IIIIII CISCO The bridge to possible

White paper Cisco public

# Network Insights – Resources for Cisco ACI and Cisco DCNM Based Data Center Fabrics

## Contents

Introduction	3
Background	3
Network Insights - Resources (NIR)	4
Event analytics	4
Resource utilization	6
Environmental	8
Flow analytics	8
Installation dependencies	13
Software dependencies	13
Hardware dependencies	13
NIR features support for Cisco DCNM	14
Scale	14
Licensing	14
Pricing and ordering	14
Caveats	14
Conclusion	15

## Introduction

Troubleshooting, root-cause analysis, and remediation of network issues are common challenges for any infrastructure operation. They require network administrators to have years of experience, a high level of domain expertise, and the ability to correlate complex IT environments to prevent or fix issues while upholding the infrastructure uptime to honor Service-Level Agreements (SLAs) with minimum disruption. The Network Insights – Resources App (NIR) builds a persistent knowledge base, including expertise and a correlation matrix, to automate troubleshooting, root-cause analysis, and remediation while enabling infrastructure owners to comply with SLAs required by businesses.

## Background

Modern data centers are managed through controllers such as Cisco ACI<sup>™</sup> or Cisco DCNM which capture the intents of network and security architects and administrators and delivers an automated, consistent policy framework across the data center. The same intent-based policies can be extended to multiple data center sites, remote branches and offices, and cloud service providers, giving centralized control and keeping the infrastructure running with desired policies, postures, and controls.

**Inbuilt automation:** Administrators are no longer exposed to risk of box-by-box configuration. Architects are no longer exposed to the risks of feature disparity, interoperability, and manual assurance of consistent configurations.

**Scalable architecture:** As the network's scope grows from a single data center to multi-site, remote locations, and the cloud, so does its scale. Sometimes single sites can grow up to scale of a few hundred leafs. With this comes the complexity of collecting and analyzing data on everything that is happening in this infrastructure. A data-center infrastructure can be running anywhere between a few thousand to a few million flows. Considering the scale of the infrastructure, at times there may be few hundred messages or events being logged every second.

**Operations test:** The challenge faced by administrators is to comprehend and correlate all these to a particular problem, such as (for example) slowness in a web application. This includes an implicit expectation that an administrator has the required knowledge and expertise (which usually takes time to build) about most if not everything happening in the infrastructure.

**Audit:** Another challenge that administrators face is furnishing proof or evidence of that, despite an actual problem, there is no deficiency in the network infrastructure, and that the source of the problem lies elsewhere. Administrators may require proof of persistent trends or patterns for audit, compliance, or even capacity planning and infrastructure reassessment.

At a fundamental level, notwithstanding the scale and complexity of an infrastructure that is ever growing, administrators are expected to prevent problems and recover from them faster when they do occur.

Network insights - Resources addresses these challenges.

## Network Insights - Resources (NIR)

NIR is a tool; its GUI is integrated as a plugin into the Cisco ACI APIC controller and Cisco DCNM GUI. NIR attracts administrator's attention to significant matters relevant to the task at hand, such as troubleshooting, monitoring, auditing, planning, etc. NIR broadly consists of the following components:

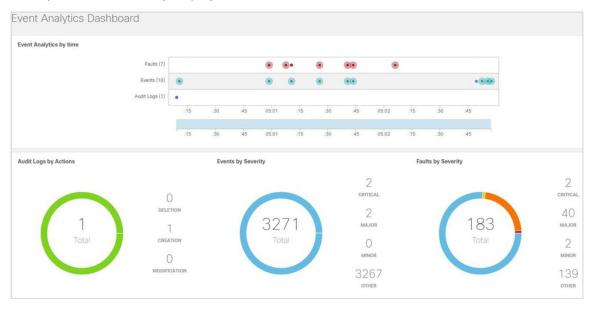
- Event analytics: This is software telemetry that leverages audit logs and events and faults data from the Cisco ACI fabric.
- Resource utilization: This is useful for capacity planning because it offers early detection of resources that are exceeding capacity thresholds.
- Environmental: Identifies anomalies by observing parameters such as CPU, memory, temperature, power draw, fan speed, etc.
- Flow analytics: Helps identify, locate and root-cause data path issues such as latency and packet drop for specific flows.

## **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).
- Remediation: recommends steps for administrators to take against a particular anomaly.

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.



#### Figure 1. Event Analytics Dashboard

- Audit logs: Show 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 administrator 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.

Details -	F1559								
General Tim	eine								
General Inf	ormation								
SEVERITY	AFFECTED OBJECT topology/pod-1/node-102/local/svc-policyelem-id-0/uni/m-vEPC/destgrp- Span_destination/dest-Span_destination	CAUSE configuration- failed	FAULT CODE F1559	LIFECYCLE	TYPE config	CREATED Feb 11 2019 12:02:59pm	NUMBER OF OCCURRENCES 1	oreginal severity Major	PREVIOUS SEVERITY Major
	aber Taaningan, aan aber Taaningi							majar	mala
Diagnostics	8								
DESCRIPTION	1								

#### Figure 2.

Fault Details

The zoom in and out function in the timeline bar helps to quickly contract or expand the timeline under investigation, as shown in the two screenshots below.

Network Insights - Resource	3 🗐 Time Range: 🔹 Feb 26th 2019, 1:04 PM - Feb 26th 2019, 2:04 PM 🗸
Dashboard	Event Analytics Dashboard
<u>ы</u> System	Event / individe Bachboard
Resource Utilization	Event Analytics by time
Environmental	
- Operations	
Flow Analytics	
Event Analytics e	Audit Lops (1) 01/25 01/30 01/35 01/40 01/45 01/50 01/55
	vi.ap 01:39 01:39 01:40 01:49 01:39 01:55
	01:10 01:15 01:20 01:25 01:30 01:35 01:40 01:45 01:50 01:55 02 PM

#### Figure 3.

Nexus Insights Resources - Timeline Bar

Netwo	rk Insights - Res	ources	(E) Time Range: Feb 26th 2019, 1:04 PM - Feb 26th 201	19, 2:04 P	M~)	l										
🚳 Das	hboard		Event Analytics Dashboard													
hi Sys	tem		Event Analytics Dashboard													
Re	source Utilization	0 🛛	Event Analytics by time													
Em	vironmental	0		ults (57)	۲	۲	۲									۲
-∿ Ope	erations						٠			000				-		•
Flo	w Analytics	0		ents (21)	۲	۲			۲		۲	••	۲	۲	0 00	
Eve	ent Analytics	•	Audit	Logs (1)				20100								
					01:33	0	1:34	01:35	01:36	01:37		01:38	01:39	01:	10 0	1:41
					-	01:10	01:15	01:20	01:25	01:30 01:3	5	01:40	01:45 01:50	01	55 02 PN	4

#### Figure 4. Nexus Insights Resources - Timeline Bar

## Resource utilization

Resource utilization shows time-series based trends of capacity utilization. Persistent trends help identify burdened pieces of infrastructure and plan for resizing, restructuring, and repurposing. Spikes help to identify transient issues and draw administrator attention for remediation.

Network Insights - Re	esources	🗐 Time Range: 🔳 Feb 9th	2019, 5:34 PM - Fe	eb 16th 2019, 5:34 PM 🗸					۵ ک
Dashboard		Resource Utilization	Dashboard	ł					
ut System	^		buonibour						
Resource Utilization	•	APIC Capacity							
Environmental	00	Contracts		Endpoint Groups	(1)	Hypervisors		dpoints	(iii)
- Operations	^	12 of 10000	used 1%	17 of 15000	Used 1%	2	29 of	225000	used
Flow Analytics	08								
Event Analytics	09	L4/L7 Devices 7 of 1200	(1%) USED	L4/L7 Graphs 2 of 1000	1% URM	Proxy Database Entries 59 or 450000	(15) Tena Used 7 of 3		15
		VMM Endpoints 12		Virtualization Ratio 58.62		Bridge Domains 26 of 15000		ontexts 3000	used
		Contracts 2840 of 10000	28%	Endpoint Groups 3885 of 15000	28% Used	Hypervisors 200		dpoints 2 of 225000	29%

#### Figure 5.

**Resource Utilization** 

Resource utilization categorizes capacity utilization as follows:

- Operational resources: This 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: This displays the capacity utilization of resources that are dependent on configurations, such as the number of VRFs, bridge domains, VLANs, EPGs, etc.
- Hardware resources: This displays port and bandwidth-capacity utilization.

Operational	Resources	Configuration Resources	Hardware Resources						
Anomaly Score	Node	VRF		D	EPG ^	VLAN		LPM	
۲	Leaf106	_	226 of 800	2949 of 3500	3672 of 3		الجمر 1188 of 3960	_	26%
۲	Leaf107		235 of 800	مر 1031 of 3500	1172 of 3		1166 of 3960	-	27%
۲	Leaf105	_	205 of 800	قبر 1350 or 3500	1086 of 3		1027 of 3960	_	25%
۵	Leaf108	_	212 of 800	مر 1017 of 3500	1058 of 3		الامر 1112 of 3960		29%
۲	Leaf101	*	9 of 800		17 of 3		32 of 3960	•	0%
•	Leaf102		7 of 800	ب محمد 15 of 3500	, 15 of 3		30 of 3960		0%
0	Leaf104	•	7 of 800		11 of 3		22 of 3960		0%
0	Leaf103		7 of 800		11 of 3		22 of 3960		<u>~</u>

#### Figure 6.

Configuration Resources

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 orange; beyond 80 percent, it is color-coded red. This helps attract the administrator's attention to resources requiring attention.

ode Details -	- Leaf106							
Configuration	Resources							
BD 3114 or 3500		(m) EPG 375	8 of 3960	(195%) (199%)			AN 177 of 3960	27% (Ged)
VRF 201 of 800		25%						
Hardware Re Port Bandwidth <b>207</b> of 720 Obp		29% U010 Port 14 c	Usage f 54 ports	26% 2054				
Environmenta	al Resources							
Anomalies	e							
Severity ~	Start Time	End Time	Resource Type	Resource Name	Nodes	Description		
O Critical	Feb 14 2019 10:13:41am	Feb 25 2019 01:19:	4pm config	EPG	Leaf106	Number of EPGs is 3564)	above critical threshold (Usage :	3758, Critical-Threshold :



Node details

• Predicts anomalies based on historical trends and rates of change and forecasts resource shortages; see the screenshot below for an example.

Network Insights - Re	sources												
<ul> <li>Operators</li> <li>Fee Analytics</li> <li>Event Analytics</li> </ul>	<ul><li>● ◎</li><li>● ◎</li></ul>	Anomalies By:	Type 1 Total		0 FLOW ANALYTIC	s	UTELEATION		O		Top 8 nodes contribut Node Lear106 Lear107 Lear107 Lear107 Lear107 Lear101 Lear101 Lear103 Spine2 Lear104	ting is Locaustan Aromaly Score 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	
		1 Total Anomal	ies										
		Start Time		End Time		Severity ^	Resource Type	N	odes	Description			
		Feb 26 2019 01:43	1:32pm	Feb 26 2019 01:43:3	12pm	Warning Warning	operational	L	eaf102	[Forecast Alert] EPI	G usage likely to excee	d maximum supported usage in less	than 24 hours

**Figure 8.** Predict anomalies

## Environmental

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

Anomaly Score	Node $\sim$	CPU		Memory	Temperature		Fan Speed		Fan PWM		Power Supply
•	Leaf101		2%	11.81 of 23.31 GB	-			80%		70%	-
۲	Leaf102		2%	12.19 of 23.31 GB	-			79%		70%	
۲	Leaf103		2%	11.64 of 23.31 GB	-			79%		70%	•
Ø	Leaf104		2%	11.61 of 23.31 GB	*			79%		70%	~
•	Leaf105		25%	<b>5</b> of 23.31 GB	-	27C		25%		28%	140 of 500
8	Leaf106	-	<b>→</b> 27%	← ← 6 of 23.31 GB	-	30C	-	28%	-	25%	136 of 500
۲	Leaf107	-	27%	6 of 23.31 GB		900		93%		92%	134 of 500

#### Figure 9. Environmental

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

CPU 27%		27% used	Fan PWM 92%	(Joed)	Fan Speed 93%		emory of 23.31 GB
Power Supply 134 of 500 W		27% Used	Temperature 90C	(17)			
Anomalies	0						
Anomalies Severity >	Start Time	End Time	Resource Typ	e Resource Name	• Nodes	Description	

#### Figure 10.

Leaf node details

## Flow analytics

To turn on flow analytics, please click on flow collection rules, as shown in the screenshot below.

Network insights - Res	ources					
Network Insights - Re	sources	Time Range: Feb 258	2019, 7:30 AM - Feb 25th 2019, 1:30 PM 🗸			۰ و ک
Dashboard		Dashboard				Application Settings
M System	^	Dubinbourd				Flow Collection Rules
Resource Utilization	00		Total Controllers		Total Nodes	Service Status
Environmental	0		0		4 O Spines	Collection Status
→ Operations	^		0		4 Leaves	Rerun Set Up
Flow Analytics	00	Anomalies by Type		Anomalies by Severity		About Network Insight

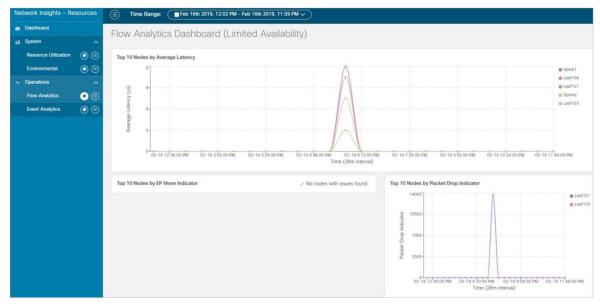
Figure 11. Flow Analytics In the next screen, as shown below, select the VRF to monitor flows.

VRF Based Rules			
Name	Tenant	VRF	
NewTestRule	mgmt	inb	
	VEPC	VRF	

#### Figure 12.

Flow Collection Rules

Flow analytics is designed to identify data-plane anomalies in the network. The flow analytics dashboard attracts administrator 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 administrator 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.



#### Figure 13.

Flow Analytics Dashboard (Limited Availability)

 Packet drop indicator: Shows time-series-based packet drop statistics. Clicking on a particular leaf drills down to detailed flow data, including at which exact point in the fabric the drop occurred, as shown in the two graphics below. This saves precious minutes during troubleshooting and helps administrators focus their attention on specific potential problem-points in the infrastructure.

SOURCE					DESTINATION						
ADDRESS POR	EPG					ADDRESS PORT	EPG				
51.1.1.50 539	EPG1					41.1.1.40 62084	EPG2				
VGRESS					EGRESS						
ODE	VRF	TENANT	PACKETS	BYTES	BURST MAX (Bytes)	NODE	VRF	TENANT	PACKETS	BYTES	BURST MAX (Bytes)
elemetry-hw-leaf	ctx1	tele2	86375	108659692	4800	telemetry-hw-leaf3	ctx1	tele2	86374	108658492	5024
START TIME						END TIME					
lov 01 2018 11:43:54am			Nov 01 2018 01:26:26pm								
ADDRESS TYPE						PROTOCOL					
PV4						UDP					
PACKET DROP INDIC	ATOR					LATENCY (µs)					
						3					
P MOVE INDICATOR											
)											
le More											

#### Figure 14.

Packet drop indicator

		=		
Source	telemetry-hw-leaf2	telemetry-hw-spine1	telemetry-hw-leaf3	Destination
	telemeny-nw-learz	Eth2/14 eth2/2	Eth1/49 eth1/2	Port: 62084

#### Figure 15.

Packet drop indicator

 Latency: Shows time-series-based latency statistics. Clicking on a particular leaf 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 administrators to focus on the root causes of the latency and remediate them. Historical trends help administrators identify persistent problems and re-evaluate the infrastructure capacity.

letwork Insights - Re	esources	Time	Range: Feb 1	7th 2019, 4:32	PM - Feb 17th	2019, 5:32 PM	$\sim$							
Dashboard		Browse	Flows (Lim	ited Ava	ilahility)									
J System	^	DIOWSC	110113 (EIIII	neu Ava	naionity)									
Resource Utilization	0	Filters												
Environmental	0													
- Operations	~	Top 10 flor	ws by: Average Late	incy	*									
Flow Analytics	0 😑		127										····	0 171.1.1.1.6
Event Analytics	0									· · · ·				0 171.1.10.1:
		(stt)	9											171.1.2.1:60 171.1.4.1:60
		Average Latency (µs)												0 171.1.5.1:6
		ge La	6-											171.1.6.1:6
		Wera												<ul> <li>171.1.7.1.6</li> <li>171.1.8.1.6</li> </ul>
		-												0 171.1.9.1:6
			02-17 4:36:00 PM	02-17 4	4:00 PM	02-17 4.52.00 PM	A 02-17	5.00:00 PM Time (2m inte	02-17 5.b8.0 rval) Source	0 PM 02-17 5	16:00 PM 0	2-17 5:24:00 PM	02-17 5:32	00 PM
		Anomaly Score	Origination Timestamp <	Nodes	Ingress Nodes	Egress Nodes	Ingress Tenant	Egress Tenant	EPG	Address	Port	EPG	Address	p
		۲	Feb 17 2019 04:51:23pm	Leaf101	Leaf101		VEPC	VEPC	PGW	171.1.3.1	0	Internet	183.1.3.1	0
		٢	Feb 17 2019 04:51:23pm	Leaf101	Leaf101		VEPC	VEPC	PGW	171.1.7.1	0	Internet	183.1.7.1	0
			o de o recoprir											

#### Figure 16.

Browse Flows (Limited Availability)

As seen in the screenshot below, by clicking on a particular leaf node in the flow analytics screen, we drill down to flows with a latency anomaly observed on a particular leaf. It also shows the exact flows that experienced the increased latency. Double-clicking on the flow shows the flow level details.

Flow Details	
SOURCE	DESTINATION
ADDRESS PORT EPG	ADDRESS PORT EPG
171.1.1.1 60 PGW	174.1.1.1 60 Ext-EPG
INGRESS	EGRESS
NODE VRF TENANT PACKETS BYTES BURST MAX (Bytes)	NODE VRF TENANT PACKETS BYTES BURST MAX (Bytes)
Leaf101 VRF vEPC 137577141 17988208444 17184	Leaf104 VRF vEPC 137577141 17988208444 24576
START TIME	END TIME
Feb 25 2019 05:28:53am	Feb 25 2019 01:30:54pm
ADDRESS TYPE	PROTOCOL
IPV4	TCP
ANOMALY SCORE	PACKET DROP INDIGATOR
61	0
LATENCY (µs)	EP MOVE INDICATOR
12	0
Hide More A	
Path Summary	
February 25 2019, 7:31 AM	
171.1.1.1 Leaf101 Spine1 Leaf104 174.1.1.1	
171.1.1         Lear101         Spine1         Lear104         1/4.1.1           Port: 60         eth/1/0 eth/1/49         eth/11 unknown         unknown eth/1/0         Port: 60	
PGW Ext-EPG	

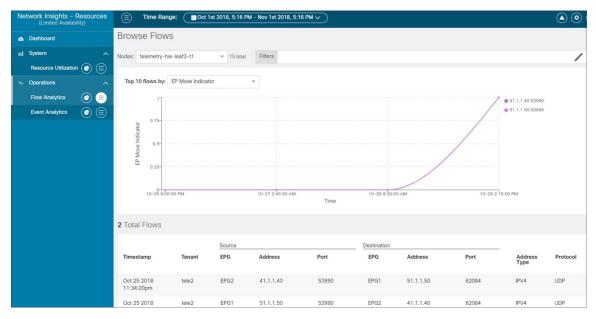


Details of the flow, such as burstiness, help identify and remediate bandwidth issues or apply appropriate Quality of Service (QoS) levels.





• EP move indicator: Shows time-series-based endpoint movement in the fabric. 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.





## Installation dependencies

- For ACI based deployment -
  - NIR app can be installed on existing APIC M3/L3 cluster to use resource utilization, environmental, event analytics and Statistics functions.
  - To use flow analytics, NIR app should be installed on Services engine appliance cluster which is targeted to ship Q3 CY19.
- For DCNM based deployment
  - NIR app on existing DCNM cluster to use resource utilization, environmental, and Statistics functions.
  - Flow analytics will be supported CY19. Service engine appliance cluster is not required.
- For the steps to install the NIR App, click here.
- To download the NIR App, click here.

## Software dependencies

The NIR App is supported on Cisco ACI and Cisco DCNM. Please click here to refer release notes for latest software compatibility information.

## Hardware dependencies

Successive generations of hardware and software enhance telemetry capabilities. The table below maps NIR functions to hardware platforms.

#### NIR features support for Cisco ACI

NIR App function	Cisco Nexus <sup>®</sup> 9300/9700 EX series	Cisco Nexus 9300/9700 FX series	Cisco Nexus 9300/9700 FX2 series
Resource Utilization	Yes	Yes	Yes
Environmental	Yes	Yes	Yes
Statistics	Yes	Yes	Yes
Event Analytics	Yes	Yes	Yes
Flow Analytics	Target CY19	Yes	Yes

## NIR features support for Cisco DCNM

NIR App function	Cisco Nexus® 9300//9500 series	Cisco Nexus <sup>®</sup> 9300//9500 EX series	Cisco Nexus 9300/9500 FX series	Cisco Nexus 9300/9500 FX2 series
<b>Resource Utilization</b>	Yes	Yes	Yes	Yes
Environmental	Yes	Yes	Yes	Yes
Statistics	Yes	Yes	Yes	Yes
Flow Analytics	Not supported	Target CY19	Target CY19	Target CY19

## Scale

Scalability of the NIR App:

- Number of leafs supported with NIR installed on APIC M3/L3 cluster (No Flow Telemetry): 100
- Number of leafs supported with NIR installed on DCNM cluster: 250
- Number of leafs supported with NIR installed on Services Engine: 250
- Number of targeted active flows: 10,000

## Licensing

For licensing details, please refer to the Cisco Nexus Insights datasheet.

## Pricing and ordering

For ordering information, please <u>click here</u>.

Alternately, Contact your Cisco Account team to learn future pricing and get additional details.

## Caveats

• NIR App Flow Analytics, NetFlow, and Cisco Tetration<sup>™</sup> cannot be simultaneously enabled. Only one of these features can be enabled at a time.

## Conclusion

Network Insights - Resources (NIR) automates a vast range of information gathering, tracking data about the infrastructure, learning of new events and determining their cause, and highlighting unexpected occurrences in the network while at the same time helping network administrators plan ahead, comply with policies and audits, and keep track of infrastructure capacity and uptime.

Network Insights - Resources attempts to be an extension of the administrator'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