..|...|.. cisco

# Cisco Nexus Dashboard Insights

## White Paper, Release 6.0.1

Page 1 of 31 Cisco Confidential

### Contents

Introduction	3
Background	3
Cisco Nexus Dashboard Insights Overview	4
Key Components of Cisco Nexus Dashboard Insights	7
Browsing Cisco Nexus Dashboard Insights	11
Diagnostics, Impact, Recommendation	26
Advisories	28
Installation Dependencies	30
Software and Hardware Dependencies with Scale	31
Licensing	31
Conclusion	31

#### Introduction

Visibility, troubleshooting, root-cause analysis, and remediation of network issues are common challenges for day-to-day network 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 different events in complex IT environments to prevent or fix issues while upholding the infrastructure uptime with minimum disruption.

Cisco Nexus Dashboard Insights, a modern networking operation service, aims to simplify and automate these operation tasks. By ingesting real-time streamed network telemetries from all devices, it provides pervasive infrastructure visibility. Starting with its 6.0 release, Nexus Dashboard Insights incorporates the Cisco Network Assurance Engine (NAE) application as a part of the integrated services. With its powerful assurance and analytics engines, it can continuously verify and validate the operational states of the network while proactively detecting any drifts from the operators' intent, 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<sup>™</sup> 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 Dashboard Insights helps with Day 2 Operations of these network sites to provide visibility, assurance, proactive detection of anomalies with correlated network, and application view. This helps identify issues, accelerate troubleshooting, thereafter remediating issues on these sites. Cisco Nexus Dashboard 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 features 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 operational 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 million 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 Challenges**: 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 Dashboard Insights addresses these challenges to bring about the following benefits:

- Increase operational efficiency and network availability with proactive monitoring and alerts: Cisco Nexus Dashboard 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 Dashboard Insights also proactively identifies vulnerability exposure of the networks to known defaults, PSIRTs or field notices and recommends the best course for proactive remediation.
- Shorten the mean time to resolution(MTTR) for troubleshooting: Cisco Nexus Dashboard 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 Dashboard 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 Dashboard 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.
- Increase efficiency and reduce risks in network operations such as configuration change
  management or software upgrade. Starting with the 6.0 Release, Nexus Dashboard Insights
  provides a dry-run place for network operators to test and validate their intended configuration
  changes against a snapshot of the actual network, understanding the impacts of the changes to the
  network, having the opportunity to catch and correct any errors in the changes before entering them
  into the production network. It minimizes the risk of the network configuration changes.

#### **Cisco Nexus Dashboard Insights Overview**

Cisco Nexus Dashboard Insights is a micro-services-based modern service for network operations. 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 Dashboard Insights.

Cisco Nexus Dashboard 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 Dashboard Insights can be accessed by an external system via its REST-APIs, or exported using Kafka where the users can subscribe to relevant topics. Users can also choose to receive email notifications on anomalies with the option to customize which anomaly types they want to see along with severity and cadence.

While network monitoring, analytics and assurance are the core functions of Nexus Dashboard Insights, it offers many other capabilities and tools to increase the efficiency of network operations and to reduce the risks in network operations. Below captures the key componets of the Nexus Dashboard Insights.

#### **Network Telemetry Based Full Visibility and Analytics**

Nexus Dashboard Insights receives the network telemetry data from the network devices. It obtains the fine-grained visibility through the telemetry data, including both the control plane and the data plane operations and performance. It analyzes and learns about the baseline behavior of the network and detects anomalies in the network. The anomalies are reported to the network operations team through the Insights UI or email notification, and can be sent to other tools via programatic methods, such as Kafka export or direct API calls.

#### **Snapshot-Based Network Assurance Through Mathematical Modeling**

In its 6.0 release, Nexus Dashboard Insights inherited the assurance analysis engine from the original Network Assurance Engine (NAE) application. The assurance engine continuously takes full snapshots of the network on a regular interval, builds a mathematical model for each snaphot that represents the network and how it operates at the point of time. It then analyizes the network behaviors against this model. It checks the network configuration for any errors, examines the consistency between the network configuration and its actual operational states. Any configuration issues, any inconsistencies between the configuration and the operational states, or any incorrect behaviors of the network components will be reported as network anomalies. It assures the network configuration, the policy space, connectivity as well as the endpoint space. The assurance functions are a comprehensive collection of automated troubleshooting processes, developed based on the deep knowledge base that is acculmulated through years of network design, deployment, and support experiences.

#### **Centralized Network Insights with One View**

Organizations scale out their data centers by deploying multiple data center sites that often are geographically dispersed. This creates a fragmented view of the network infrastructure that creates challenges for Day-2 operations teams leading to slower incident detection, correlation, and resolution. Starting with Nexus Dashboard 2.1 release, users can link their multiple Nexus Dashboard clusters together to operate their network sites from this one central point and obtain an aggregated view of the operations of all their network sites. Enabled by the "One View" capability on Nexus Dashboard, the Insights service itself can now provide its users with the centralized visibility across all the network sites on the linked Nexus Dashboards and enable the smooth navigation among the different sites on the same Insights UI.

#### Pre-Change Analysis for Risk-Free Configuration Change Management

Network Configuration Change management has been considered as an operation with risks by nature because the network team did not have a good tool to fully qualify the changes before implementing the changes into the product network. Pre-Change Analysis is a function originally offered by Cisco Network Assurance Engine (NAE) to tackle this challenge by giving the network team a tool to fully test drive their intended configuration changes. Cisco NAE is integrated into Cisco Nexus Dashboard Insights Release 6.0. Now the Insights users can take full advantage of the same pre-change verification capability to proactively validate the configuration changes against the latest snapshot of the network. This is a long-desired capability by the network operations team. Now, they can simply submit their intended changes to the Insights service. The Insights service will analyze the impacts of the changes to the network, calling out any errors or potential issues if there are any. The network team gets an opportunity to review and correct the errors and only implement the fully qualified configuration changes to the network. This pre-change

analysis function removes the guess work from network configuration change management, minimizes the risks of the change management and therefore increases the availability of the entire network.

#### Automated Continuous Compliance Assurance

Most organizations have some types of compliance requirements for their networks. It can be industry regulatory compliance requirements, or the organizations' internal requirements for security or business functions. Additionally, the network teams often have their own established best practices, standard configuration, or standardized naming conventions that they would like to implement or enforce during the ongoing network operation. All these requirements can be assured by Nexus Dashboard Insights through its compliance assurance functions. These capabilities are originally in the Cisco NAE application, and now become a part of the Insights service since its 6.0 release.

The compliance assurance functions in the Insights service gives the network team one more place to directly describe and submit their intents for the network, then automatically and continuously verifies and validates the intents in the network for them. Any deviation from the intents will be captured as compliance violation anomalies and reported to the network team immediately. With the automated, continuous security, and configuration compliance analysis, Nexus Dashboard Insights enables true intent-based network operation.

#### Query your Network Like a Database Using Natural Language

Explorer, originally from the Cisco NAE application, is now a part of Nexus Dashboard Insights since its 6.0 release. It is a tool for the network teams to conveniently explore the entire network like a database using natural-language-based queries. Explorer can answer questions such as "Can EPG A talk to EPG B?" "How can they talk?", "What VRFs are deployed in my tenant space X?", "What endpoints are attached to the leaf switch 101 port 1/1?". It is a highly efficient way to find the objects and discover how the objects are associated with one another in the network.

Network operators can easily create natural language queries to get their discovery tasks done efficiently. For example, they can quickly locate a specific object, such as a particular endpoint out of thousands of them in the entire network , or just simply get a per-device or network-wide inventory of certain network object types in the network, or find out the communication relationship between different objects throughout the network that can either communicate or are isolated from each other using past or present snapshots of the network.

Explorer is an effective tool to assist in the troubleshooting of the network configuration, operational states, and network change planning, etc.

#### Network Software Upgrade Made Easy and Safer

Starting with its 6.0 release, Nexus Dashboard Insights offers software upgrade analysis to ease and reduce the risk of a software upgrade workflow. It can assist the network team to choose the right target software version for the upgrade. Based on the pre-upgrade analysis results, the network team can prepare for the upgrade by clearing up the identified issues or faults in the network if any, get a clear expectation of what issues will be solved by the update, and be aware if the target version would introduce any new caveats. The post-upgrade analysis shows the network team the differences in the network state (endpoints, routes, interface status, etc.) before and after the upgrade, so they can quickly tell if the

network has come through the upgrade without any issues, or if something is missing. The pre and post upgrade analysis makes the software upgrade operation easier and safer.

#### **Key Components of Cisco Nexus Dashboard Insights**

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

#### **Cisco Nexus Dashboard Insights Site Overview**

It provides a direct view into the site level anomalies (issues) that need attention, all of which are calculated by Cisco Nexus Dashboard Insights. The anomalies are consolidated into the Overview screen and sorted by category and severity. The Insights service further groups the anomalies by top nodes, timeline view, site health score, and advisories. Lastly a node inventory by roles, and corresponding health score, allows click access to the in-depth node-level visibility which gives all details on the nodes including trends of anomalies observed.

Cisco Nexus Dashboard Insights also allows users to create Custom Dashboards for any charts as seen in the service.

diade Nexus Dashbo	pard	Feedback Hep - admin -
₹ Insights		Central Daethours 🙆 🔝 🧕
Overview     Destroard     Overview     Destroard     Overview     Destroard     Overview	Overview within the last 2 hours ~	Last Updated. 1 minute age
tal Analyze Alanta ∨ Concelanos % Troubleshoot ∨ & Browse ∨ £ Change Management ∨	Aberts Summary (A Advisation (B) Major October (B) Major October (B) Major (C) Major	+Haminy +Haminy +Check +Haminy +Chec
	Aint Detection Trimeline           Image: Second sec	a2 es     abres     abres     abres       Adviseres Breaktown By Cangary >
	Top Nodes - LeadS1 Node - LeadS1 Major D Major Reserved Major Reserved Major	Ware a

#### Interactive Network Topology Overlayed with Operational States

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.



#### **Analyze Alerts**

In addition to the rolled up summary presentation of the anomalies and alerts, Nexus Dashboard Insights users can also interactively browse, search, and analyze the anomalies and advisory alerts generated by the service.

Anomalies are the issues found around the following network operations:

- Resource utilization
- Environmental issues like power failure, memory leaks, process crashes, node reloads, CPU, memory spikes
- Interface and Routing protocol issues such as 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 or policy drops, etc. using Flow Table Events (FTE) which is another form of hardware telemetry
- o Endpoint duplicates, rapid endpoint movement, rogue endpoints
- o Issues in the network configuration --- detected and reported as change analysis anomalies
- Violations to the compliance requirements for compliance assurance --- detected and reported as compliance anomalies
- Issues found in the network forwarding analysis and assurance --- detected and reported as forwarding anomalies
- Application issues as calculated by AppDynamics and Cisco Nexus Dashboard Insights (AppD Integration required)

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

**Advisories** – Nexus Dashboard Insights can identify Field Notices, software/hardware products EOL/EOS announcements, as well as PSIRTs that can potentially impact the network sites that it is monitoring, and generate advisory alerts to the network operations team. The alerts consiss of relevant impacts of the identified Field Notices, EOL/EOS or PSIRTs, as well as the affected devices in the network. Nexus Dashboard Insights also performs targeted bug scanning to alert the network operations team about the known defects that are relevant to their specific network environment based on its hardware/software versions, features that are enabled in the network, as well as network configuration. This helps the network team to carry out the remediation actions on the affected switches quickly or to form a software or hardware upgrade plan accordingly.

#### **Network Delta Analysis**

Starting with the 6.0 release, Nexus Dashboard Insights can run network delta analysis. It is a capability inherited from the Cisco NAE application. Users of the Insights service now can select any two snapshots of the network site and ask Insights to analyze the differences between them, including configuration differences, and differences in anomalies and advisories that reveal the differences in how the network was operating at the two points in time.

Understanding the differences in the network configuration and operations is important and extremely helpful for many different scenarios. When troubleshooting a network incidence, the differences in the network configuration or operations can often help identify the cause of the issue. When performing network maintenance, such as configuration changes, software upgrade or hardware replacement, it is helpful to check the differences in the network before and after the maintenance task. It can tell whether the network has converged or restored to how it should be after the task, or whether the task has resolved the issues that it is supposed to resolve, or if it has introduced any new issues. The Delta Analysis function increases network operation efficiency for these maintenance tasks, and helps reduce the Mean Time to Resolution (MTRR) for troubleshooting.

#### Log Collector

Nexus Dashboard Insights can assist the network team to collect tech-support logs per node. It turns the tedious task into a simple one-step automated job. 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).

Collection - TAC	ASSIST_Instant1		Aug 31st 2020, 6:01 PM - Aug 31st 2020, 6:16	PM DC-ifav201
Status	General Information			
OVERALL STATUS	START TIME NODES JOB IF	D		
Complete	Aug 31 2020, 05:52:00.716 PM 1 TACA	ASSIST4dbfc86c-obod-11ca-a2f2-a61c36f9201c		
Selected Nodes				
Node	Version	Status	Actions	
ifav201-leaf10	n9000-15.1(0.76)	© Complete	(	)
			Do	wnload File 1
			Do	wnload File 2
			Do	wnload File 3
			Up	load File 1 to TAC Assi
			Up	load File 2 to TAC Assi

#### **Connectivity Analysis**

Allows user to run a quick or full analysis for a flow within one NX-OS network site or spanning multiple NX-OS network sites to:

- o Trace all possible forwarding paths for a given flow across source to destination endpoints
- o Identify the offending device with the 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

The following screenshot shows an example of 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.



Site-	Site-1-BG-2									
Inte	erfaces									
	Ethernet1/41 Ethernet1/42 Ethernet	ernet1/24 Ethernet1/23								
	Description	Command	Status	Error						
	Physical Front Panel Port Link state validator	show consistency-checker link-state interface Ethernet1/23 brief	⊘ Pass							
	L3 physical routed port state validator	show consistency-checker I3-interface interface port- channel1301 brief	⊘ Pass							
	L3 physical routed port state validator	show consistency-checker I3-interface interface Ethernet1/49 brief	⊘ Pass	*						
	Physical Front Panel Port Link state validator	show consistency-checker link-state interface Ethernet1/41 brief	Pass							
	Physical Front Panel Port	show consistency-checker link-state interface	Pass							

#### **Browsing Cisco Nexus Dashboard Insights**

Let's delve into the Browse functionality available in Cisco Nexus Dashboard 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 this, Cisco Nexus Dashboard Insights baselines utilization of resources, monitors trends, and generates anomalies on abnormal usage of resources across nodes to help a 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.

Network Insights - Resources	Time Range 🗍 Aug 31st 2020, 4:40 PM - Aug 31	st 2020, 5:40 PM	Site: DC-ifev201 >			View all sites 🔕 🔘 😂 🔮
<ul> <li>Site Overview</li> <li>Dashboard</li> <li>Construction</li> </ul>	Resource Utilization					
kil Analyze Alerts	APIC Capacity					
Anomalies ***	Bridge Domains 24 of 15K	Contracts 18 of 10K	1%	Endpoint Groups 23 of 15K	1%	Hypervisors 3
A Browse A	IP Endpoints 2015 of 225K	L3 Contexts 20 of 3K	1%	L4/L7 Devices 0 of 1.2K	0%	L4/L7 Graphs 0 of 1K 0%
Environmental Statistics				Resource not uti	Rzed	Resource not utilized
Flow Analytics Endpoint Analytics Event Analytics	Proxy Database Entries 6086 of 450K	Tenants 15 of 3K	1%	VMM Endpoints 20		Virtualization Ratio 0%
	Top Nodes by Utilization					
	S Healthy Ifav201-spine3		G Healthy ifav201-leaf3		G Healthy	ifav201-leaf4
	Port Usage 4 of 1 Ingress Port Bandwidth 24.78 Egress Port 24.78	8 ports of 160 Gaps of 160 Gaps	Port Usage	9 of 54 ports 2033 of 12.29K 2019 of 12.29K	Port Usage IPV6 Host Ri IPV6 Reame	2 of 54 ports butes 1512 of 12.29K d) 1506 of 12.29K
			IPV4 (learned)	2021 of 24.58K	IPV4 (learner	d) 1509 of 24.58K

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.

source Details - se	caleleaf-207						talamatry 🖈 🗮	
General Information								
ANOWALY SCORE NO	os Asteaf-207							
Resource Trends							C	11
Operational Resource	es							~
PV4 (learned) 24330 of 24.53K		(98%) <sup>10</sup>	V4 Hest Routes 288 of 49,15K	25%	IPV6 (barned) 6144 of 24.55K	25%) PMS Host Routes 3072 of 12.19K	25%	
MAC (loamed) 6144 of 24.58%		25% M	iniciant Rounes 48 of 8.198	(25%)				
Configuration Resou	rces							Ŷ
Hardware Resource	i							~
Anomalies								
Severity	Detection Time	Last Seen Time	Resource Type	Resource Name	Nodes	Description	Cleared	
😁 Critical	Jul 14 2020 09:11:07.579 AM	Aug 31 2020 05:43:44.224 PM	operational	(PV4 (learned)	scale/eaf-207	Number of IPV4 (learned) entries is above critical threshold (Ourrent Usage : 24330, Critical-Threshold : 22118 [90%])	false	
A Critical	Jul 14 2020	Aug 31 2020	Tarchesen	LPM	scate/eaf-207	Number of LPM entries is above critical threshold (Current Usage : 92%,	fator	

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

	omalies					
Filters Category +	= Resources ×					/ 0
Anomalies By:	Type +					^
		(	12 Total	Fisos (0)     Rajources (12)     Environmental (0)     Statistics (0)     Endpoint (0)     Application (0)	Top 5 modes contributing to Anomaly Score       Node     Anomaly Score       scalarad-202     C Prival       scalarad-202     C Prival       scalarad-202     C Prisal       scalarad-203     C Prisal       scalarad-203     C Prisal       scalarad-203     C Prisal	
12 Total Anoma	alies	Last Seen Time	Desource Tune	Notes	Description	Cleared
12 Total Anoma Severity Oritical	Jlies Detection Time Jul 14 2020 09:11:07:579 AM	Last Seen Time Aug 31 2020 05:43:44.224 PM	Resource Type	Nodes scaleleaf-205	Description Number of BDs is above critical threshold (Current Usage : 3465, Critical-Threshold : 3150 (99%))	Cleared
12 Total Anoma Severity Oritical Oritical	Biles	Last Seen Time Aug 31 2020 05:43:44.224 PM Aug 31 2020 05:43:44.224 PM	Resource Type config operational	Nodes scaleleaf-205 scaleleaf-202	Description Namber of 80s is above critical threshold (Current Usage : 3466, Critical-Threshold : 3150 (99%)) Namber of 804 (searced) entries is above critical threshold (Current Usage : 24230, Critical-Threshold : 22118 (90%))	Cleared false
12 Total Anoma severity Critical Critical Critical	Detection Time           Juli 14 2020           09:11:07.579 AM           Juli 14 2020           09:11:07.579 AM           Juli 14 2020           09:11:07.579 AM	Last Seen Time Aug 31 2020 05:43:44.224 PM Aug 31 2020 05:43:44.224 PM Aug 31 2020 05:43:44.224 PM	Resource Type config operational operational	Nodes scaleleaf-205 scaleleaf-202 scaleleaf-206	Description Number of BDs is above critical threshold (Current Usage : 3465, Critical-Threshold : 3150 (90%)) Number of IPV4 (eerred) entries is above critical threshold (Current Usage : 24330, Critical-Threshold : 22118 (90%)) Number of IPV4 (eerred) entries is above critical threshold (Current Usage : 24330, Critical-Threshold : 22118 (90%))	Cleaned false false
12 Total Anoma Sevenity Critical Critical Critical Critical Critical	Juies           Detection Time           Jail 14 2020           99:11:07.579 AM           Jail 14 2020           69:11:07.579 AM           Jail 14 2020           09:11:07.579 AM           Jail 14 2020           09:11:07.579 AM           Jail 14 2020           09:11:07.579 AM	Last Seen Time Aug 31 2020 05:43:44.224 PM Aug 31 2020 05:43:44.224 PM Aug 31 2020 05:43:44.224 PM Aug 31 2020 05:43:44.224 PM	Resource Type config operational operational operational	Nodes scateleaf-205 scateleaf-202 scateleaf-206 scateleaf-206	Description           Number of BOs is above critical threshold (Current Usage : 3465, Critical-Threshold : 3150 (99%))           Number of BO4 (served) entries is above critical threshold (Current Usage : 24330, Critical-Threshold : 22118 (99%))           Number of BPV4 (served) entries is above critical threshold (Current Usage : 24330, Critical-Threshold : 22118 (99%))           Number of BPV4 (served) entries is above critical threshold (Current Usage : 24330, Critical-Threshold : 22118 (99%))           Number of BPV4 (served) entries is above critical threshold (Current Usage : 24330, Critical-Threshold : 22118 (99%))	Cleaned false false false
12 Total Anoma Severity Critical Critical Critical Critical Critical Critical	Detection Time           Jul 14 2020           09:11:07.079 AM           Jul 14 2020           09:11:07.579 AM           Jul 14 2020           09:11:07.579 AM           Jul 14 2020           09:11:07.579 AM	Last Seen Time Aug 31 2020 05:43:44.224 PM Aug 31 2020 05:43:44.224 PM Aug 31 2020 05:43:44.224 PM Aug 31 2020 05:43:44.224 PM	Resource Type config operational operational operational	Nodes scateleaf-205 scateleaf-202 scateleaf-206 scateleaf-206 scateleaf-205	Description           Number of RDs is above critical threshold (Current Usage : 3466, Critical-Threshold : 3150 (90%))           Number of RDs is above critical threshold (Current Usage : 24330, Critical-Threshold : 22118, [90%])           Number of RD4 (earned) entries is above critical threshold (Current Usage : 24330, Critical-Threshold : 22118, [90%])           Number of RD4 (earned) entries is above critical threshold (Current Usage : 24330, Critical-Threshold : 22118, [90%])           Number of RD4 (earned) entries is above critical threshold (Current Usage : 12165, Critical-Threshold : 1059 (90%))           Number of RD4 (earned) entries is above critical threshold (Current Usage : 12165, Critical-Threshold : 1059 (90%))           Number of RD4 (earned) entries is above critical threshold (Current Usage : 12165, Critical-Threshold : 12118, [90%])	Cleared false false false false false false
12 Total Anoma Severity Critical Critical Critical Critical Critical Critical Critical Critical	Julies           Detection Time           Jail 14 2020           06:11:07.579 AAI	Last Seen Time Aug 31 2020 054.34.4.224 PM Aug 31 2020 054.34.4.224 PM Aug 31 2020 054.34.4.224 PM Aug 31 2020 054.34.4.224 PM Aug 31 2020 054.34.4.224 PM	Resource Type config operational operational operational operational	Nodes scaleboaf-205 soulebeaf-202 scalebeaf-206 scalebeaf-206 scalebeaf-206	Description           Number of BDs is above critical threshold (Current Usage : 3465, Critical-Threshold : 3150 (90%))           Number of BV4 (cerned) entries is above critical threshold (Current Usage : 24330, Critical-Threshold : 22118, [90%))           Number of BV4 (eerned) entries is above critical threshold (Current Usage : 24330, Critical-Threshold : 22118, [90%))           Number of BV4 (eerned) entries is above critical threshold (Current Usage : 24330, Critical-Threshold : 22118, [90%))           Number of BV4 (eerned) entries is above critical threshold (Current Usage : 24330, Critical-Threshold : 22118, [90%))           Number of BV4 (eerned) entries is above critical threshold (Current Usage : 24330, Critical-Threshold : 22118, [90%))           Number of BV4 (eerned) entries is above critical threshold (Current Usage : 24330, Critical-Threshold : 22118, [90%))	Cleaned I false false false false false false
12 Total Anoma Severity Critical Critical Critical Critical Critical Critical Critical Critical	Jiles           Detection Time           Jail 14 2020           05:11:07.579 AM           Jail 14 2020           05:11:07.579 AM           Jail 14 2020           06:11:07.579 AM	Last Seen Time Aug 31 2020 054.314.42.224 PM Aug 31 2020 054.314.224 PM Aug 31 2020 054.314.4224 PM Aug 31 2020 054.314.4224 PM Aug 31 2020 054.314.4224 PM Aug 31 2020 054.314.4224 PM Aug 31 2020	Resource Type config operational operational operational operational operational	Nedes scateleaf-202 scateleaf-202 scateleaf-202 scateleaf-206 scateleaf-206 scateleaf-205 scateleaf-205	Description           Number of BDs is above critical threshold (Current Usage : 3465, Critical-Threshold : 3150 (99%))           Number of BD4 (served) entries is above critical threshold (Current Usage : 24330, Critical-Threshold : 22118, [96%])           Number of BP4 (served) entries is above critical threshold (Current Usage : 24330, Critical-Threshold : 22118, [96%])           Number of BP4 (served) entries is above critical threshold (Current Usage : 24330, Critical-Threshold : 22118, [96%])           Number of BP4 (served) entries is above critical threshold (Current Usage : 24330, Critical-Threshold : 22118, [96%])           Number of BP4 (served) entries is above critical threshold (Current Usage : 24330, Critical-Threshold : 22118, [96%])           Number of BP4 (served) entries is above critical threshold (Current Usage : 24330, Critical-Threshold : 22118, [96%])	Cleaned Isloc Isloc Isloc Isloc Isloc Isloc Isloc

When it comes to policy TCAM analysis for an ACI network site, Nexus Dashboard Insights not only monitors it but also gives the network team the ability to analyse the per-contract/per-filter usage at a site or switch level. This allows the network team to easily understand which contracts are the ones using the most TCAM (globally or at a switch level) as well as understanding how much a contract is used by real

traffic. This allows the network team to remove un-used contracts or optimize the high TCAM consumption contracts.

nalyze Site EF	T-Lab ~ on Sep	10th 2021, 4:32 F	PM ~				
Overview							
Nodes By Policy CAM U	tilization		Nodes By	Policy CAM Anomalies			
<ul> <li>0% - 60% (4)</li> <li>75% - 90% (0)</li> </ul>	• 60% - • >90%	75% (0) (0)	Total • Healt • Major • Warni	y (4) (0) ng (4)	<ul><li>Critical (0)</li><li>Minor (0)</li></ul>		Tota
Associated Policies							
Selecting any combination	on of objects or policies will up	date the tables below					
Provider Tenant	Consumer Tenant	(EPG) Provider EPG	EPG Consumer EPG	C Contract	Filter	😣 Node	
lilian-ni	lilian-ni	systemdefault	systemdefault	systemdefault	systemdefault	Leaf30	01
138 of 479 Entries	138 of 479 Entries	104 of 479 Entries	104 of 479 Entries	104 of 479 Entries	104 of 479 Entries	166 of 6	5.5 K Entries
dpita	dpita	common-services	payroll-app-tier-e	P-E-common-serv	implicit	Leaf40	)2
134 of 479 Entries	110 of 479 Entries	-Subhets 60 of 479 Entries	80 of 479 Entries	60 of 479 Entries	88 of 479 Entries	162 of 6	5.5 K Entries
systemdefault	systemdefault	navroll-app-tier-e	vrf1/anv	doita-inband-file	default	Leaf30	)2
104 of 479 Entries	104 of 479 Entries	pg	48 of 479 Entries	36 of 479 Entries	44 of 479 Entries	81 of 65	5 K Entries
		48 of 479 Entries					
View All (8)	View All (8)	View All (39)	View All (25)	View All (26)	View All (34)	View All	(4)
Policy CAM Statist	ics						
All Policy CAM Rules	by Hit Count by EPGs, Leafs,	Contracts, Filters					~
Filter by attributes							
Filter	Consumer VR	F Action	1 Month	1 Week 1 I	Day 1 Hour	Cumulativ e	Policy Cam Count
default	inb	PERMIT	1730526	1730526 62	6507 18058	142035954	2
dpita-icmp	vrf1	PERMIT	33376	33376 33	376 4616	4816530	1
	vrf1	PERMIT	34864	34864 34	864 4614	44328	2
dpita-icmp							
dpita-icmp implicit	vrf2	PERMIT	116786	116786 59	919 3470	461419	1

#### **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. Hence, monitoring environmental anomalies becomes very reactive and cumbersome. Cisco Nexus Dashboard 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 whether 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 data 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.

Top Nodes by	: CPU	-						~
100.0	CPU							
75- 86 50- 125-	Memory Temperature Fan Utilization Power Supply	-1-1-				s sadetar 2010 s sadetar 2010 - 002 s sadeta 2010 - 002 s sadetar 2010 - 003 s sadetar 2010 s sadetar 201	Notes by CPU           old         CPU           side/2-201         WE           side/2-205         375           side/2-201         376           side/2-201         376           side/2-201         376           side/2-201         376           side/2-201         376           side/2-209         385           side/2-209         385           side/2-201         395           side/2-202         395           side/2-208         395	
0+ 08-31 4:45:	53.000 PM	08-31 5:00:53.000 PM	08-31 5	15/53,000 PM 08-31 5:20 Time	53.000 PM 08-31 545-53.0	000 PM		
08-31 4:45: Anomaly Score	53.000 PM Node	08-31 5:00:53,000 PM	08-31.5	1553.000 PM 06-31 5:10 Time Memory	53.000 PM 08-31 5-45-53.0 Temperature	Fan Utilization	Power Supply	Storage
06-31 4453 Anomaly Score	Node scalelesf-205	08-31 5:00:53,000 PM	08-31 5 ~** 37%	15:53.000 PM 06-31 5:30 Time Memory 1.95 of 6:05 08	55.000 PM 08-31 54553.0 Temperature	Fan Utilization	Power Supply	Storage 
06-31 6453 Anomaly Score Critical	Node scaleleaf-205 scaleleaf-202	08-33 5.00/52,000 PM	08-31 5 27% 37%	115(52,000 PM 01-31 52d Time 01-31 52d Memory 2 1.95 of 6.05 30 1.95 of 6.05 30	55.000 PM 06-31 54553.0 Temperature 2390 260	Fan Utilization	Power Supply 58 of 90 W	Storage 0.01 of 4.77 GB
08-31 4455 Anomaly Score Critical Critical	Node scalelesf-205 scalelesf-202 scalelesf-201	08-31 SOCISS.000 PM	08-31 5 	1552.200 PM 04-31 536 Time 1.95 of 6.05 GB 1.95 of 6.05 GB 1.95 of 6.05 GB	53.000 PM 08-31 54553.0 Temperature 26C 26C 26C	Fan Utilization	Power Supply 59 of 30 w 62 of 30 w 88 of 30 w	Storage 0.01 of 4.77 G 4.776 of 4.77 G
e+ e	S3.000 PM Node scalelesf-205 scalelesf-202 scalelesf-201 scalelesf-201	04-31 5 5053 000 PM	08-31 5 37% 36% 96%	1552.000 PM 06-31 5.30 Time 99 06-31 5.30 1.45 of 6.05 08 1.45 of 6.05 08 1.45 of 6.05 08 1.45 of 6.05 08	53.000 PM 06-31 54553.0 Temperature 260 260 240 240	Fan Utilization SITX 60% 61%	Power Supply 58 of 50 W 62 of 50 W 88 of 50 W 60 of 50 W	Biorage 0.01 of 4.77 GB 4.776 of 4.77 GB 0.01 of 4.77 GB 0.01 of 4.77 GB

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

ironmental Deta	iils - scaleleaf-20	5				Aug 31st 202	10, 4:45 PM - Aug 31st 2020, 5:45 PM	telemetry 🕺	
General Informatio	л								
ANOMALY SCORE	NODE scaleleof-205								
Resource Trends									~ <u>I</u>
CPU 37%		37%	en Utilization 8%-	58%	Memory 1.95 of 6.05 GB	32%)	Power Supply 59 cl 90 W		65%
Storage 0,01 of 4.77 08		18	omperature 90	(97%)					
Anomalies									
Severity	Detection Time	Last Seen Time	Resource Type	Resource Name	Nodes	Description		Cleared	
🚱 Critical	Jul 14 2020 09:21:08:389 AM	Aug 31 2020 05:43:44.224 PN	environmental	Temperature	scale/cof-205	[Outlet Sensor] : Temperature is above Ontical-Threshold : 36.0 C [90%])	e critical threshold (Correct Value : 39 C,	taise	

#### **Statistics**

Statistics is all about interfaces and routing protocols. Cisco Nexus Dashboard 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 the user to quickly identify interfaces to investigate errors.

	Sep 1s	at 2020, 5:38 PM	- Sep 1st	2020, 6:38 PM	Site (	telemetry	$\sim$					000
Top No:	des by Inter	rface Utilization										~
	80			-				-			<ul> <li>scaleleaf-210</li> <li>scaleleaf-205</li> <li>scaleleaf-203</li> </ul>	
Usage	60- 40-	Sep 01 2020 05 scaleleaf-20	5:40:00.00 )9 73.783:	0 PM 33333333333 %	]						<ul> <li>scaleleaf-207</li> <li>scaleleaf-208</li> <li>scaleleaf-204</li> <li>scaleleaf-202</li> <li>scaleleaf-201</li> <li>scalespine-601</li> </ul>	
	20-										💩 scaleleaf-209	
09-0	1 5:38:08.000	PM	09-01 5	:53:08.000 PM		09-01 6:08:08.000 I Time	РМ	09-01 6:23:08.0	00 PM	09-01 6:38	08.000 PM	
p Nod	les by In	terface										
p Nod ≥ <sub>Major</sub>	les by In scaleleaf-	terface 202			S Major :	caleleaf-203			S Major s	scaleleaf-201		
p Nod ≥ Major	les by In scaleleaf- Receive (	terface 202 Gbps) Transmi	t (Gbps)	Errors	S Major : Interface	scaleleaf-203 Receive (Gbps)	Transmit (Gbps)	Errors	S Major s	scaleleaf-201 Receive (Gbps)	Transmit (Gbps)	Errors
p Nod Major Interface eth1/4	des by In scaleleaf- Receive (	terface 202 Gbps) Transmi	it (Gbps)	Errors 70.73 K 🛹	<ul> <li>Major</li> <li>Interface</li> <li>eth1/6</li> </ul>	scaleleaf-203 Receive (Gbps)	Transmit (Gibps)	Errors _ 68 ↔	<ul> <li>Major s</li> <li>Interface</li> <li>eth1/1</li> </ul>	Receive (Gbps)	Transmit (Gbps)	Errors 70.72 K 📌
p Nod Major Interface eth1/4 eth1/2	des by In scaleleaf- Receive ( 59% of 10 59% of 10	terface 202 Gbps) Transmi	it (Gbps) c	Errors 70.73 K 🔊 212.06 K 🔊	S Major : Interface • eth1/6 • eth1/15	scaleleaf-203 Receive (Gbps) 97% of 10	Transmit (Gbps) 74% of 10 78% of 10	Errors _ 68 ↔ _ 80 ↔	Major s Interface • eth1/1 • eth1/50	Receive (Gbps)	Transmit (Gbps)	Errors 70.72 K ≁ 65 →
p Nod Major Interface eth1/4 eth1/2 eth1/12	des by In scaleleaf- Receive ( sax of 10 sax of 10 7	terface 202 Gbps) Transmi 766 of 1 126 of 1 126 of 1 126 of 1	it (Gbps)	Errors 70.73 K ↔ 212.06 K ↔ 67 ↔	<ul> <li>Major</li> <li>Interface</li> <li>eth1/6</li> <li>eth1/15</li> <li>eth1/1</li> </ul>	scaleleaf-203 Receive (Gbps) 97% of 10 78% of 10	Transmit (Gbps) 74% of 10 76% of 10	Errors 68 -> 80 -> 73 ->	C Major s Interface eth1/1 eth1/50 eth1/27	scaleleaf-201 Receive (Gbps) 71% of 10 76% of 10 77% of 10	Transmit (Gbps) 75% of 10 76% of 10 76% of 10	Errors 70.72 K → 65 → 76 →
p Nod Major Interface eth1/4 eth1/2 eth1/13	des by In scaleleaf- Receive ( 55% of to 55% of to 55% of to	terface 202 Gbps) Transmi 200 at 1 200 at 1 200 at 1 200 at 1 200 at 1 200 at 1 200 at 1	it (Gbps)	Errors 70.73 K 🔊 212.06 K 🔊 67 🛶	<ul> <li>Major</li> <li>Interface</li> <li>eth1/6</li> <li>eth1/15</li> <li>eth1/1</li> <li>vpc-41</li> </ul>	scaleleaf-203 Receive (Gbps) 87% of 10 78% of 10 78% of 10	Transmit (Gbps) 74% of 16 76% of 10 76% of 10	Errors - 68 -> - 80 -> - 73 -> - 70 ->	<ul> <li>Major s</li> <li>Interface</li> <li>eth1/1</li> <li>eth1/50</li> <li>eth1/27</li> <li>eth1/28</li> </ul>	Acceletesf-201 Receive (Gbps) 71% of 10 74% of 10 75% of 10	Transmit (Gbps)	Errors . 70.72 K 🔊 . 65 . 76 . 74

Browse view helps deep dive into Interface and Protocol Statistics.

Interface statistics provide a view into the trend of utilization, errors such as CRC, FCS, Stomped CRC.



Protocol Statistics provide a view into what interfaces protocols such as CDP, LLDP, LACP, BGP, PIM, IGMP, IGMP snoop are active, 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 -

Neighbors						
Neighbor	VRF	Operational State	Address Family	Connection Attempts	Prefixes Sent	Accepted Paths
12.6.204.129	blue	<ul> <li>Established</li> </ul>	lpv4, ipv6	15	16	16
12.6.204.130	blue	e Established	ipv4, ipv6	15	15	12
12.6.204.131	blue	Established	ipv4, ipv6	15	8	10
12,6.204.132	blue	<ul> <li>Established</li> </ul>	lpv4, lpv6	15	13	13
12.6.204.133	blue	• Established	lpv4, lpv6	15	12	8
12.6.204.134	blue	· Established	ipv4, ipv6	15	11	9
12.6.204.135	blue	• Established	ipu4, ipu6	15	10	9
12.6.204.136	blue	• Established	iped, ipeli	15	11	13
12.6.204.137	blue	· Established	ipv4, ipv8	15	13	13
12.6.204.138	blue	Established	ipud, ipu6	15	12	12

Example of PIM Interfaces and groups -

fulficast PIM Inter	faces										
Fitters											1
Interface	Admin State	Oper Status		WRF	Tenant	IP Address	Designated Route Address	Designated Router Priority	Neighbor Address	Errors	
vizn404	Enabled	Up		yefow201	71	2.1.150.150	2.1.150.150	0	66.1.128.23/32	62.~~	
vian403	Enabled	Up		yełow/201	<b>R</b> 1	21,150,149	2.1.150.149	0	66.1.128.18/32	41	
vian402	Enabled	Up		yellow/201	61	2 1,150,140	2.1.150.145	0	66.1.126.13/32	59+	
vian401	Enabled	Up		yellow201	6	2.1.150.147	2,1.150.147	.0	66.1.126.8/32	58.~~	
vian400	Enabled	Up		yellow201		2.1.159.146	2.1.150.145	Ð	46.1.128.3/32	44	
vise404	Enabled	Up		witeba201	17	2 1.150.150	2.1.150.150	D	66.1.128.24/32	53	
vian403	Enabled	Up.		white201	11	2.1.150.149	2.1.150.149	D	66.1.128.19/32	62	
vian402	Enabled	Up		white201	u	2.1.150.148	2.1.150.145	0	66.1.126.14/32	51	
vtan401	Enabled	Up		white201	¢1	2.1.150.147	2.1.150.147	0	66.1.128.9/32	82	
	and the second sec										
18 <sup></sup> Roxo	Enabled	05		white201	u	2.1.150.146	2.1.150.146	0	P301 1	07 ↔ 06 :2 [4 ≪ 3-10	0 al 25
10 Pava	ps	Us.		white201	e.	21.190.146	2.1.150.146	0	66.1.128.4/32 Pape 1	67 ↔ at 2 [4 ≪ 1-10	0 of 25
10 × Roxo 10 × Roxo Audicast PIM Grou	P10043	Up		white201		2.1.150.146	2.1.150.146	0	66.1.128.4/32 Pope 1	67 ↔ at 3 14 < 1-to	o of 25 - 1
Nuhicast PIM Grou Ribicast PIM Grou Ribics Source	ps Group Address	Up Tenant	VRF	white201	L1 Ig Interface	2 1.150.146 RPF Neighbor	2.1.150.146 BPF Source	0 Cutgoing Interfaces	66.1,125.4/32 Pige 1	67 ↔ cf 3 [4 < 1-10 State	o of 25 - 1
Nubleast PIM Grou Nubleast PIM Grou Filters Source 180.1.0.7	Ended Foreigned Group Address 226.1.6.7/32	Up Tenant ti	VRF yellow201	white201 Becomin eth1/12	L1 Ig Interface	2.1.150.146 RPF Neighbor H2.1.350.153	2.1.150.146 BPF Source 2.1.150.153	0 Outgoing Interfaces Vien 1001, vien 1001, valn1002	es.1,128.4/32 Pion 1	67 ->> of 3  4 + 1-10 Scate © Active	0.ef 25 - 1
Nin400 10 Yest hubbcast PIM Grou Fibers 5ource 160.1.0.7 160.1.0.2	Endez 99 Group Address 226.1.0.2722 226.0.0.2722	Up Tenant ff	VRF yellow201 yellow201	willb201 Bicomh eth://12 eth://11	u Ig Interface	2.1.150.146 RPF Neighbor H2.1.150.153 82.1.150.148	2.1.150.146 <b>RPF Source</b> 2.1.150.153 2.1.150.148	0 Ovtgolng Interfaces visin1000, visin1001, vash1002, visin1001, vash1002,	es.1,128.4/32	67 ↔ of 3 [4 ≪ 1-10 State ⊙ Active ⊙ Active	o ef 25
Markdo	Entenez	Up Tenant tf tf	VRF yealcos201 yealcos201 yealcos201	wilk201	11 Ig Inderface	2.1.150.116 RPF Nutphor 82.1.150.153 82.1.150.153 82.1.150.158	2.1.150.146 <b>BPF Source</b> 2.1.150.153 2.1.150.153 2.1.150.168	0 Ovtgring Interfaces visit1000, visit1001, visit1002, visit1001, visit1002, visit1001, visit1002, visit1001, visit1002, visit1000, visit1001,	66.1728.432	67 → of 3 14 4 3-10 State ⊙ Active ⊙ Active ⊙ Active	o of 25 - 1
Vando) 10 × Rover Auticast PIM Grou Fibers Source 160, 1.0.7 160, 1.0.7 *	Endez p p Group Address 236.1.6.7/32 236.1.6.7/32 236.1.6.17/32 236.1.6.17/32	Up Terent 11 11	<mark>ЧЯР</mark>	wilk201	zi Ig løterface	2.1.150.146 RPF hulphor R2.1.150.153 82.1.150.158 82.1.150.163 82.1.150.158	2.1.150.146 BPF Source 2.1.150.153 2.1.150.153 2.1.150.153 2.1.150.155	0 Dutgring Interfaces winc1000, winc1001, winc1002, winc1002, winc1002, winc1002, winc1002, winc1002, winc1002, winc1001, winc1002, winc1001, winc1002,	Res	67	a el 25
10 × 80x00 10 × 80x0 Auticesst PM Grow Fibers 100.1.0.7 100.1.0.17 100.1.0.8	Endez p p Group Address 236 1.6.7/32 236 1.6.7/32 236 1.6.17/32 236 1.6.17/32 236 1.6.17/32 236 1.6.17/32	Up Terent II II II	V8F yatkas201 yatkas201 yatkas201 yatkas201 wtite201	wilk2201 keomin ath1/12 eth1/12 eth1/13 eth1/13 eth1/13	zi g ktorface	2.1.190.146 RPF heighbor R2.1.190.148 R2.1.190.148 R2.1.190.148 R2.1.190.148 R2.1.190.158	2.1.150.146 RPF Searce 2.1.150.153 2.1.150.153 2.1.150.155 2.1.150.155 2.1.150.155	0 Dutgoing Interfaces whom 1000, whom 1001, whom 1000, whom 1001, whom 1000, whom 1001, whom 1000, whom 1000, whom 1000, w	Ref. 128.432	67	/

Statistical data is also used for correlation in Cisco Nexus Dashboard Insights. For instance, if there is a CRC error, Cisco Nexus Dashboard 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).

alyze - Anomaly - eth1/1			telemetry 📕 … — >
Analyze	Analysis Time Range: 20 minutes *	Affec	ted Entities > 30.70.240 2 > access > app_epg2 > app_bd-2 > 9d as 32:e0.db:7e
Lifespan		26.20 tenant	3.218.27 20 > access > app_epg20 > app_bd-20 > 2f.bf:54:65:64:94
• •		141.1 tecant	183.238.157 21 > access > app_epg21 > app_bd-21 > 29:7e:32:ef:f0:6a
09 AM 09:15 09:30 09:45	) AM 10:15 10:30 10:45 11 AM	11:15 11:30 12.15 tenant	5.80.69 22 > access > app_epg22 > app_bd-22 > 54:14:de:65:b2:5
Estimated Impact		32.17 tenant	7.123.172 23 > access > app_epg23 > app_bd-23 > ed:4f:a6:a1:c7-1
25 IP(s) will be affected. View Report Ildp protocol(s) on this interface will be affected		183.7 tenant	7.103.132 24 > access > app_mpg24 > app_bd-24 > 81:14:b1:d5:64:
Recommendations		Conte	ext Path: Tenant tenant3 > Application Profile ss > EPG app_epg3 > BD app_bd-3 > MAC
1. Please inspect SFPs		6b:cb box:- tenent	x9bx00:86:c2 13:100:100 3 > access > app_epg3 > app_bd-3 > 6b:cb:9b:00:8x:c2
Mutual Occurences		▼ ::: ) 117.1 tenant	159.159.135 4 > access > app_epg4 > app_bd-4 > 94:28:68:b9:60:a5
Anomalies (4080) 🔗 🔗 🚱 🧐 🔗 🔗	9 09	99.10 tenant	53.64.34 5 > access > app_epg5 > app_bd-5 > 05:41:3d:df:04:16
Faults (4)	• •	• (2.13	76 101 120
1203/0228		43.17	0,101/120

#### **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 imperative as we deal with business critical applications in the data center. The tools for network operations today often have very limited insights on data plane counters, flows, latency, and drops. Even if we can get the data plane flow data from the network switches, how can the data from the inviditual switches be pieced together to form an end-to-end view of a flow while it is traversing the network? How can the end-to-end network latency of a flow be extracted from the flow data ? It used to be the network team that had to do all of these complex flow analysis tasks with limited helping tools, which means a lot of man hours. With Cisco Nexus Dashboard Insights, using Flow Telemetry, the service consumes flow records and respective counters, correlates this data over time to provide end to end flow path and latency. Cisco Nexus Dashboard 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 an 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 help 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 the user to drill into top flows that have 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.



Record Deta	ills from 172.2	5.229.31	to 172.25.:	229.32					Sep 1st 20	020, 6:25 PM - Sep 1st :	2020, 6:40 PM te
ow Record Info	ormation										
ANOMALY SCORE	RECORD TIME		FLOW TYPE	PROTOCOL	PACKET DROP INDICATOR	LATENCY (pa)	FLOW MOVE INDICA	TOR			
C Healthy	Sep 01 2020, 06	27:37.535 PM	IPv4	TOP	0	4	0				
~											
			Source					D	estination		
NODE	ADDRESS	PORT	EPG	TENANT	VIUF	NODE	ADDRESS	PORT	tPG	TENANT	490
scaleleaf-203	172.25.229.31	8080	EPG2	AppDynamics	ctx1	scaleleat-205	172.25.229.32	8050	EPG4	AppDynamics	ctx1
PACKETS	RYTES	BURST MAX Byte	s)			PACKETS	<b>EVITES</b>	BURST MAX (Bytes)			
372617	372617000	1984				372617	372617000	0			
areasted Flor	w Information										
Jgregateu nov	COUNT OF FLOW R	121825	START TIME		END TIME	FLOW TYPE	PROTOCOL	PACKET DROP INDIG	ATOR	LATENCY (pi)	FLOW MOVE INDICA
VAORATA RCORE.						10.0	100	1.4			
C Healthy	6		Sep 01 2020, 05:56	5:17.557 PM	Sep 01 2020. 05:38:38.766 PM	8.84	TOP	0			0
C Healthy	6		Sep 01 2020, 05:54	6:17.557 PM	Sep 01 2020, 00:38:38,766 PM	1914	TOP	D	estination	1	0
C Healthy	6 ADDRESS	PORT	Sep 01 2020, 05:5/ Source EP0	5:17.557 PM	Sep 01 2020, 05:38:30.766 PM	NODE	ADDRESS	D PORT	estination EPG	TENANT	0 VRF
NODE Scalebalf-203	6 ADDRESS 172-25-229.31	PORT 8080	Sep 01 2020, 05:50 Source EPG EPG2	5:17.557 PM TENUNT AppDynamics	Sep 01 2020, 05:38:38,766 PM	NODE scaleleaf-205	ADDRESS 172.25.229.32	0 D PORT 8080	estination BPG EPG4	TENANT	0 VBF ctx1
NODE scaleleaf-203 PACKETS	6 ADORESS 172.25.229.31 BYTES	PORT 8080 IURST MAX (Bytes)	Sep 01 2020, 05:54 Source EPG EPG2	TENUNT AppDynamics	Sep 01 2020, 06:38:38,766 PM	NODE scalelest-205 packets	ADDRESS 172.25.229.32 DVTES	D PORT BORD BURST MAX (Bytws)	estination BPG EPC4	TENANT AppDynamics	0 VRF cfx1

Miloritalies								
Detection Time	Last Seen Time	Severity	Node	Resource Type	Resource Name	Description		Cleared
Jul 14 2020 08:46:06.337 AM	Sep 01 2020 07:02:07.685 PM	🧐 Major	scale/eaf-202	Bow	drop	Packet drop is detected doe to Buffer Drop.		lalse
							Page 1	of 1 [4 4 1-1 of 1 + +]
Path Summary								
			Buffer Dvop	Healthadica				
Surre			andaland, 900	6.16.10.25				

#### **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.

General Informat	tion										
ANOMALY SCORE	MAC ADDRESS b1:90:4f;48:80:69	IP ADORESS 222.181.45.56	LAST UPDATE TIME Sep 01 2020, 06:3	38:50.935 PM							
		Configuration						Operat	ional		
TENANT	VRF	BD	EPG/LSOUT	ENCAP	NODES	INTERFACE	VM NAME	HYPERVISOR	ROBUE	BEHIND VPC	PEER ATTACHED
tenant-tahoe	app_vrf-tel	app_bd-tel	epg-telemetry	vian-103	scaleleaf-203	eth1/3	8	-	False	False	False
					STATIC	LEARNED					
					False	True					

Endpoint History									
Filters									/0
Anomaly Score	IP Address	Nodes	Interface	Time	Status	Tenant	VRF	Sep 01 2020 05 38:50.935 PM	Changes
S Major	222,181,46.56	acabeteat-203	stb1/3	Sep 01 2020 06:38:50,935 PM	Active	tenant-tahoe	app_vrf-tel	Notes sectored 204 scalefeaf-203 Interface	Nodes, Interface, Cosas
C Major	222,181,46.56	scaleleaf-204	sth1/2	Sep 01 2020 06:38:50.933 PM	Active	tenant-tahoe	app_vrf-tel	sector eth1/3	Nodes, interface, Encap
G Major	222.181.46.55	scaleleaf-203	eth1/3	Sep 01 2020 06:38:50.931 PM	Active	tenant-tahoe	app_vrf-tel	epg-tolemetry ylan-103	Nodes, interface, Encap

Endpoint health and consistency is also monitored by Nexus Dashboard Insights:

- Duplicated endpoint ? Problem solved. The Insights service will detect them quickly and point the user to the switch and port from where the duplication is present.
- Stale endpoints? The Insights service provides built-in automation to remediate this situation with a single click

#### Applications

With Cisco AppDynamics and Cisco Nexus Dashboard Insights integration, users get a single pane of glass for application and network statistics and anomalies. Cisco Nexus Dashboard Insights consumes data streamed from AppDynamics controller and in addition to showing application, tier, node health and metrics, Cisco Nexus Dashboard 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 Dashboard 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 -

AppDynamics	- EComm	-NPM		Feb 20, 2019	), 8:45AM - Feb 2	0, 2019, 10:00AM	<b>—</b> — >
General Information Anomaly Score Account Critical Account	Name Usernam 1 Usernam	e Host e 1 10.24.131.186	Connectivity Status † Up				
Health Information Application Health Busin Critical	* Normal (10) • Vianning (0) • Criticol (1)	h Tier Health 4 *Normal (4) • Varning (0) • Critical (0)	Node Health 10 • Vamin • Critical	(10) (0)			<b>—</b> 11
Throughput 8.7 KB/s	~~~~	TCP Loss 1 per mille	~	PIE 66 events	**	Errors 1 million	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Packets 2 per second		Lateral					

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

ynamics -	EComm-NPM	И			May 17th 2020, 12:33 AM - Ma	y 17th 2020, 6:33 AM telemetry 🖈 📕 –
Normal	ORD-N1_0	Order-Tier 33.	33 210	1	172.25.229.53:8080 - Inv-Tier	
<ul> <li>Normal</li> </ul>	ORD-N1_1	Order-Tier 33.	33 210	1	Q, Search	0 Hermork Connection 172.25.229.53 - 172.25.229.49
10 ~ Ro	ws				172.25.229.53:8080 ////0 proxy → Node 172.25.229.53 172.25.229.49	Browse Network Flows
					172.25.229.53:8080 INV-N1_0 proxy → Node 172.25.229.53 ⊕172.25.229.49	customer1 APPLICATION EComm-NPM
Application Netw	rork Links					SOURCE TYPE proxy
Filters						SOURCE
Source Type	Source	Destination Type	Destination	Thro (KB/:		SOURCE IP
ргоку	172.25.229.53:8080	tier	Inv-Tier	2		172.25.229.53
tier	Ecom-Tier	proxy	172.25.229.53:8080	2		node
tier	Order-Tier	tier	Payment-Tier	2		DESTINATION
tier	Order-Tier	backend	APPDY1-MySQL-D8-5.5.58- 0ubuntu0.14.04,1	2		INV-N1_0 DESTINATION IP 172.25.229.49
						PROTOCOL
						TCP

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

				Page 1 of 1 14 4 0-0 of 0 + +
Path Summary				
Source )		Destination		
172.25.229.53         scaleleaf -201           Port: 8080         eth1/2 eth1/3           EPO: EPO1         eth1/2 eth1/3	scalespine-601 eth1/4 uth1/5	scaleleaf-202 172.25.229.49 eth1/2 eth1/3 Port 8060 EPG: EPG3		
View reverse path				
View reverse path Related Details Average Latency By : Trending	×		Burst By: Trending *	
View reverse path Related Details Average Latency By : Trending 4	×	• 172.25.229.53.6060	Burst By: Trending	Ingress burst max     Egress burst max

This integration is vital to blurring the lines of silos inside the organization enabling operators to see the network from the applications point of view. The operator does not need to know which IP is associated to which application or which application flow through which nodes at any given time. Cisco Nexus Dashboard Insights provides all this information, enriches the data, and correlates it for a holistic unified operational view.

#### **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 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 changes to a stable state and helps 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.

General	limeline									
General	formation									
sevter S Cri	AFFECTED OBJECT cal topology/pod-1/nede-20	1/sys/aggr-[po3]/aggrif	cause Interface-physical-down	FAULT CODE \$532	LIFECYCLE raised	TYPE communications	CREATED Sep 01 2020, 07:15:32.000 AM	NUMBER OF OCCURRENCES 2	ORMINAL SEVERITY Critical	PREMIOUS SEVERITY Cleared
Diagnost	cs									
DESCRIP Port is a	1014 own, reason being noCperMember	s(connected), used by EPC	3 on node 201 of febric telemet	ry with hostname	scaleleaf-201					
Change	iet									
una; apg	0									

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

© 2021 Cisco and/or its affiliates. All rights reserved.

#### **Diagnostics, Impact, Recommendation**

Cisco Nexus Dashboard Insights monitors different sets of data from all nodes in the fabric and baselines the data to identify "normal" behavior. Any deviation from this normal is represented as an anomaly in the service dashboard. This helps the operator spend time on resolving the issue instead of finding where in the network the issue really arose. With the correlation algorithms that Cisco Nexus Dashboard 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 service 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 a myriad 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 Dashboard 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 the bursts. 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 for how to fix this anomaly.

Example of a microburst anomaly -

🔗 Major	Aug 20 2020 12:04:03.089 AM	Aug 20 2020 02:46:07.089 PM	interface	ifav201- leaf4	[eth1/45] Ingress I bandwidth (Curren	eth1/35	×
🕙 Major	Aug 19 2020 11:35:23.000 PM	Aug 20 2020 02:45:47.000 PM	interface	ifav201- spine2	[eth1/1] Packet dro Cumulative drop co	Active AFFECTED OBJECT eth1/35	
Major	Aug 19 2020 11:38:33.000 PM	Aug 20 2020 02:48:57.000 PM	interface	ifav201- spine2	[eth1/35] Packet d errors. Cumulative	NODES ifav201-leaf3	
Major	Aug 19 2020 11:39:30.000 PM	Aug 20 2020 02:49:59.000 PM	interface	ifav201- spine4	[eth1/36] Packet d errors. Cumulative	Defection TIME Aug 20 2020 12:19:08.089 AM	
Minor	Aug 20 2020 01:36:03.089 PM	Aug 20 2020 01:51:05.089 PM	interface	ifav201- leaf3	Microbursts detect queue-8	Aug 20 2020 02:46:12.089 PM	
Minor	Aug 20 2020 12:19:08.089 AM	Aug 20 2020 02:46:12.089 PM	interface	ifav201- leaf3	Microbursts detect queue-8	- CATEGORY	
Minor	Aug 20 2020 12:19:08.089 AM	Aug 20 2020 02:46:12.089 PM	interface	ifav201- leaf4	Microbursts detect queue-8	statistics TYPE interface	
> Warning	Aug 20 2020 02:31:04.089 PM	Aug 20 2020 02:31:04.089 PM	interface	ifav201- spine4	[Rate of Change] E than 10% in the pa	DESCRIPTION Microbursts detected at interface eth1/35 in the following queue(s): queue-8	
						Recommendations 1. The identified unicast flows are the top 100 with large max burst values, which may indicate heavier buffer usage by these flows	

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

time span -

Analuze	Analysis Tim	Affected Entities		×
Lifespan		Q.  Search	Fine Record 50,10.1,136 to 50.8,1.136	Ľ
<b>.</b>		50.10.1.136:32855 -> 50.8.1.136:32855 UDP	VRF ctx1	
Thu 20 01 AM 02	AM 03 AM 04 AM 05 AM 06 AM 07 AM 08 AM 09 AM	50.10.0.120:47619 -> 50.8.0.120:47619 UDP	EPG instP-13out2-13-routed_subint-v4	
		50::a:0:a0:48159 -> 50::8:0:a0:48159 UDP	PACKETS	
Estimated Impact		50.10.1.166:25385 -> 50.8.1.166:25385 UDP	1622	*
Detected 100 unic may experience hi	ast flow(s) that may have contributed to the detected microburst(s), gher latency/delay during burst periods. View Report	50.10.0.238:48737 -> 50.8.0.238:48737 UDP	BYTES 14598000	
		50.10.1.218:15473 -> 50.8.1.218:15473 UDP	BURST MAX (BYTES)	
Recommendation	s	50::a:0:3a:17057 -> 50::8:0:3a:17057 UDP	Destination	~
<ol> <li>The identified ur</li> <li>Consider rebala</li> </ol>	nicast flows are the top 100 with large max burst values, which may ncing application traffic load to reduce bursts and avoid potential bu	50.10.1.167:36922 -> 50.8.1.167:36922 UDP	ADDRESS	
		50::a:0:27:26538 -> 50::8:0:27:26538 UDP	50.8.1.136 POPT	
Mutual Occurrenc	es	50::a:0:15:54020 -> 50::8:0:15:54020 UDP	32855	
Anomalies (1244)	000000000000000000	50.10.1.218:15473 -> 50.8.1.218:15473 UDP	Egress	~
Faults (4)	۲	50::a:0:3a:17057 -> 50::8:0:3a:17057 UDP	NODE ifav201-leaf4	
Events (0)		50.10.1.167:36922 -> 50.8.1.167:36922 UDP	TENANT	
		50::a:0:27:26538 -> 50::8:0:27:26538 UDP	tn1	

Recommendations for 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.

Lifespan				Anomaly Details	
• 📀	AM 03 AM 04 AM 05 AM	02 PM	General Information SEVERITY Minor		
Estimated Impact Detected 100 unic may experience his	sst flow(s) that may have contr gher latency/delay during burs	interface	Active Active AFECTED OBJECT eth1/35		
Recommendation 1. The identified ur 2. Consider rebala	a licast flows are the top 100 wi heing application traffic load to	se flows	INUES Ifav201-feat3 DEFECTION TIME Aug 20 2020 > 12:19:08.089 AM		
Mutual Occurrenc	es		- CATEGODY		
Anomalies (1244)	00000000		0	statistics	
Faults (4)	۲	•		TYPE	
Events (0)				DESCRIPTION	
				Microhumts detected at interface oth1/2E in the	

#### **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 Dashboard 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 Dashboard 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 identified 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 Dashboard 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 Dashboard 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 defects or PSIRTS by getting proactive alerts and taking preventive remediation actions.

Example of an Advisory on Field Notice -

Advisory - Field Notice : FN64210     April 20, 2020, 1:00PI	М - Мау 20, 2020, 1:00РМ 🖈 🔳 🌤 — 🗙
Analyze  Lifespan  19:40 19:45 19:5 20:0 20:2 20:1 20:3 20:2 20:4 20:3 20:4 20:3 20:1 20:0  Description  View Full Cisco's Statement  Cisco has recently identified a defect in the Cisco Application Centric Infrastructure (ACI) that could potentially affect customers who run these Cisco has recently identified a defect in the Cisco Application Centric Infrastructure (ACI) that could potentially affect customers who run these Cisco has recently identified a defect in the Cisco Application Centric Infrastructure Cisco Integrated Management Controller (CAPIC) appliances: Saner - APIC-Ciuster-L2 Server - APIC-Cluster-M2 Server - APIC-M2 Server - APIC-Cluster-M2 Server - APIC-Cluster-M2 Server - APIC-M2 Server - APIC-Cluster-M2 Server - APIC-Server - APIC-M2 Server - APIC-Server - APIC-Cluster-M2 Server - APIC-Cluster-M2 Server - APIC-M2 Server - APIC-Server - APIC-Cluster-M2 Server - APIC-Server - APIC-M2 Server - APIC-Server - APIC-Cluster-M2 Server - APIC-Server - APIC-M2 Server - APIC-Server - APIC-Serv	Advisory Details General Information Severity Major Status Citeared Affected Nodes 2 Category Field Notice Detection Time
Recommendation     View Full Recconnendation     APIC servers with an incorrect CIMC network mode can be reconfigured to Dedicated mode or Shared_Lom mode through the CLI or GUI.     Complete these steps in order to reconfigure the CIMC mode to Dedicated mode:     Make sure that there is a cable connected to the CIMC MGMT port in addition to the Ethernet ports on the motherboard (LOM).     Power up the unit and log in with your usemame and password.     Enter these commands from the CIMP complete T248-CE1844V103 /cimc/network If set mode dedicated	Feb. 10, 2019, 09:15:30 AM Last Seen Time Feb. 10, 2019, 09:15:30 AM Clear Time Feb. 10, 2019, 09:15:30 AM
Connectivity Analysis Troubleshoot, connectivity or configuration issues, etc.	
Bug Scanner           Perform a bug scan evaluation on this node and any affected nodes.	
Log Collector     Get help by contacting tech-support and allowing them to automatically collect your logs.	

Example of firmware upgrade recommended by Cisco Nexus Dashboard Insights -

Trooonininendou i	Firmware					
FW n9000	-5.0(1k)	• FW	n9000-4.2	(4i)	0	
June 10,	2020		May 10, 2020			
Applicable Neda						
Applicable Node	15					
Anomaly Score	Advisories	Node	Model	Туре	Serial	Current Firmware
Critical	🔫 (1)	ifav201-apic1-leaf1	n9000	Leaf	ABCDEFJH20	4.2(9d)
Critical	<del>, (</del> 1)	ifav201-apic1-leaf2	n9000	Leaf	ABCDEFJH21	4.6(2a)
S Critical	🔫 (1)	ifav201-apic1-leaf3	n9000	Leaf	ABCDEFJH22	4.8(3d)

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 Dashboard Insights –

mware Update Analysi	S Cate APC writer	- >
pdate Status	Update Summary	4.3(1m) Release Note Summary >
© Disruptive	Object Type Selected Nodes Target Firmware 5.0(1k)	View Full Release Notes Open Bugs 10
ecommended Update Paths		Caveats
Starting Firmware: 4.3(1m) Current FW 4.2(9d)	FW FW FW FW FW	Procedure 1) Upgrade the Cisco APICs. Unless otherwise stated, we recommend upgrading to the latest letter release in the tars release train. 2) After the Cisco APICs are upgraded successfully, upgrad the switches using 2 or more maintenance groups.
Starting Firmware: 4.6(2a)	Immediata Target	
FW		

#### **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 services, such as Cisco Nexus Dashboard 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 services that are hosted on Cisco Nexus Dashboard.

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

See the following documents for more references:

- <u>Cisco Nexus Dashboard Insights Data Sheet</u>
- <u>Cisco Nexus Dashboard Insights User Guide, Release 6.0(1) for Cisco ACI</u>
- <u>Cisco Nexus Dashboard Insights User Guide, Release 6.0(1) for Cisco DCNM</u>
- Cisco Nexus Dashboard Insights FAQ
- Cisco Nexus Dashboard FAQ

#### Software and Hardware Dependencies with Scale

The Nexus Dashboard Insights service is supported on Cisco ACI and Cisco DCNM. Please refer to <u>Cisco</u> <u>Nexus Dashboard and Services Compatibility Matrix</u> for the latest software compatibility information.

#### Licensing

The Cisco Nexus Dashboard Insights service 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 including Cisco Nexus Dashboard Insights.

Both the above licenses are a subscription-only Smart License. For a more detailed overview on Cisco Licensing, go to <a href="https://www.cisco.com/go/licensingguide">https://www.cisco.com/go/licensingguide</a>

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 the Cisco DCNM based fabric.

Pricing and ordering:

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

#### Conclusion

Cisco Nexus Dashboard Insights provides actionable insights using predictive analytics, network assurance, and AlOps. 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 Dashboard 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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA