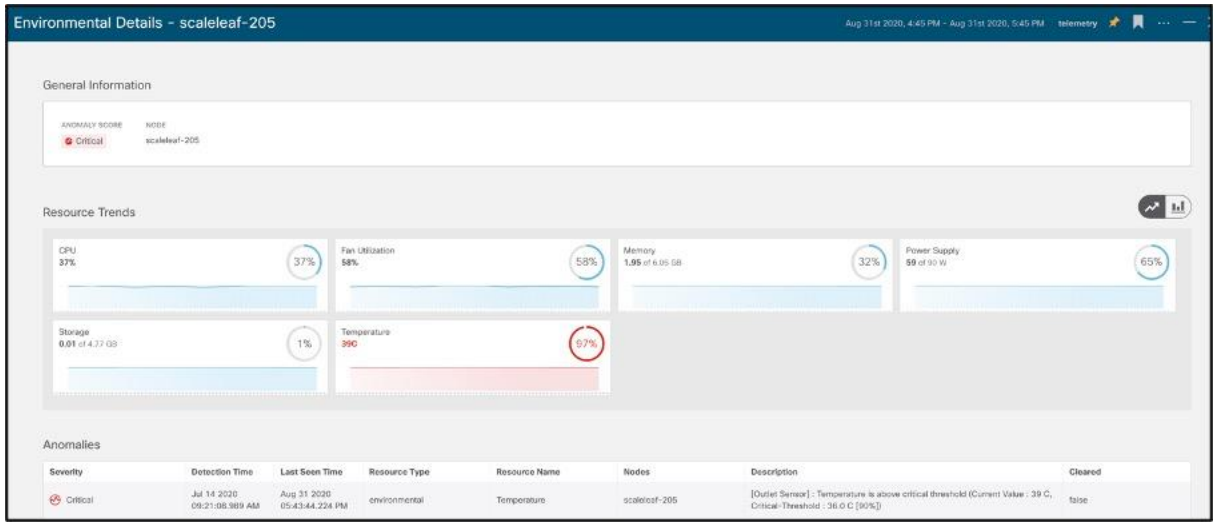


Environmental

Most often, environmental data is monitored using traditional applications like SNMP, CLI etc. Data from these applications are difficult to post process, is device specific, not historical in nature, and requires manual checks. Monitoring environmental anomalies hence becomes very reactive and cumbersome. Cisco Nexus Insights consumes environmental data using streaming Software Telemetry, baselines trends and generates anomalies every time the utilization exceeds pre-set thresholds. It enables the user to determine which process is consuming CPU, hogging memory, when storage is overfilled, process crashes or there are memory leaks – providing all this data over time with historical retention per node, to allow users to delve into specific anomalies while having full visibility.

Environmental provides anomaly-detection capabilities in hardware components such as CPU, memory, temperature, fan speed, temperature, power, storage etc. As in the other screens, it highlights components exceeding thresholds and requiring the operator's attention.

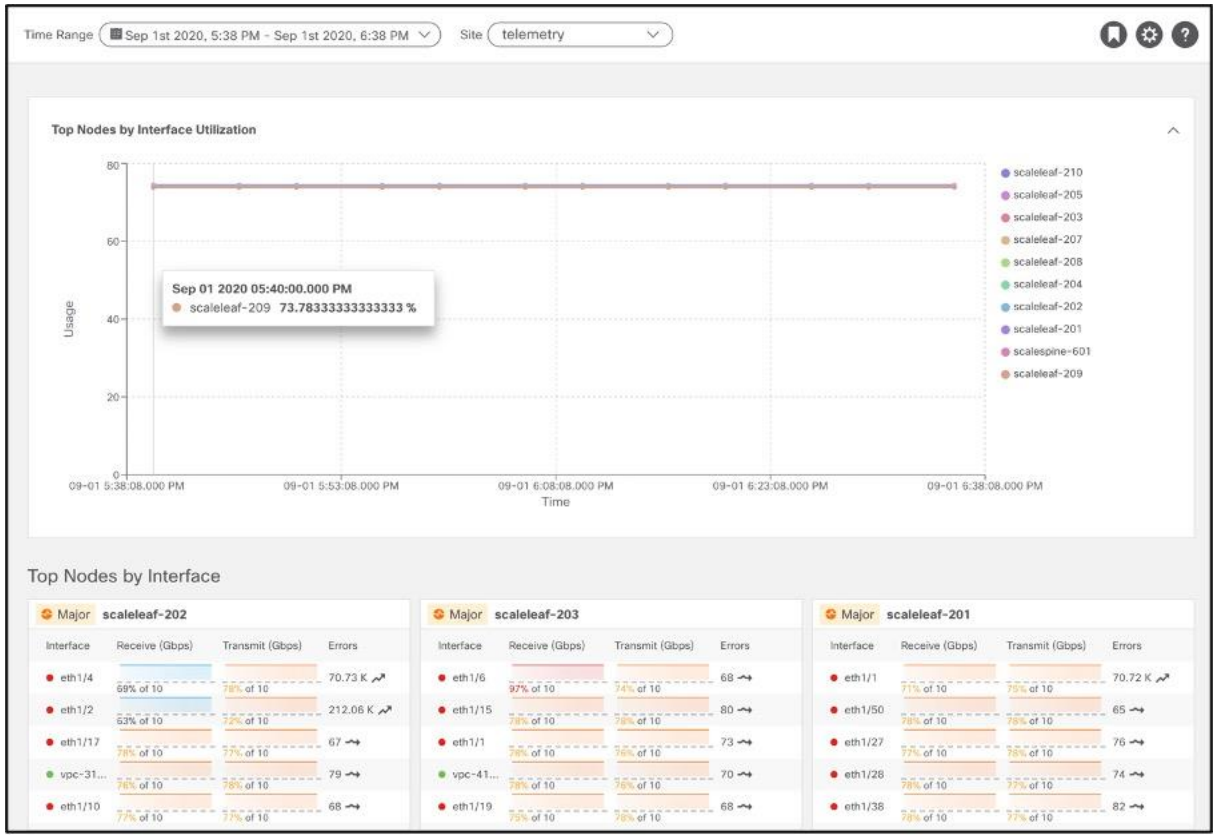
Screens with more details provide additional visibility into hardware component anomalies.



Statistics

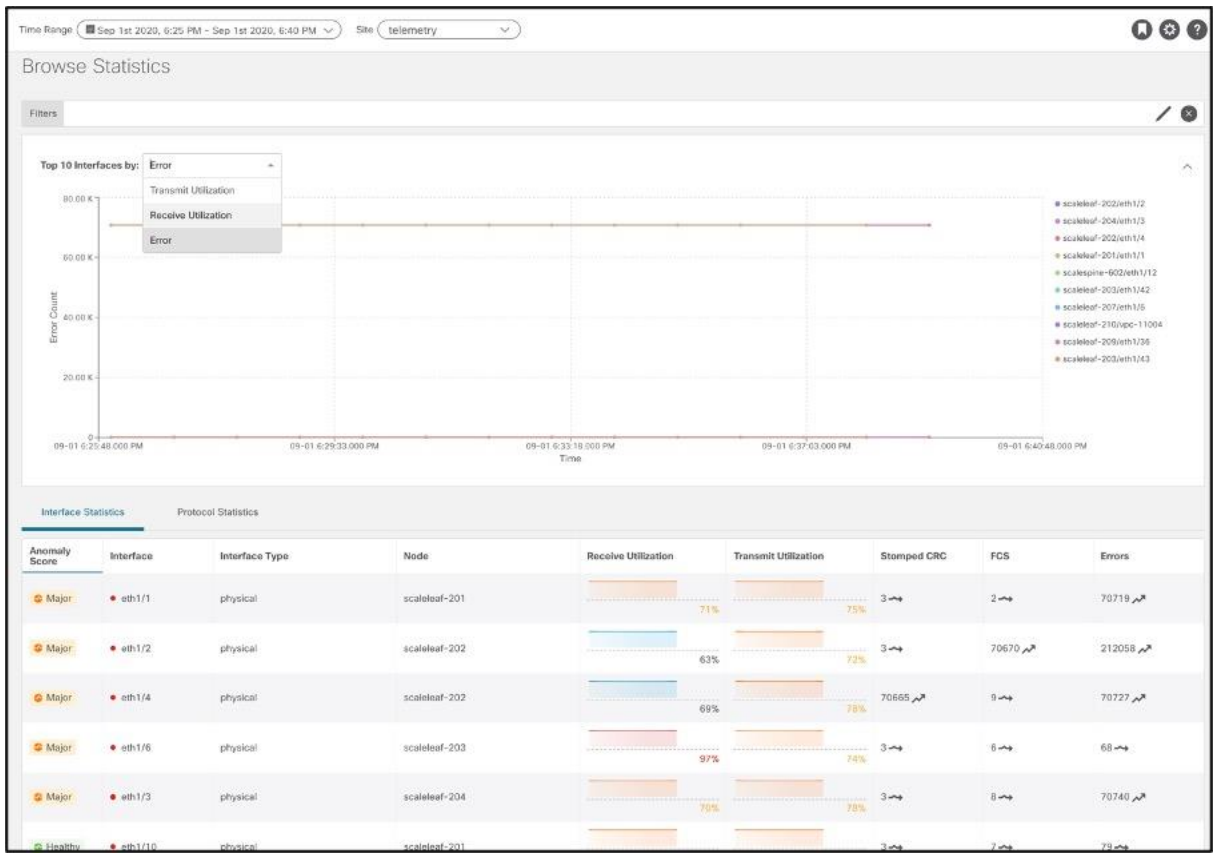
Statistics is all about interfaces and routing protocols. Cisco Nexus Insights ingests data from each node in the fabric using streaming Software Telemetry. The data is then baselined to derive trends and identify when any of these data sets suddenly show a rapid decline (for example) in interface utilization or rapid increase in drops or CRC errors over time.

Dashboard view presents top nodes by interface utilization and errors thereby allowing user to quickly identify interfaces to look into for errors.



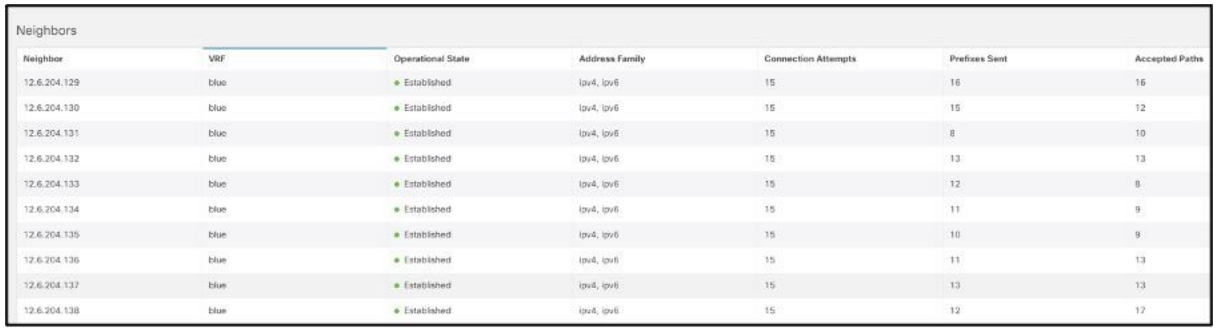
Browse view helps deep dive into Interface and Protocol Statistics.

Interface statistics provide view into trend of utilization, errors like CRC,FCS,Stomped CRC.

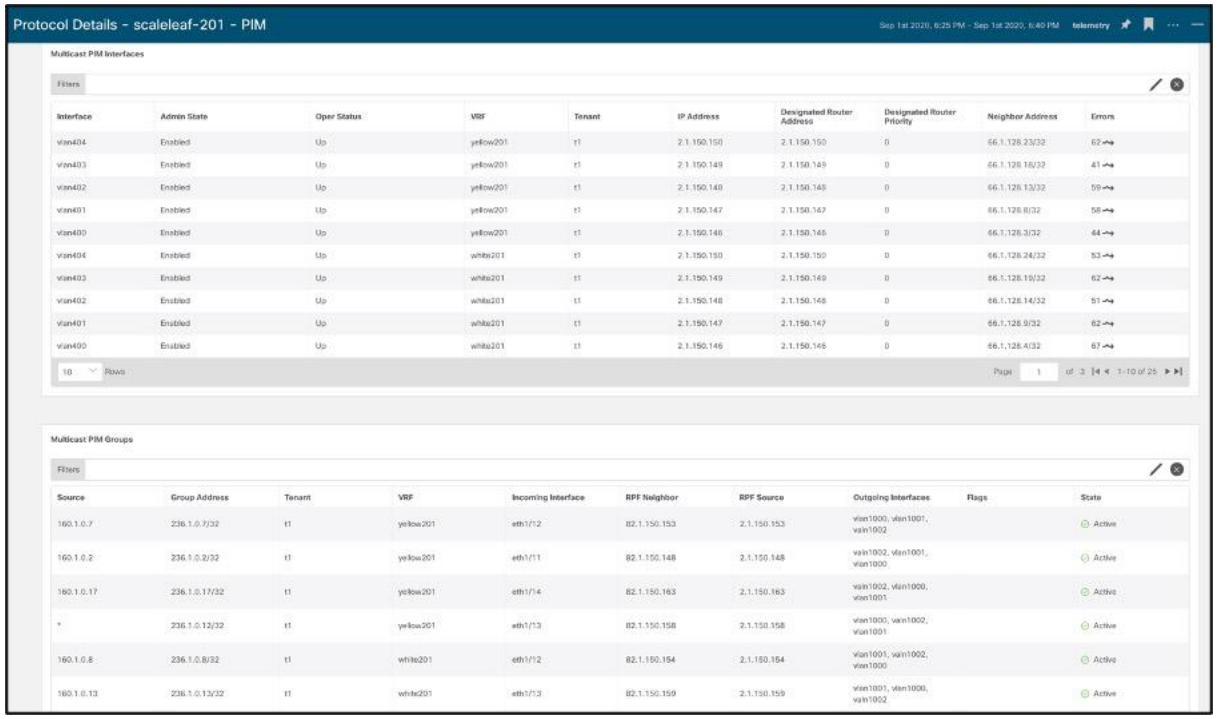


Protocol Statistics provide a view into what interfaces protocols like CDP, LLDP, LACP, BGP, PIM, IGMP, IGMP snoop are active on, protocol details like neighbors, incoming and OIFs for a (*,G), (S,G) entry along with trends of errors like a lost connection or neighbor, OIF flaps, invalid packet etc.

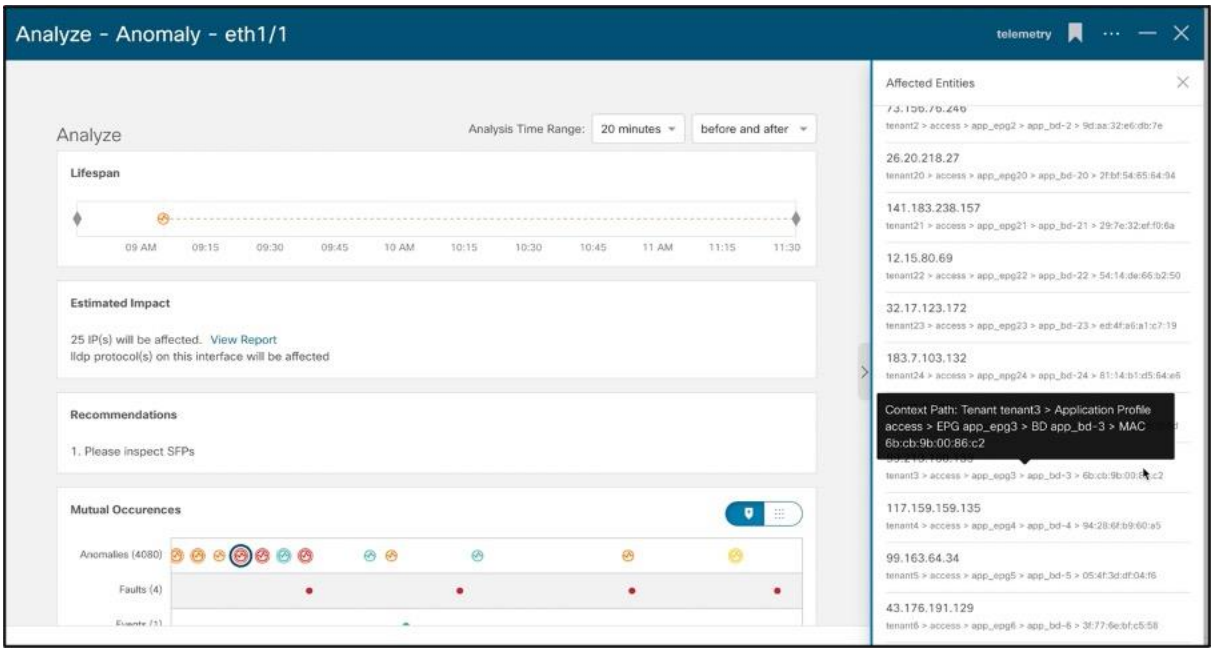
Example of BGP neighbors –



Example of PIM Interfaces and groups –



Statistical data is also used for correlation in Cisco Nexus Insights. For instance, if there is a CRC error, Cisco Nexus Insights will use other data sets to find out the estimated impact (like impacted Endpoints) and provide a recommendation based on other anomalies seen at that time (like a DOM anomaly which could potentially be causing CRC errors).



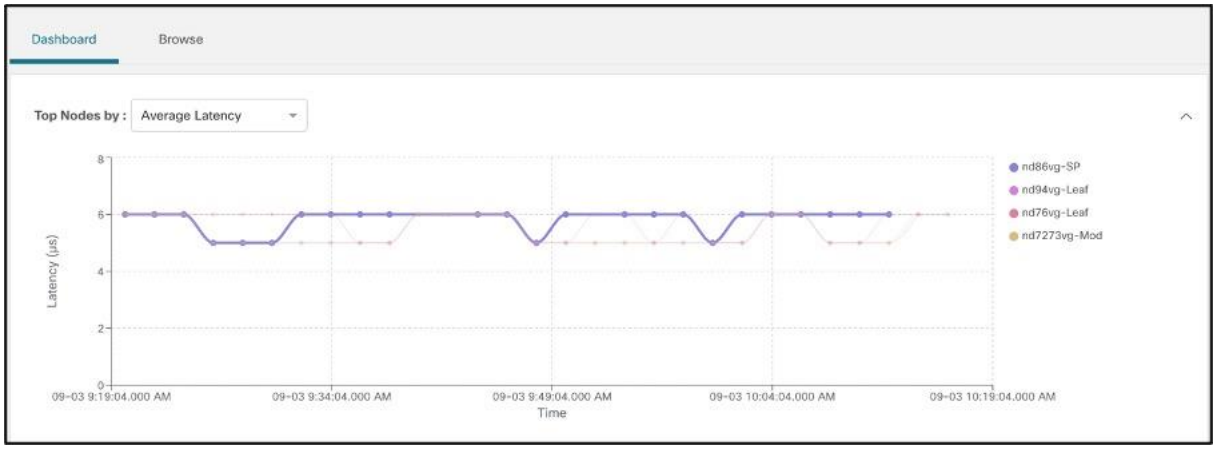
Flows

Application problem or network problem? This is a frequently asked question in the data center world. If anything, it always begins with the network. The time to innocence and mean time to resolution become critical as we deal with business critical applications in the data center. The applications we have today often have very limited insights on data plane counters, flows, latency, and drops. The nature of this data and analysis of these is very complex to begin with. Even if we get the flows from the nodes, who is to

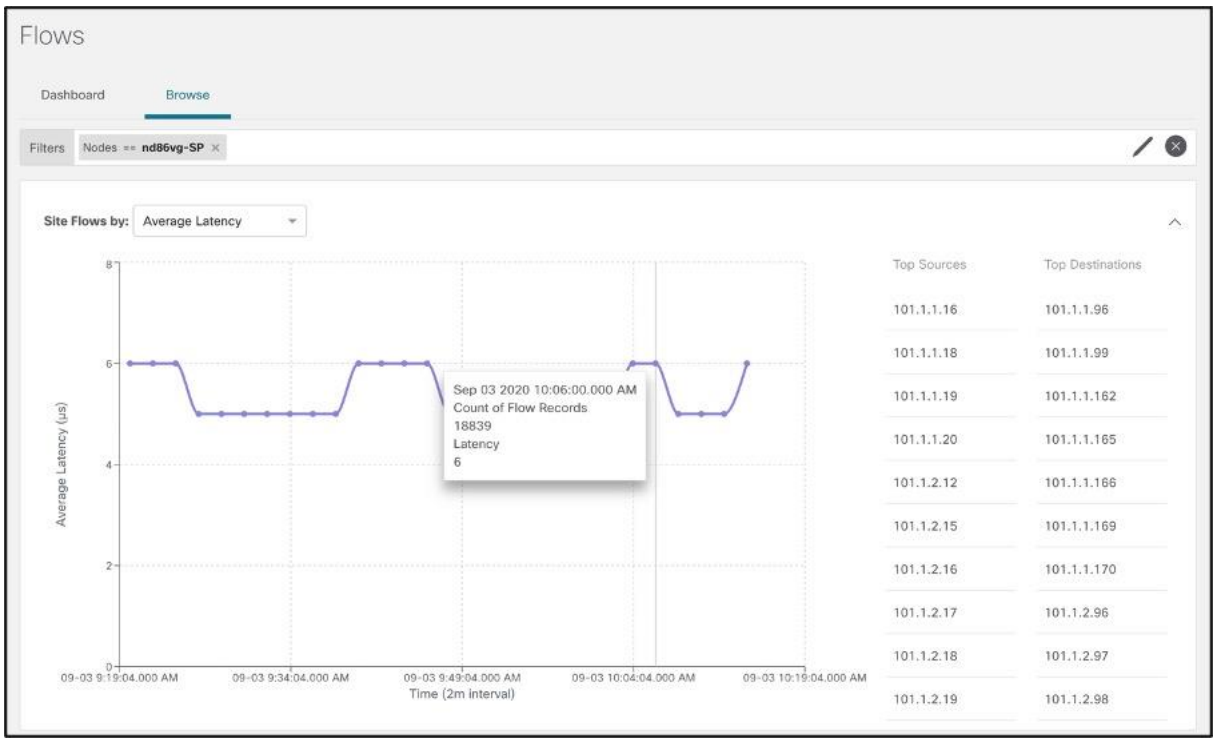
stitch them to get end to end flow path, latency? It is the user who has to do all of this which means a lot of man hours. With Cisco Nexus Insights, using Hardware Telemetry, the application consumes flow records and respective counters, correlates this data over time to provide end to end flow path and latency. Cisco Nexus Insights understands what is the “normal” latency of each flow. When the latency exceeds this normal, it alerts the users and shows the abnormal latency increase as anomaly on the dashboard.

Flow analytics dashboard attracts operator attention to key indicators of infrastructure data-plane health. Time-series data offer evidence of historical trends, specific patterns, and past issues and helps the operator build a case for audit, compliance, and capacity planning or infrastructure assessment. The flow analytics dashboard provides a time-series-based overview, as shown below, with the capability to drill down on specific functions by clicking on the graph.

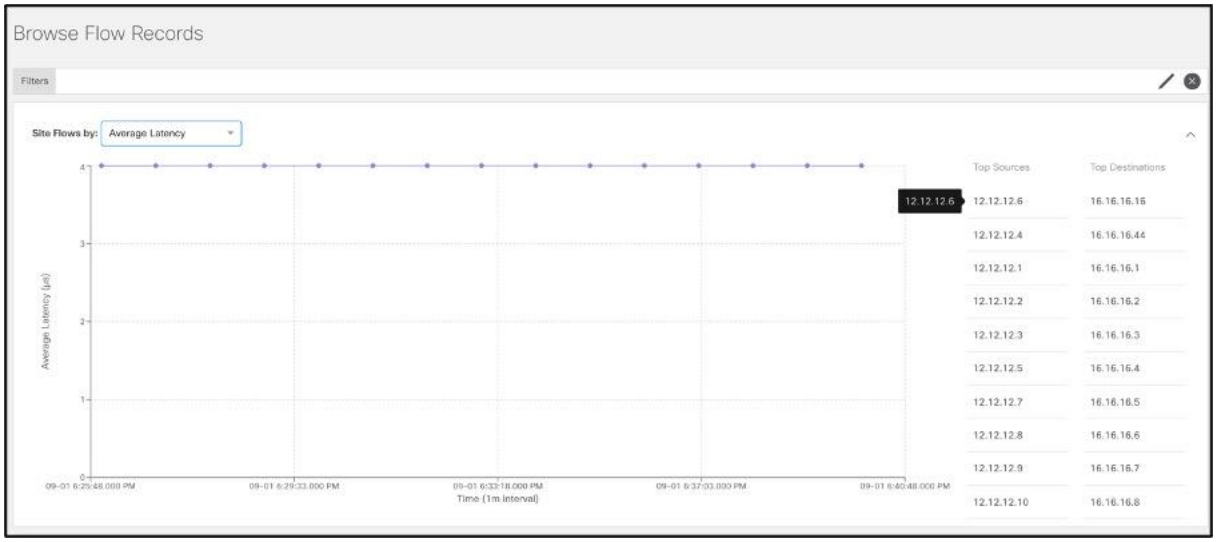
- Top Nodes by Average latency: Shows top nodes by highest average end to end latency. This results in egress nodes with flows having maximum end to end latency.



Clicking on a node results in all flows with that node as an Egress node, thereby allowing user to drill into top flows having high latency passing through a particular egress node.

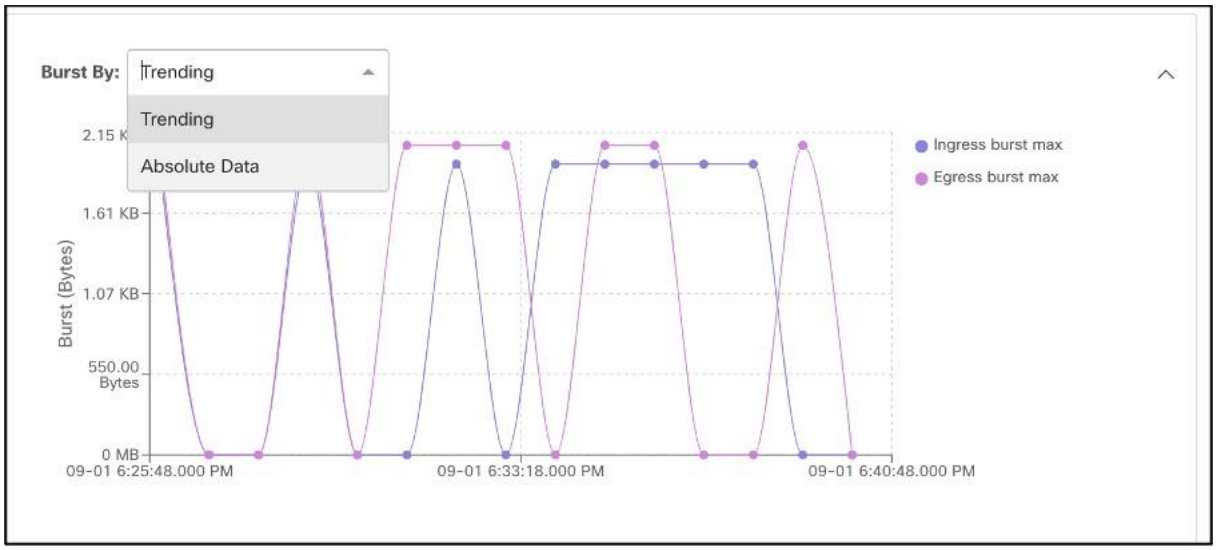


- Top flows by Average Latency: Shows time-series-based latency statistics. Clicking on a particular flow drills down to detailed flow data, including latency numbers, the exact path of the flow in the fabric, and the end-to-end latency. This takes away trial-and-error and manual steps otherwise required to pinpoint latency hot spots in the infrastructure. This leads operators to focus on the root causes of the latency and remediate them. Historical trends help operators identify persistent problems and re-evaluate the infrastructure capacity.

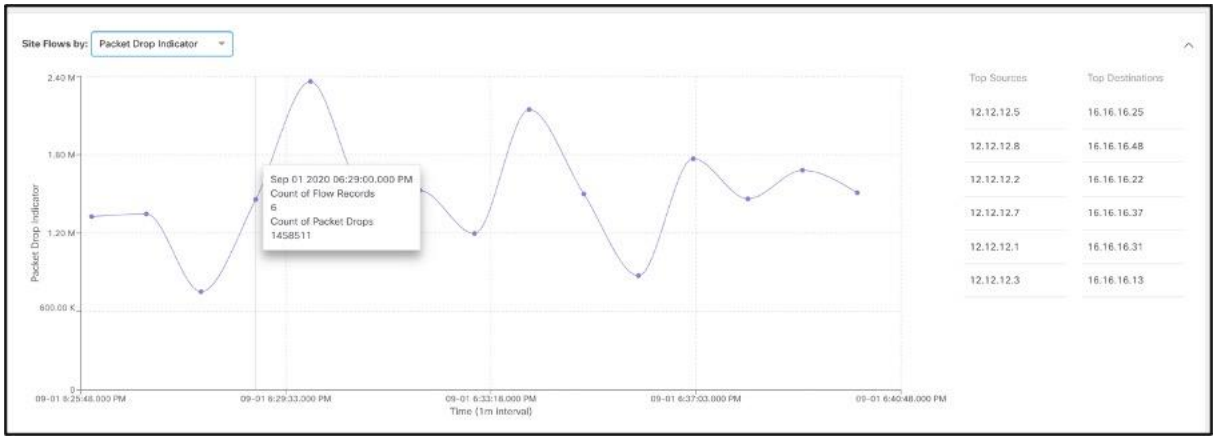


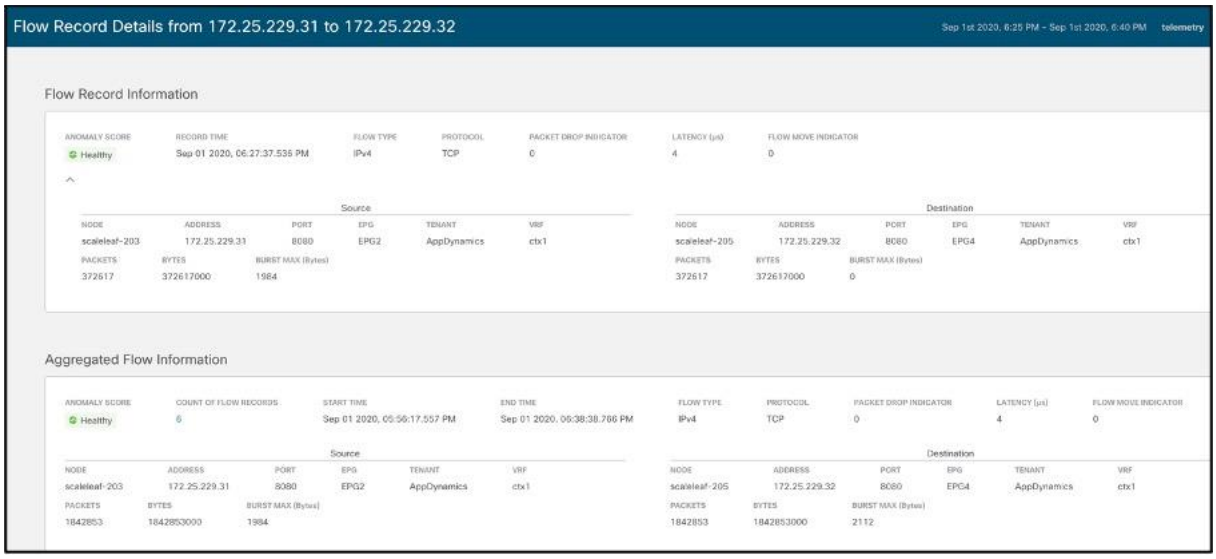
Double-clicking on the flow shows the flow level details.

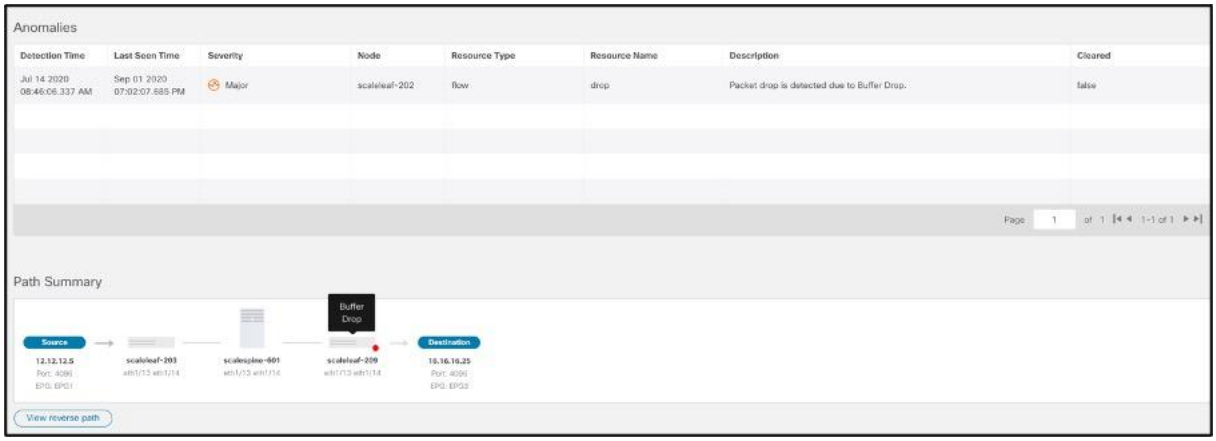
Details of the flow, such as burstiness, help identify and remediate bandwidth issues or apply appropriate Quality of Service (QoS) levels.



- Top Flows by Packet drop indicator: Shows time-series-based packet drop statistics. Clicking on a particular flow drills down to detailed flow data, including at which exact point in the fabric the drop occurred and why they occurred, as shown in the two graphics below. This saves precious time during troubleshooting and helps operators quickly identify and locate the specific potential problem-points in the infrastructure.

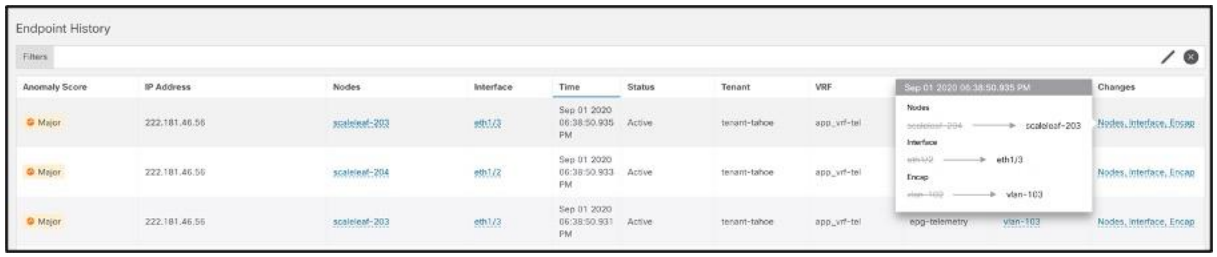






Endpoints

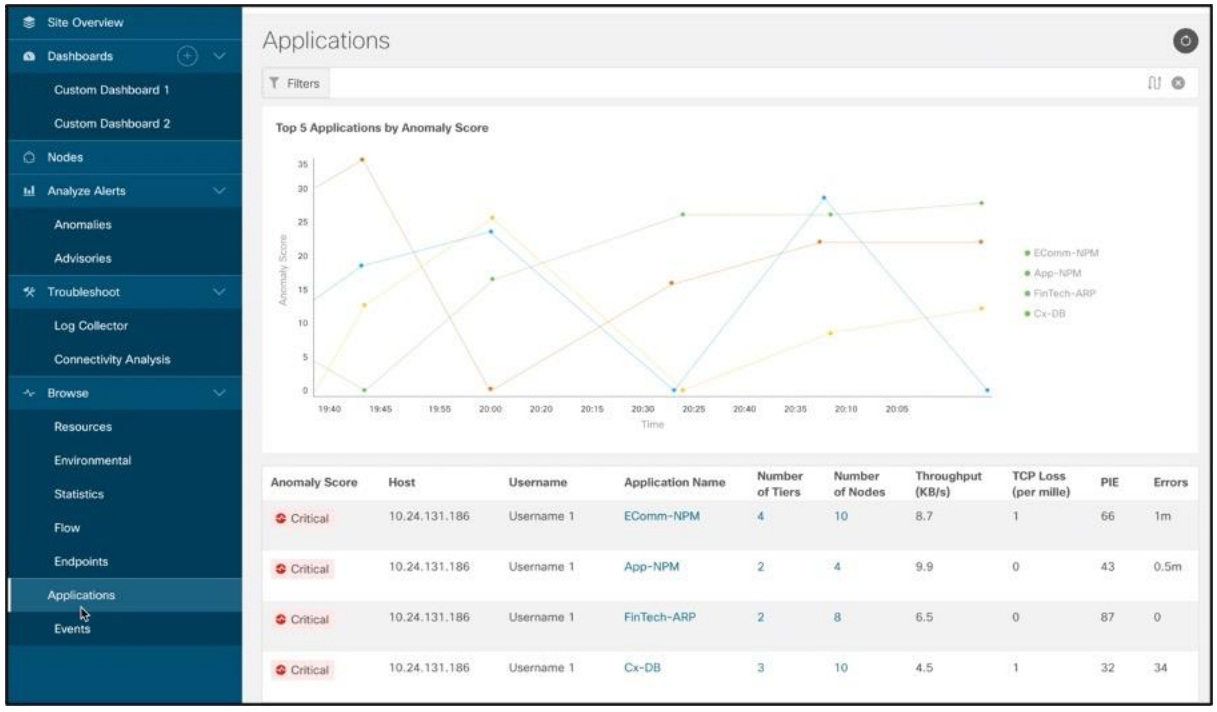
Shows time-series-based endpoint movement in the fabric, with endpoint details, and endpoints with duplicate IPs. In virtualized data center environments, this keeps track of virtual machine movement, which is extremely useful to identify its current location and its historical movements in the fabric. It provides proof points in establishing virtual-machine movements and thus aids constructively in problem solving while working with other IT teams. See the screenshot below.



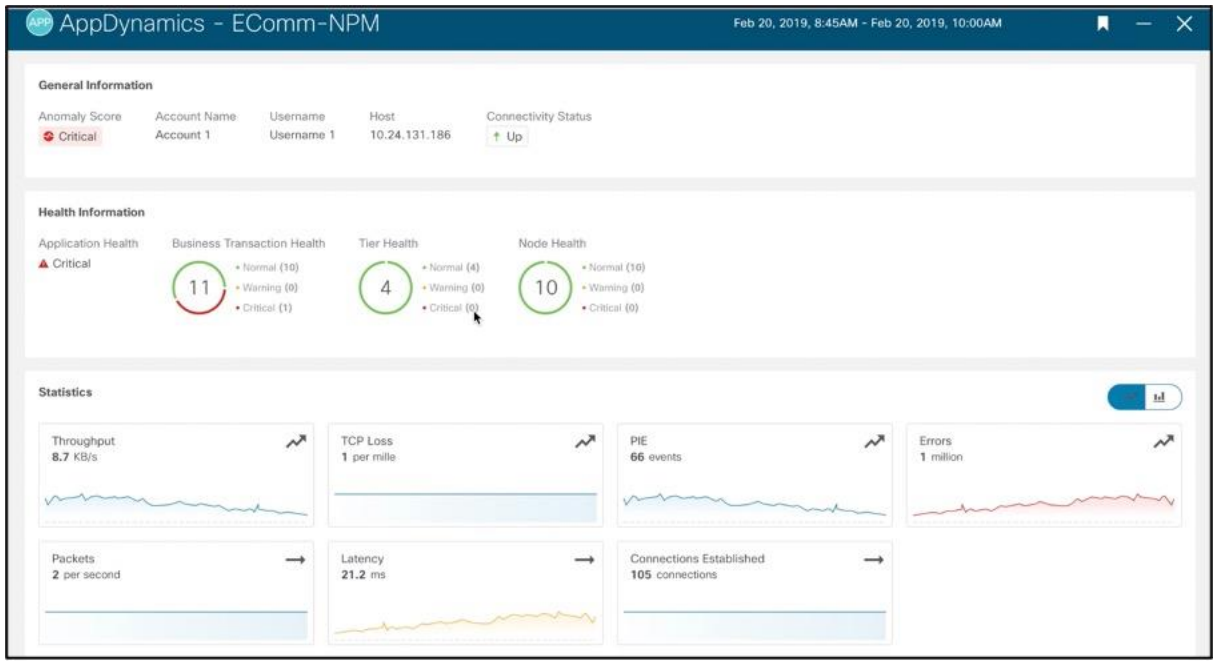
Applications

With Cisco AppDynamics and Cisco Nexus Insights integration, users get a single pane of glass for application and network statistics and anomalies. Cisco Nexus Insights consumes data streamed from AppDynamics controller and in addition to showing Application, Tier, Node health and metrics, Cisco Nexus Insights derives baseline of Network Statistics of these applications like TCP loss, Round trip Time, Latency, Throughput, Performance Impacting Events (PIE) and generates anomalies on threshold violations. For any AppDynamics flows, Cisco Nexus Insights also provides an in-depth end of end path, latency, drops if any, and drop reasons to help users identify if app slowness or issues are resulting from network issues.

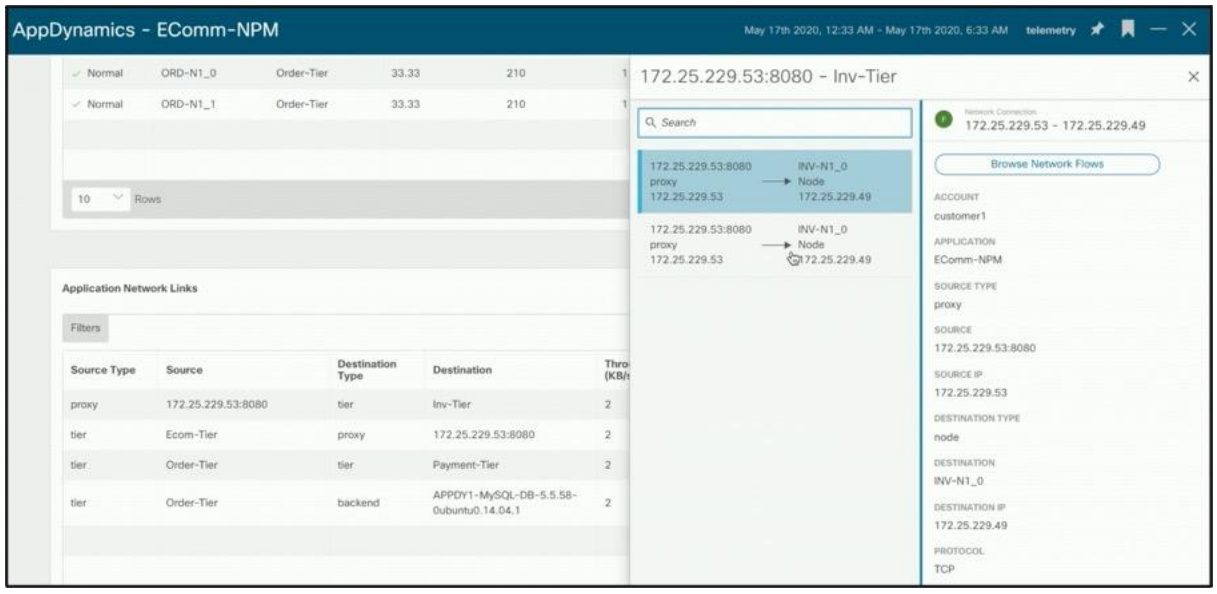
Application Dashboard showing all applications and respective statistics –



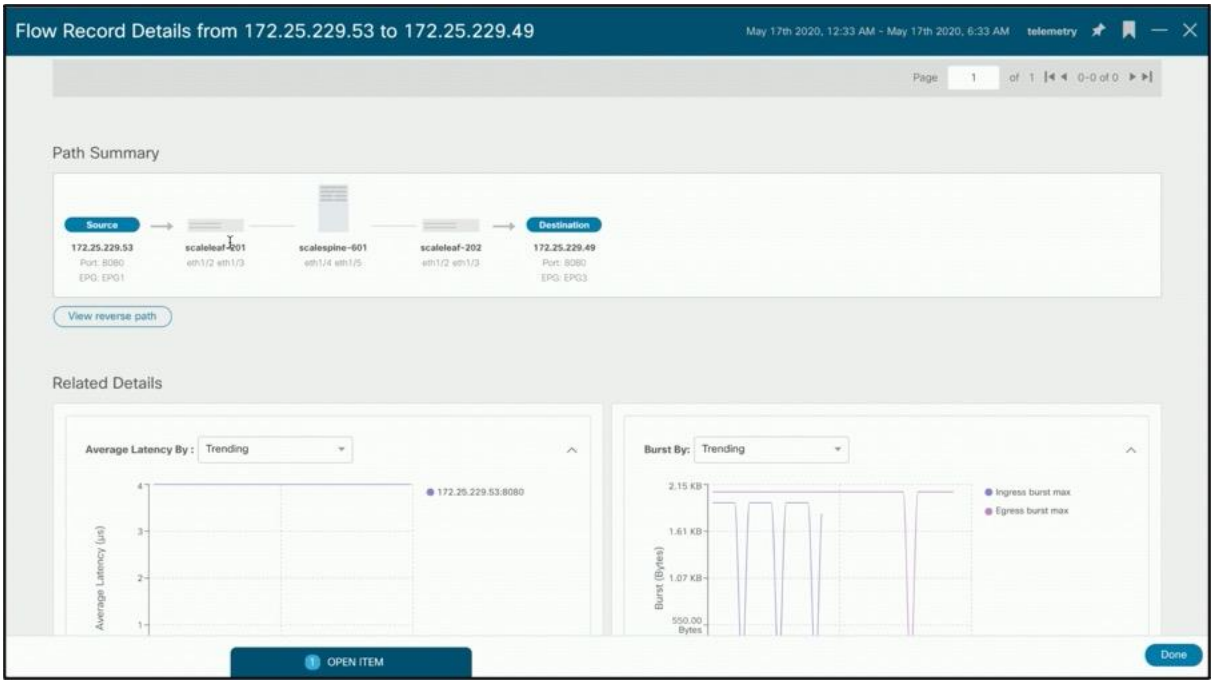
Delve deeper into an application to see health, respective Tiers and Nodes –



A network link is communication between Tiers. Cisco Nexus Insights maps links to respective flows traversing the fabric thereby allowing users to see flow details and path with drops if any –



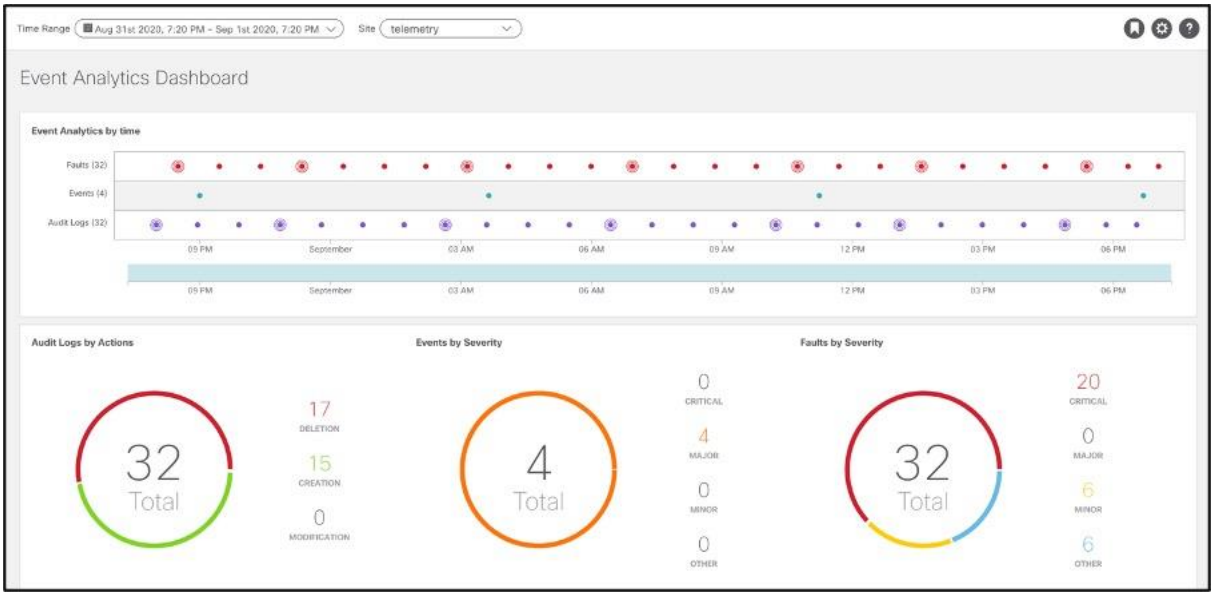
Clicking on the above flow takes you to the detailed flow page to analyze abnormal latency or drops if existing.



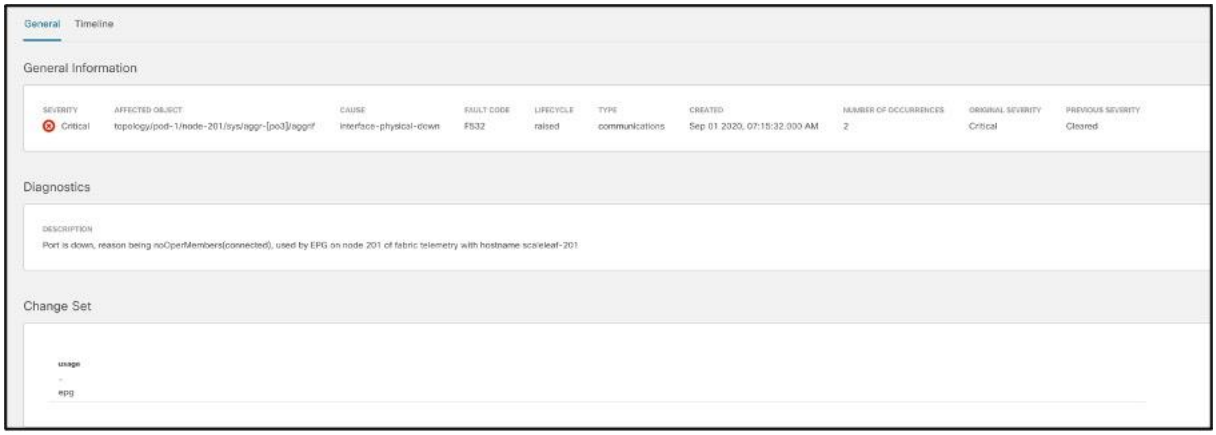
Event analytics

- Event analytics is tuned for control-plane events in the infrastructure. It performs the following:
- Data collection: configuration changes and control plane events and faults
- Analytics: Artificial Intelligence (AI) and Machine-Learning (ML) algorithms determine the correlations between all changes, events, and faults
- Anomaly detection: output of AI and ML algorithms (unexpected or downtime-causing events)

The event analytics dashboard displays faults, events, and audit logs in a time-series fashion. Clicking on any of these points in the history displays its historical state and detailed information. Further, all these are correlated together to identify if deletion of configuration led to a fault.



- **Audit logs:** Shows the creation, deletion, and modifications of any object in Cisco ACI; for example, subnet, IP address, next-hop, EPG, VRF, etc. This is useful for identifying recent changes that may be a potential reason for unexpected behavior. It can aid in reverting back changes to a stable state and help assign accountability. The facility of the filters makes it convenient to narrow focus to specific changes by severity, action, description, object, etc. Drilling down on the audit logs provides details for each log.
- **Events**: Shows operational events in the infrastructure; for example, IP detach/attach, port attach/detach on a virtual switch, interface state changes, etc.
- **Faults**: Are mutable, stateful and persistent managed objects and show issues in the infrastructure; for example, invalid configurations. This function speeds up operator action toward problem rectification, thus reducing the time lost in root-cause analysis and rectification, which usually requires multiple steps, expertise, correlation of symptoms, and perhaps a bit of trial and error.



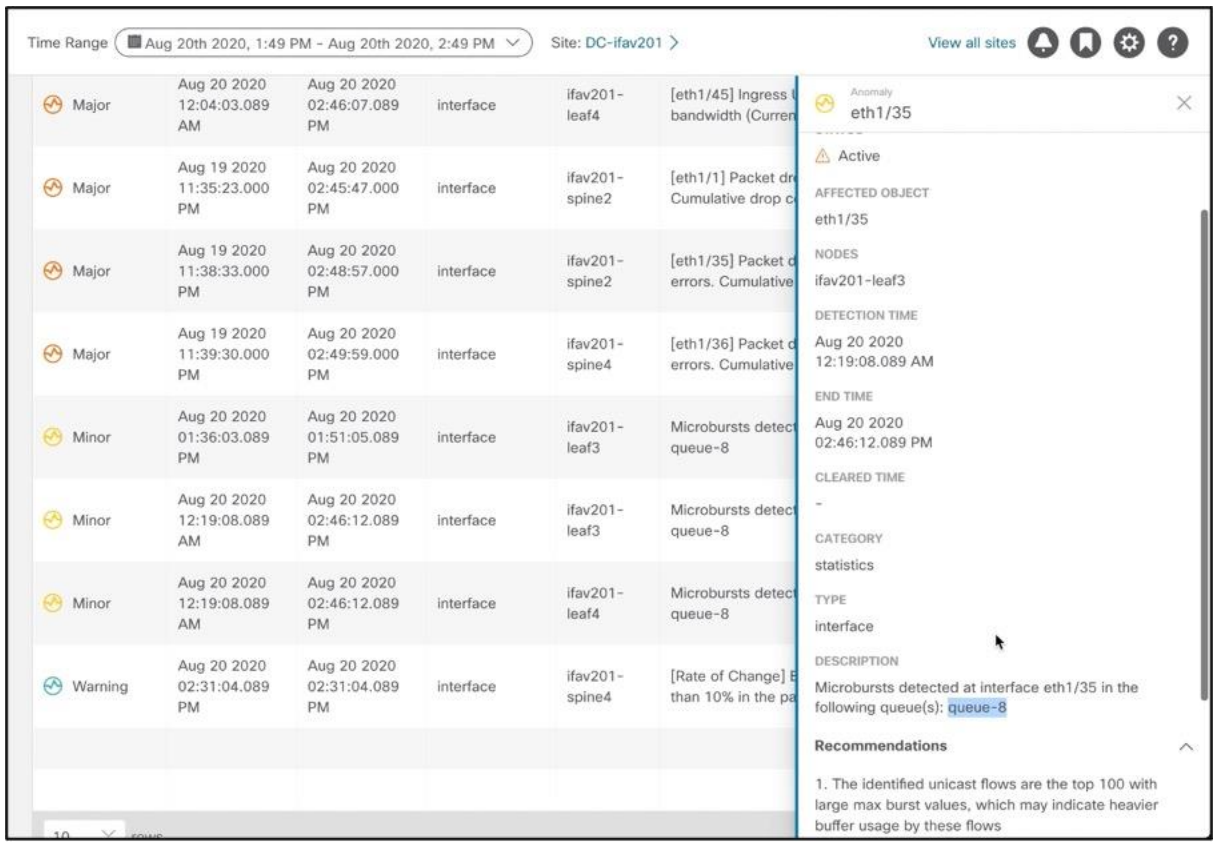
The zoom in and out function in the timeline bar helps to quickly contract or expand the timeline under investigation.

Diagnostics, Impact, Recommendation

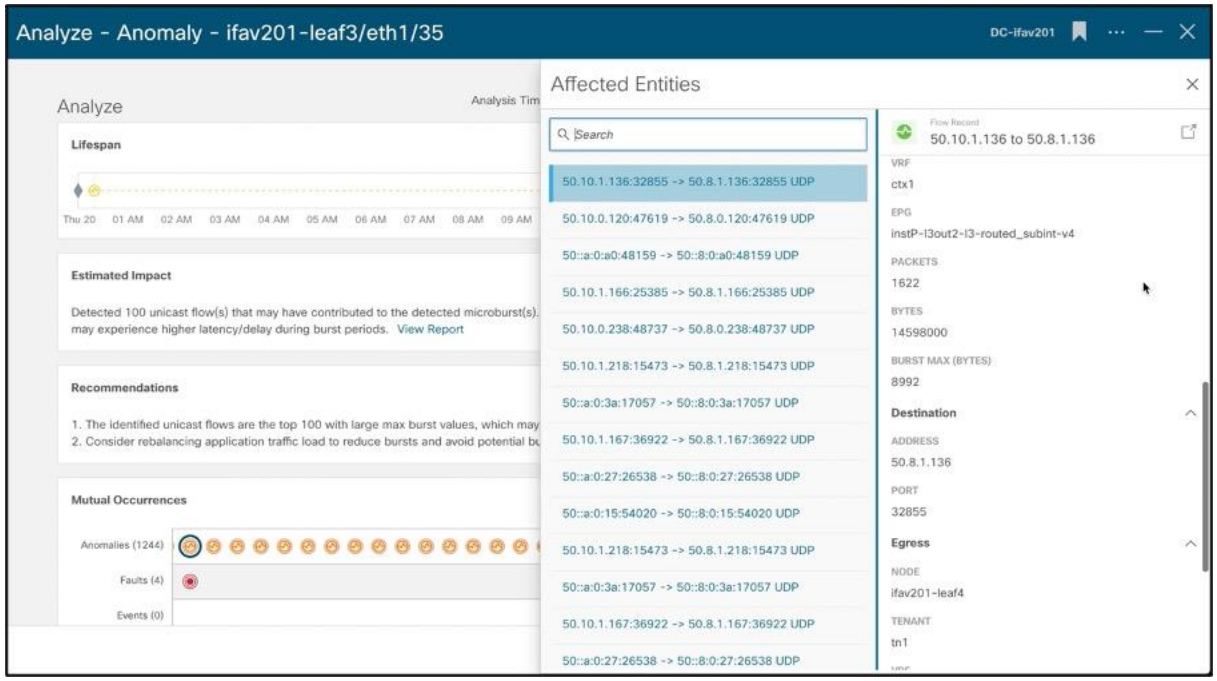
Cisco Nexus Insights monitors different sets of data from all nodes in the fabric and baselines the data to identify the “normal” behavior. Any deviation from this normal is represented as an anomaly in the application dashboard. This helps the operator spend time on resolving the issue instead of finding where in the network the issue really arose from. With the correlation algorithms that Cisco Nexus Insights has in place, in addition to the anomaly, it can also point to an estimated impact of this anomaly helping the user identify what is the potential impact of a problem. With the impact, the application will also generate a recommendation depending on the nature of the anomaly reducing the Mean Time to Troubleshooting and Resolution.

For example, let’s look at this Microburst anomaly. Microbursts are complex to identify and cause myriad kind of network issues. For applications that require reliable and low-latency networks, Microbursts can pose serious issues. Since microbursts occur in the order of microseconds, looking at a graph of overall packets-per-second will make the overall transmission appear smooth. Cisco Nexus Insights detects these microbursts due to its rapid cadence of gathering data and details what flows could be impacted due to these bursts and even causing them. It makes it easier for the operator to not only detect that a burst occurred on a particular node, interface, and queue but also flows impacted with a recommendation on how to fix this anomaly.

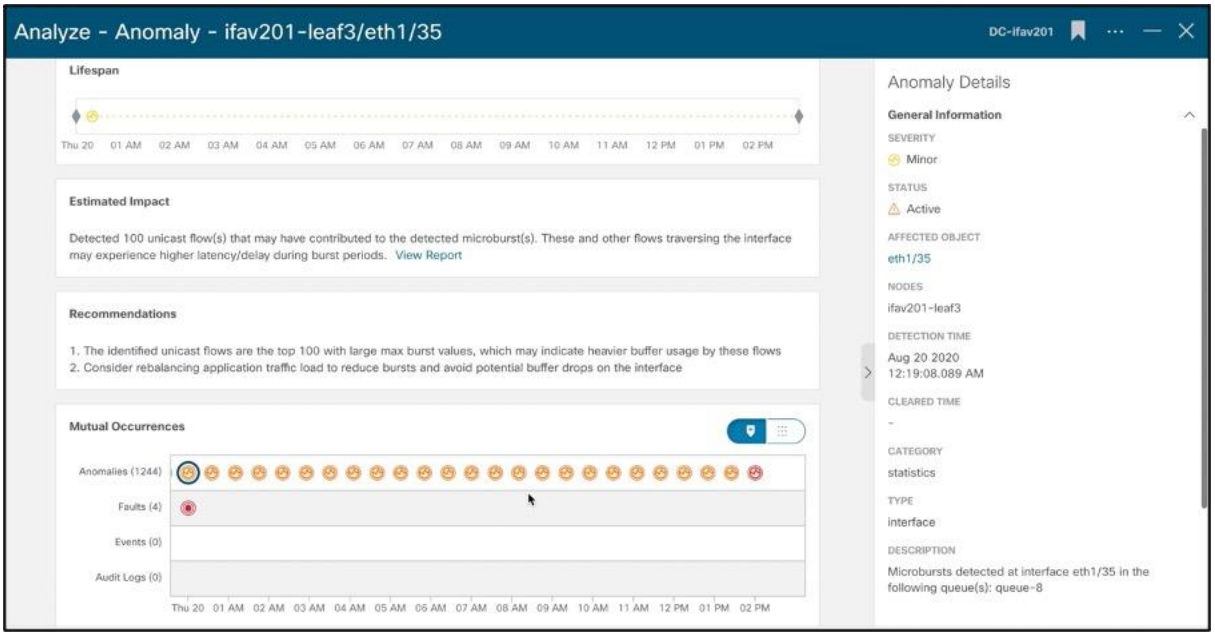
Example of a microburst anomaly –



Example of what flows could be experiencing high latency due to the occurrence of microburst at this particular time span –



Recommendations on how to remediate this anomaly along with mutual occurrences of other issues in that node as noted by Nexus Insight. It also displays Audit Logs, Events, Faults to keep all the information in one page to allow for quick troubleshooting.



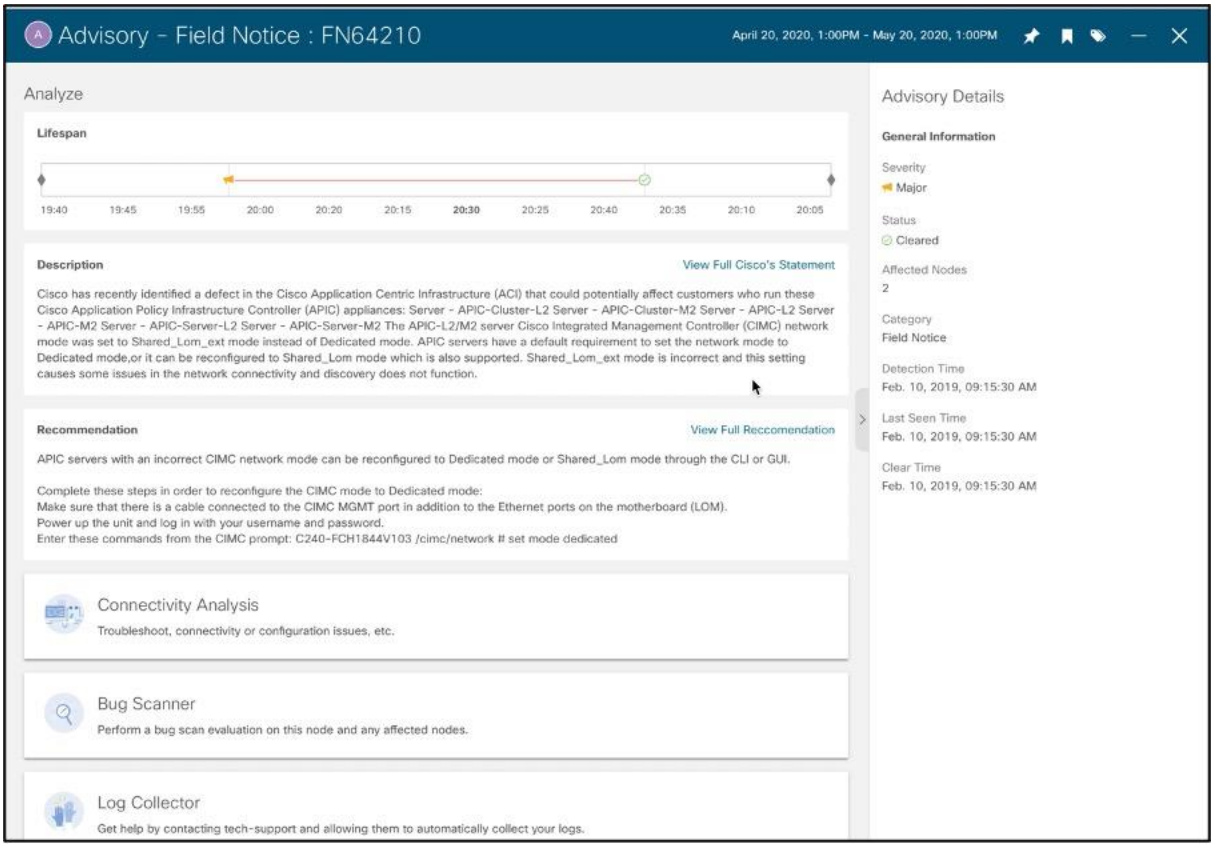
Advisories

To maintain data center network availability and minimize the downtime, it is critical for network operators to ensure that their network infrastructure is built with up-to-date switch platforms, and is running the right versions of software. It requires periodic and thorough audits of the entire infrastructure, which is historically a manual and time-consuming task. Cisco Nexus Insights turns this task into an automated process, using digitized signatures to determine the vulnerability exposure of the network infrastructure at the click of a button.

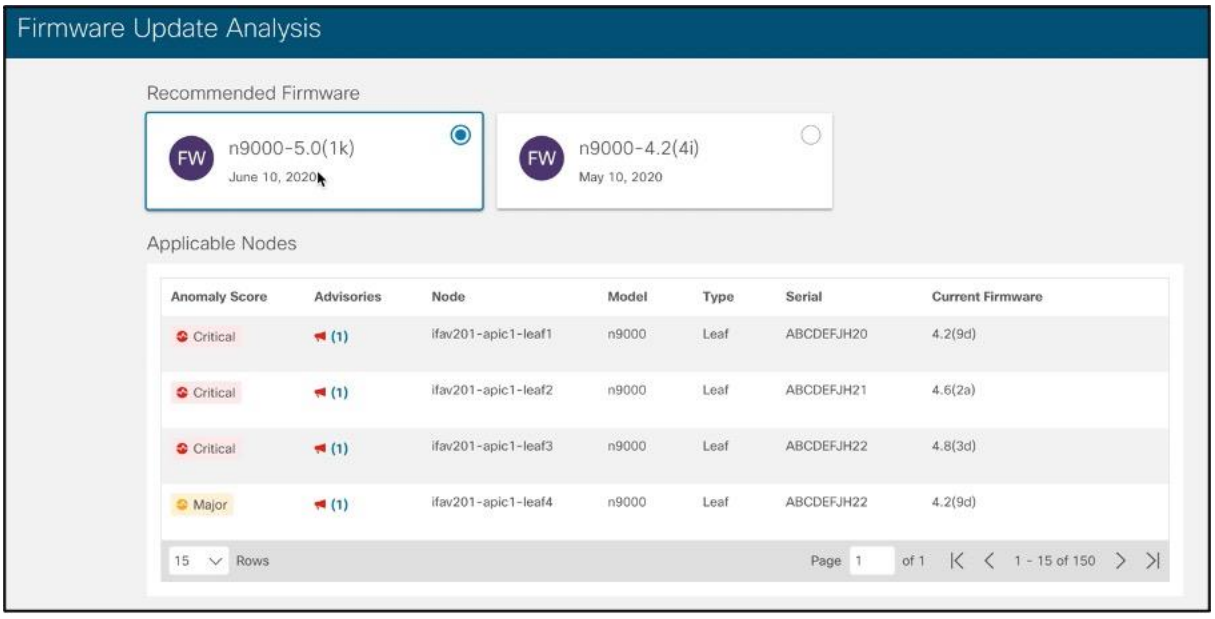
Cisco Nexus Insights scans the entire network to collect the complete information on its hardware, software versions, and active configuration. It then runs analysis against the digitalized database of known defects, PSIRTs, field notices to identify the relevant ones that can potentially impact the particular network environment, matching on its hardware and software versions, features and topologies, etc. It then proactively alerts the network operators of the found vulnerabilities, and advises them on the right hardware and/or software versions for remediation. It also analyzes and advises on whether the network is running any out-of-date hardware or software based on Cisco product EoL (End of Life) or EoS (End-of-Sales) announcement and schedule. For any of the discovered issues, Cisco Nexus Insights lists the impacted devices, vulnerability details, and mitigation steps aka advisories. With the advisories, it recommends the best software version for the resolution, and the upgrade path, either a single-step upgrade or through intermediate software versions. It also reveals the impact of the upgrade, either disruptive or non-disruptive, so that the operators can proactively plan for the upgrade accordingly.

With the automated scanning, network-context-aware vulnerability analysis, and actionable recommendations, the advisory function in Cisco Nexus Insights makes it so much easier for the operation team to maintain an accurate audit of the entire network and avoid the downtime due to product detects or PSIRTS by getting proactively alerts and taking preventative remediation actions.

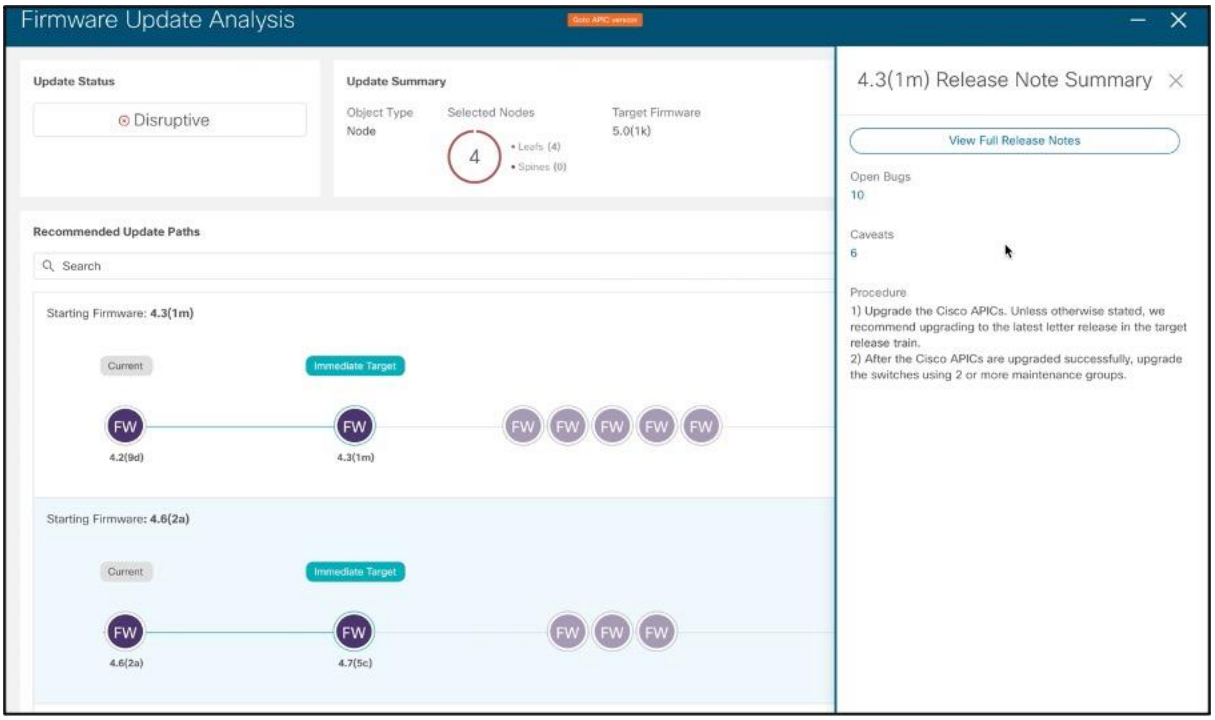
Example of an Advisory on Field Notice –



Example of firmware upgrade recommended by Cisco Nexus Insights –



Example of Upgrade Analysis – list of intermittent upgrades to get to the destination software, upgrade impact, release notes for each release linked directly in Cisco Nexus Insights –



Installation Dependencies

Cisco introduced Cisco Nexus Dashboard as a central management console for all the onboarded data center sites and a central hosting platform for data center operation applications, such as Cisco Nexus Insights. It simplifies the operation and life cycle management of various applications, and reduces the infrastructure overhead to run the different applications by providing a common platform and application infrastructure. Additionally, it provides a central integration point for API-driven 3rd party applications with the applications that are hosted on Cisco Nexus Dashboard.

Cisco Nexus Insights is a micro-services-based application designed to be hosted on Cisco Nexus Dashboard. Nexus Dashboard provides a cluster of compute nodes which are horizontally scalable. As an application natively hosted on Cisco Nexus Dashboard, the sizing and number of compute nodes required for Cisco Nexus Insights depends on the number of fabrics, number of switches in each fabric and the flows/second that the users wants the application to support.

See Cisco Nexus Dashbooard Data Sheet and Cisco Nexus Dashboard FAQ.

Software and Hardware dependencies with Scale

The NI App is supported on Cisco ACI and Cisco DCNM. Please refer to Cisco Data Center Networking Applications Compatibility Matrix for the latest software compatibility information

Licensing

The Cisco Nexus Insights App license is included as part of the Cisco ACI or NX-OS Premier license. Customers that have a Cisco ACI or NXOS Essentials license, or Advantage license can purchase the add-on DCN Day2Ops include Cisco Nexus Insights and Assurance apps.

Both the above licenses are a subscription-only Smart license. For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide. The number of device licenses required is the total number of leaf switches in the Cisco ACI fabric and/or total number of nodes in Cisco DCNM based fabric.

Pricing and ordering

For ordering information, click here. Alternately, contact your Cisco Account team to learn future pricing and get additional details.

Conclusion

Cisco Nexus Insights provides actionable insights using predictive analytics, network assurance and AIOps. It uses a vast range of information, tracking data about the infrastructure, learning new events and determining their cause, and highlighting unexpected occurrences in the network while at the same time helping network operators plan ahead, comply with policies and audits, and keep track of infrastructure capacity and uptime. Cisco Nexus Insights attempts to be an extension of the operator's brain to prevent failure in the network, or to focus attention on remedial steps to recover faster from failure when it does occur.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA Cxx-xxxxxx-xx 01/20