GESTALT IT

SolarWinds Network Automation Manager vs. CA Spectrum and CA Network Flow Analysis

A Complete Solution for Modern Monitoring

A comparative analysis created by Tom Hollingsworth of Gestalt IT with SolarWinds assistance and funding. This report may utilize information, including publicly available data, provided by various companies and sources, including SolarWinds. The opinions are those of the author and do not necessarily represent SolarWinds' position.

April 2018

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report provides a comparison between SolarWinds® Network Automation Manager (NAM) and equivalent products from CA, namely CA® Spectrum® and CA Network Analysis. Analysis was performed with public information from both companies and resources found on the internet to provide pricing and features. The findings of this report include determinations of how each solution monitors systems and provides data about network traffic analysis.

The conclusion of the report is that SolarWinds NAM provides much more value for the implementation cost in addition to being easier to implement from an engineering perspective as described below. The factors that influence the decision-making process should be evaluated carefully to account for all data points before proceeding.

FEATURE TABLE

Pricing shown in U.S. currency and as of April 2018.

FEATURE	SOLARWINDS NAM	CA SPECTRUM
TOTAL COST FOR 1000 NODES	$95,000	$522,295
MODEL-DRIVEN DATABASE		✓
NETWORK MONITORING	✓	✓ (With Network Flow Analysis)
UI INTEGRATION	✓	✓ (With CA Unified Infrastructure Management)
CONFIGURATION MANAGEMENT	✓	
IP ADDRESS MANAGEMENT	✓	
WAN BANDWIDTH MANAGEMENT	✓	
HIGH AVAILABILITY	✓	
EASY SNMP STRING IMPORT	✓	

COMPARATIVE ANALYSIS INTRODUCTION

Network monitoring is a very complicated subject. The days of having a single tool capable of monitoring every aspect of the network is long gone. Instead, the modern network administrator needs a combination of tools dedicated to offering different pieces of the overall picture.

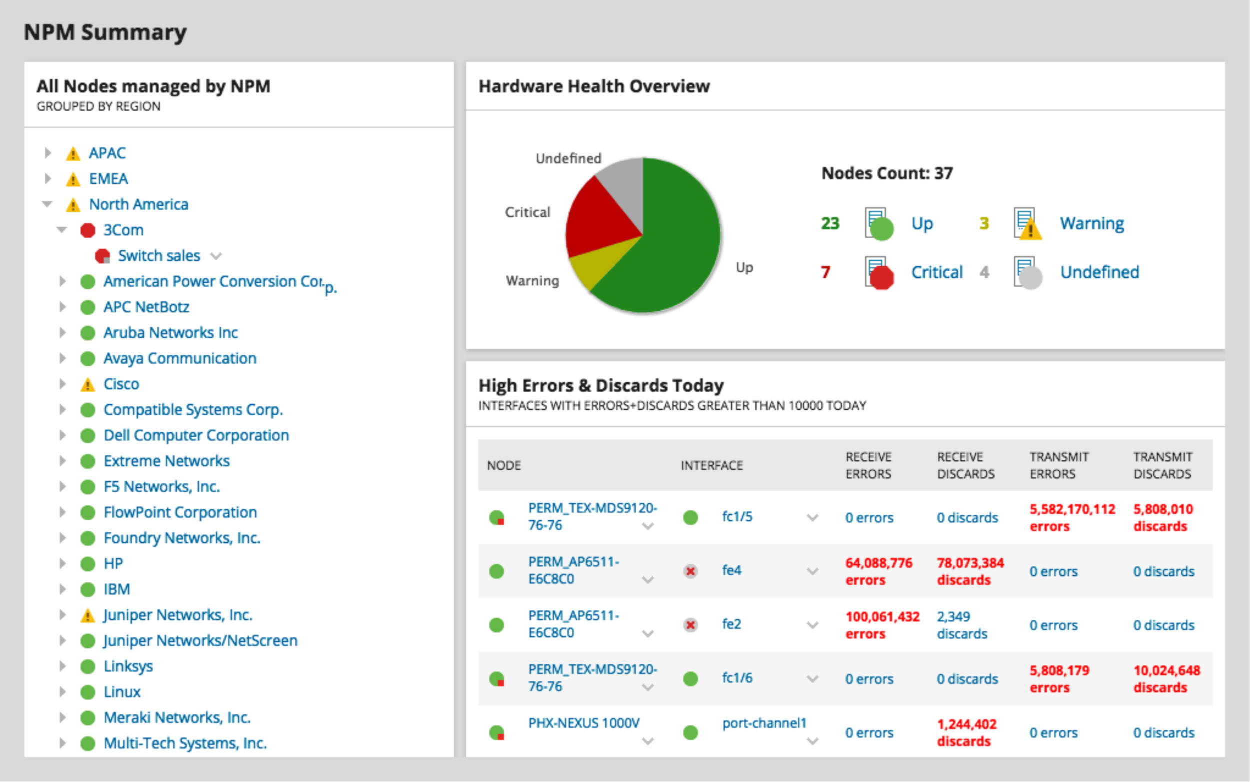
When making a purchasing decision for one of these systems, it is critical to understand how each of the components interact with each other. It is also crucial to determine what is necessary for the minimum viable platform for a given set of needs. The licensing of those pieces can dictate the overall makeup of the platform and how much visibility and monitoring it can provide.

In this report, we will compare CA Technologies Spectrum and Network Flow Analysis with SolarWinds Network Automation Manager (NAM).

SOLARWINDS NAM OVERVIEW

SolarWinds Network Automation Manager (NAM) is an integrated network monitoring solution that encompasses a broad range of capabilities, including network performance monitoring, traffic and bandwidth analysis, configuration and change management, WAN performance monitoring, and IP address management. Each of these capabilities is similar to functions found in CA Spectrum and CA Network Flow Analysis.

NETWORK PERFORMANCE MONITORING



NPM Summary

All Nodes managed by NPM
GROUPED BY REGION

- ⚠ APAC
- ⚠ EMEA
- ⚠ North America
  - ● 3Com
    - ● Switch sales
  - ● American Power Conversion Corp.
  - ● APC NetBotz
  - ● Aruba Networks Inc
  - ● Avaya Communication
  - ⚠ Cisco
  - ● Compatible Systems Corp.
  - ● Dell Computer Corporation
  - ● Extreme Networks
  - ● F5 Networks, Inc.
  - ● FlowPoint Corporation
  - ● Foundry Networks, Inc.
  - ● HP
  - ● IBM
  - ⚠ Juniper Networks, Inc.
  - ● Juniper Networks/NetScreen
  - ● Linksys
  - ● Linux
  - ● Meraki Networks, Inc.
  - ● Multi-Tech Systems, Inc.

Hardware Health Overview

Nodes Count: 37

23	Up	3	Warning
7	Critical	4	Undefined

High Errors & Discards Today
INTERFACES WITH ERRORS+DISCARDS GREATER THAN 10000 TODAY

NODE	INTERFACE	RECEIVE ERRORS	RECEIVE DISCARDS	TRANSMIT ERRORS	TRANSMIT DISCARDS
PERM_TEX-MDS9120-76-76	fc1/5	0 errors	0 discards	5,582,170,112 errors	5,808,010 discards
PERM_AP6511-E6C8C0	fe4	64,088,776 errors	78,073,384 discards	0 errors	0 discards
PERM_AP6511-E6C8C0	fe2	100,061,432 errors	2,349 discards	0 errors	0 discards
PERM_TEX-MDS9120-76-76	fc1/6	0 errors	0 discards	5,808,179 errors	10,024,648 discards
PHX-NEXUS 1000V	port-channel1	0 errors	1,244,402 discards	0 errors	0 discards

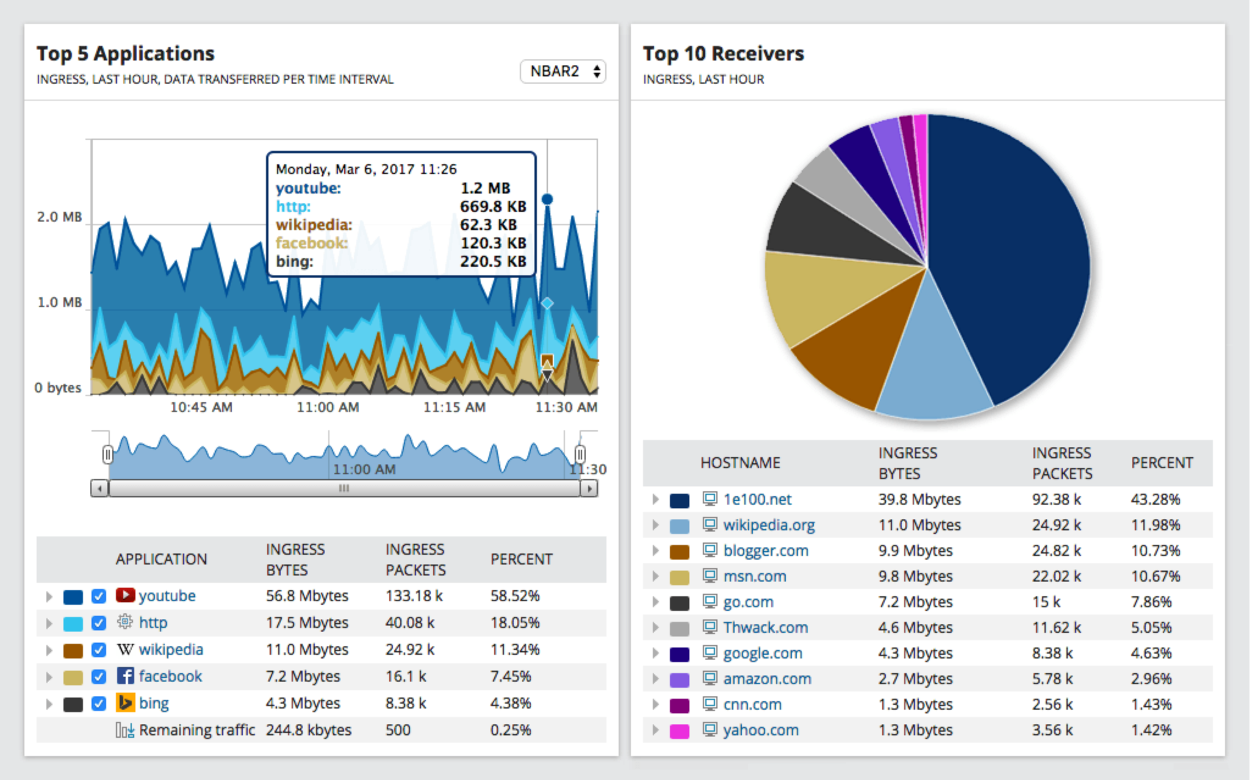
NAM monitors a wide variety of network manufacturer devices through a variety of configuration avenues, such as SNMP.

NAM takes the information gathered from monitored devices and displays it through a customized performance management dashboard. This allows administrators to have a visual method of troubleshooting different devices and data sources and see correlations between events that would not otherwise be apparent in non-visual data.

NAM also has intelligent alerting, which reduces the number of alerts generated from events. This can be configured to suppress alerts when critical links go down, for instance, to prevent response personnel from being overwhelmed by continuous messages about systems that are only affected because of failed dependencies.

One feature included in NAM that is not found in CA Spectrum or CA Network Flow Analysis is the ability to monitor wireless networks. This not only includes basic information about access point availability, but also rogue AP detection and the ability to build coverage heat maps.

TRAFFIC AND BANDWIDTH ANALYSIS



Top 5 Applications

INGRESS, LAST HOUR, DATA TRANSFERRED PER TIME INTERVAL

NBAR2

Monday, Mar 6, 2017 11:26
youtube: 1.2 MB
http: 669.8 KB
wikipedia: 62.3 KB
facebook: 120.3 KB
bing: 220.5 KB

		APPLICATION	INGRESS BYTES	INGRESS PACKETS	PERCENT
■	☑	youtube	56.8 Mbytes	133.18 k	58.52%
■	☑	http	17.5 Mbytes	40.08 k	18.05%
■	☑	wikipedia	11.0 Mbytes	24.92 k	11.34%
■	☑	facebook	7.2 Mbytes	16.1 k	7.45%
■	☑	bing	4.3 Mbytes	8.38 k	4.38%
		Remaining traffic	244.8 kbytes	500	0.25%

Top 10 Receivers

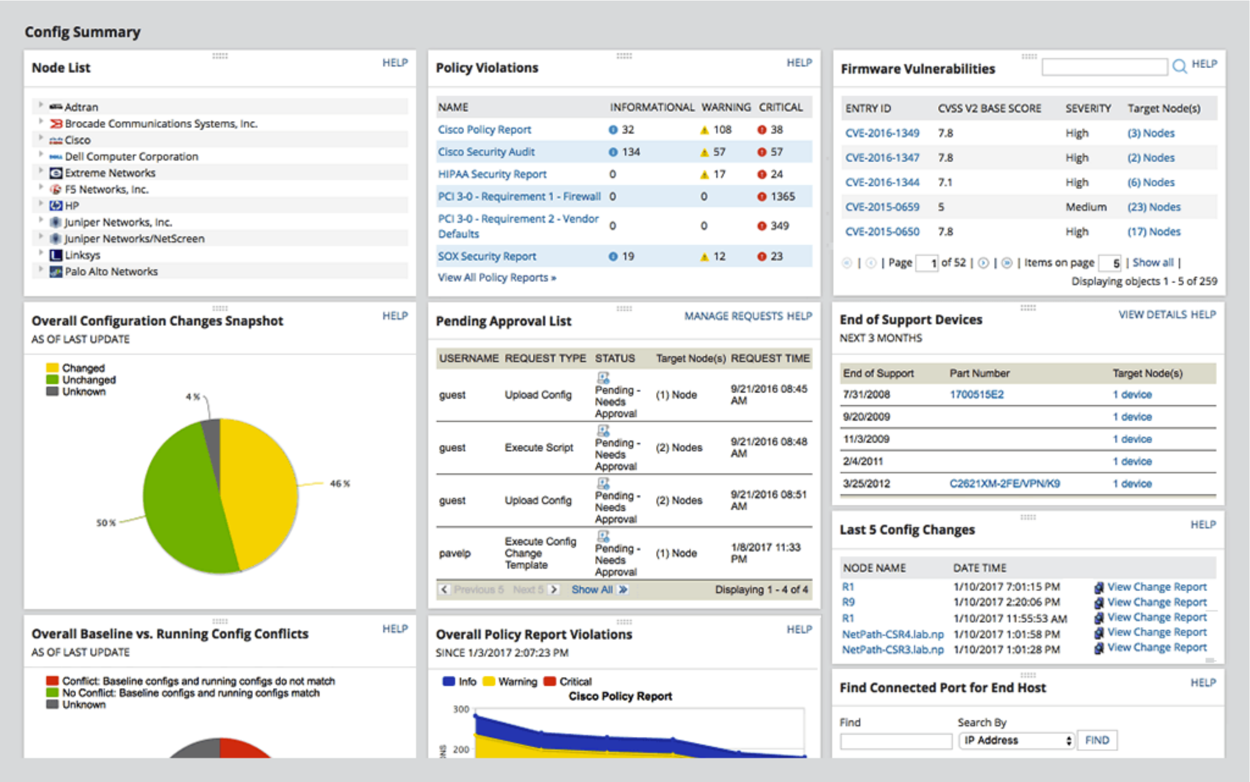
INGRESS, LAST HOUR

	HOSTNAME	INGRESS BYTES	INGRESS PACKETS	PERCENT
■	1e100.net	39.8 Mbytes	92.38 k	43.28%
■	wikipedia.org	11.0 Mbytes	24.92 k	11.98%
■	blogger.com	9.9 Mbytes	24.82 k	10.73%
■	msn.com	9.8 Mbytes	22.02 k	10.67%
■	go.com	7.2 Mbytes	15 k	7.86%
■	Thwack.com	4.6 Mbytes	11.62 k	5.05%
■	google.com	4.3 Mbytes	8.38 k	4.63%
■	amazon.com	2.7 Mbytes	5.78 k	2.96%
■	cnn.com	1.3 Mbytes	2.56 k	1.43%
■	yahoo.com	1.3 Mbytes	3.56 k	1.42%

NAM traffic and bandwidth analysis most easily corresponds to CA Network Flow Analysis. NAM takes data from NetFlow and IPFIX sources as well as protocols from Juniper®, HPE®, and Huawei®, and builds a database of traffic patterns. This database helps you determine which applications and hosts are consuming the most bandwidth on the network.

NAM traffic and bandwidth analysis is displayed on the same dashboard as network performance analysis data, which allows for events to be correlated and traffic patterns to be detected to determine when congestion issues start, helping plan for high traffic times. NAM also includes a component to monitor wireless LAN traffic to help visualize what wireless clients are doing and how they are affecting the bandwidth usage in your network.

NETWORK CONFIGURATION MANAGEMENT



Config Summary

Node List

- Adtran
- Brocade Communications Systems, Inc.
- Cisco
- Dell Computer Corporation
- Extreme Networks
- F5 Networks, Inc.
- HP
- Juniper Networks, Inc.
- Juniper Networks/NetScreen
- Linksys
- Palo Alto Networks

Policy Violations

NAME	INFORMATIONAL	WARNING	CRITICAL
Cisco Policy Report	32	⚠ 108	38
Cisco Security Audit	134	⚠ 57	57
HIPAA Security Report	0	⚠ 17	24
PCI 3-0 - Requirement 1 - Firewall	0	0	1365
PCI 3-0 - Requirement 2 - Vendor Defaults	0	0	349
SOX Security Report	19	⚠ 12	23

View All Policy Reports »

Firmware Vulnerabilities

ENTRY ID	CVSS V2 BASE SCORE	SEVERITY	Target Node(s)
CVE-2016-1349	7.8	High	(3) Nodes
CVE-2016-1347	7.8	High	(2) Nodes
CVE-2016-1344	7.1	High	(6) Nodes
CVE-2015-0659	5	Medium	(23) Nodes
CVE-2015-0650	7.8	High	(17) Nodes

| Page 1 of 52 | | Items on page 5 | Show all |
Displaying objects 1 - 5 of 259

Overall Configuration Changes Snapshot
AS OF LAST UPDATE

Pending Approval List

USERNAME	REQUEST TYPE	STATUS	Target Node(s)	REQUEST TIME
guest	Upload Config	Pending - Needs Approval	(1) Node	9/21/2016 08:45 AM
guest	Execute Script	Pending - Needs Approval	(2) Nodes	9/21/2016 08:48 AM
guest	Upload Config	Pending - Needs Approval	(2) Nodes	9/21/2016 08:51 AM
pavelp	Execute Config Change Template	Pending - Needs Approval	(1) Node	1/8/2017 11:33 PM

Previous 5 Next 5 Show All Displaying 1 - 4 of 4

End of Support Devices
NEXT 3 MONTHS

End of Support	Part Number	Target Node(s)
7/31/2008	1700515E2	1 device
9/20/2009		1 device
11/3/2009		1 device
2/4/2011		1 device
3/25/2012	C2621XM-2FE/VPN/K9	1 device

Last 5 Config Changes

NODE NAME	DATE TIME	
R1	1/10/2017 7:01:15 PM	View Change Report
R9	1/10/2017 2:20:06 PM	View Change Report
R1	1/10/2017 11:55:53 AM	View Change Report
NetPath-CSR4.lab.np	1/10/2017 1:01:58 PM	View Change Report
NetPath-CSR3.lab.np	1/10/2017 1:01:28 PM	View Change Report

Overall Baseline vs. Running Config Conflicts
AS OF LAST UPDATE

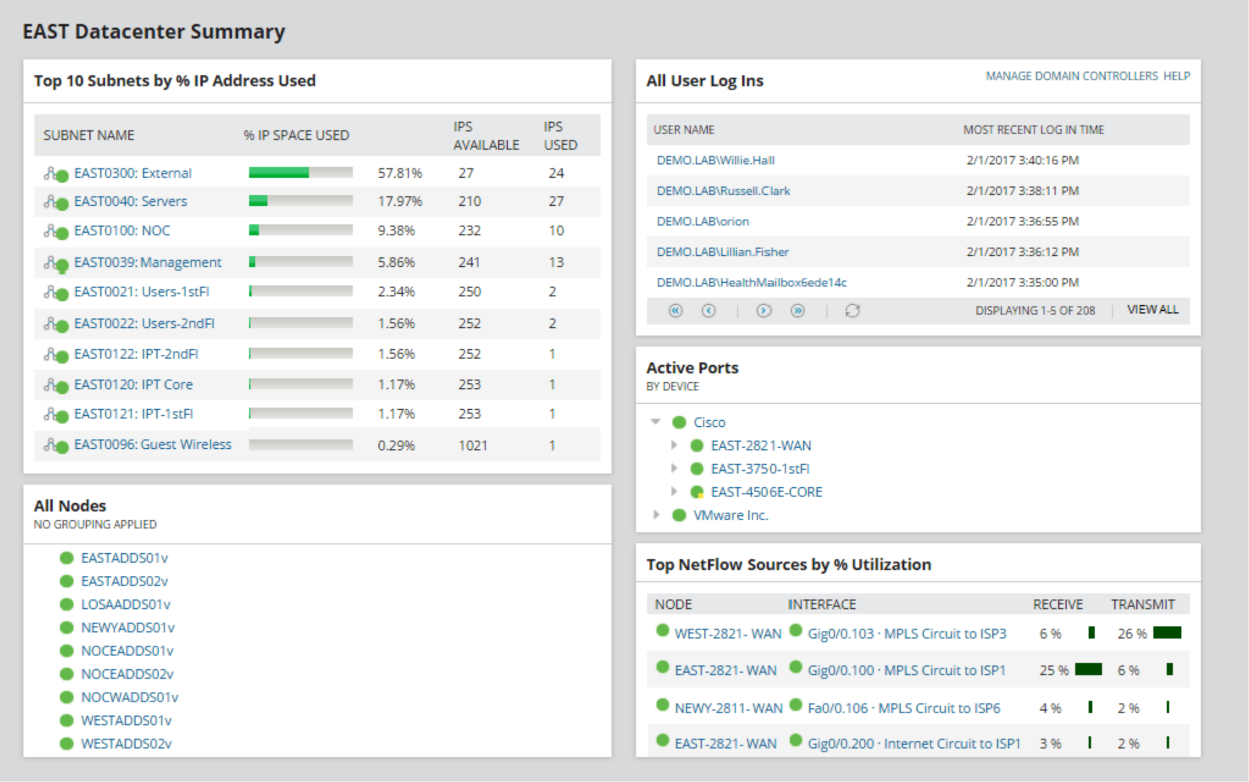
Overall Policy Report Violations
SINCE 1/3/2017 2:07:23 PM

Find Connected Port for End Host

NAM network configuration management helps network administrators to quickly audit the configuration of a device and create a backup as needed. NAM also allows administrators to quickly and concurrently roll out changes to multiple devices across the network.

NAM can also help ensure that these changes are validated against corporate change policies by monitoring devices for unauthorized changes and rolling those changes back if they violate constraints. This compliance testing also includes assessment of potential vulnerabilities against the National Vulnerability Database to help ensure that current and future exploits and security issues can quickly be detected in the environment and corrected by exposure.

IP ADDRESS MANAGEMENT



EAST Datacenter Summary

Top 10 Subnets by % IP Address Used

SUBNET NAME	% IP SPACE USED		IPS AVAILABLE	IPS USED
EAST0300: External		57.81%	27	24
EAST0040: Servers		17.97%	210	27
EAST0100: NOC		9.38%	232	10
EAST0039: Management		5.86%	241	13
EAST0021: Users-1stFl		2.34%	250	2
EAST0022: Users-2ndFl		1.56%	252	2
EAST0122: IPT-2ndFl		1.56%	252	1
EAST0120: IPT Core		1.17%	253	1
EAST0121: IPT-1stFl		1.17%	253	1
EAST0096: Guest Wireless		0.29%	1021	1

All Nodes

NO GROUPING APPLIED

- EASTADDS01v
- EASTADDS02v
- LOSAADDS01v
- NEWYADDS01v
- NOCEADDS01v
- NOCEADDS02v
- NOCWADDS01v
- WESTADDS01v
- WESTADDS02v

All User Log Ins

MANAGE DOMAIN CONTROLLERS HELP

USER NAME	MOST RECENT LOG IN TIME
DEMO.LAB\Willie.Hall	2/1/2017 3:40:16 PM
DEMO.LAB\Russell.Clark	2/1/2017 3:38:11 PM
DEMO.LAB\orion	2/1/2017 3:36:55 PM
DEMO.LAB\Lillian.Fisher	2/1/2017 3:36:12 PM
DEMO.LAB\HealthMailbox6ede14c	2/1/2017 3:35:00 PM

DISPLAYING 1-5 OF 208 | VIEW ALL

Active Ports

BY DEVICE

- Cisco
  - EAST-2821-WAN
  - EAST-3750-1stFl
  - EAST-4506E-CORE
- VMware Inc.

Top NetFlow Sources by % Utilization

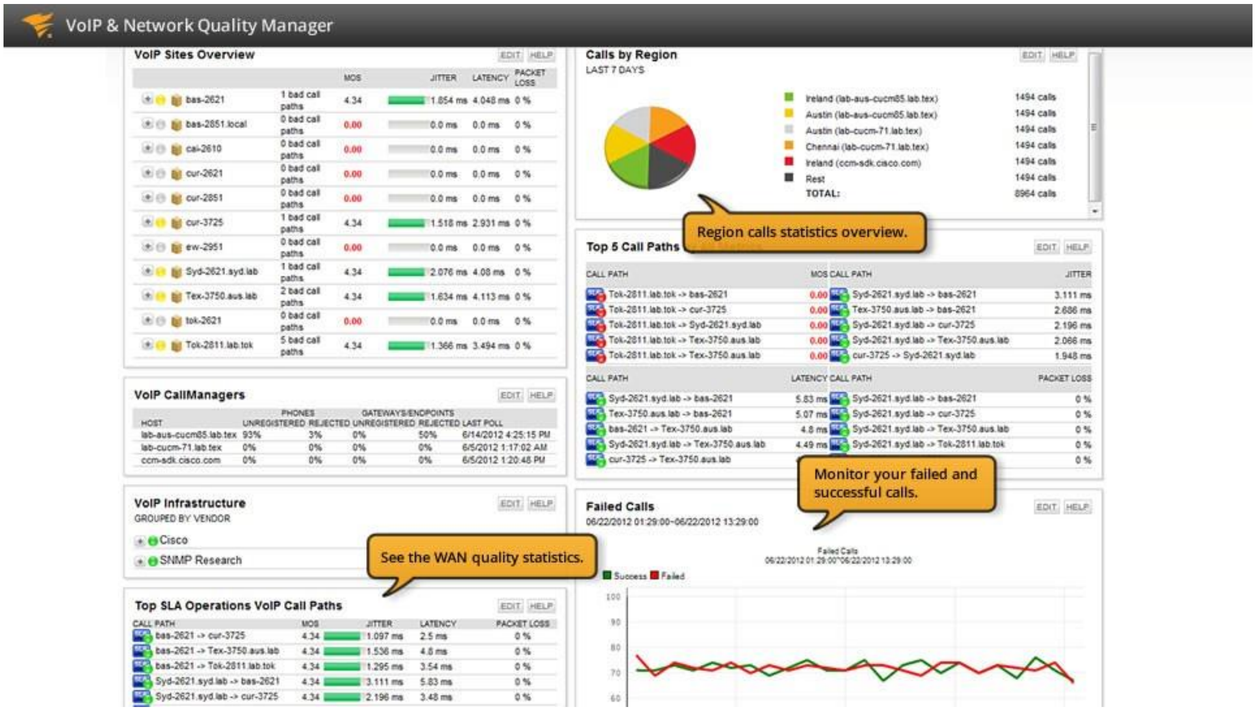
NODE	INTERFACE	RECEIVE	TRANSMIT
WEST-2821- WAN	Gig0/0.103 · MPLS Circuit to ISP3	6 %	26 %
EAST-2821- WAN	Gig0/0.100 · MPLS Circuit to ISP1	25 %	6 %
NEWY-2811- WAN	Fa0/0.106 · MPLS Circuit to ISP6	4 %	2 %
EAST-2821- WAN	Gig0/0.200 · Internet Circuit to ISP1	3 %	2 %

© 2018 SolarWinds Worldwide, LLC. All rights reserved.

NAM IP address management helps network and systems administrators automatically track and maintain information about device address assignments. NAM gives the organization the opportunity to move away from management through static spreadsheets and instead use a dynamic database of addresses that is centrally managed and automatically updated.

NAM has integrated management for DHCP and DNS management, as well as offering the ability to manage third-party DHCP and DNS systems such as those from Microsoft® and Cisco®. The rich reporting capability allows administrators to quickly find unused address space and make assignments for new devices, as well as tracking the history of devices and address assignments.

VOIP & NETWORK QUALITY MANAGER



VoIP Sites Overview

		MOS	JITTER	LATENCY	PACKET LOSS
bas-2621	1 bad call paths	4.34	1.854 ms	4.048 ms	0 %
bas-2851.local	0 bad call paths	0.00	0.0 ms	0.0 ms	0 %
cai-2610	0 bad call paths	0.00	0.0 ms	0.0 ms	0 %
cur-2621	0 bad call paths	0.00	0.0 ms	0.0 ms	0 %
cur-2851	0 bad call paths	0.00	0.0 ms	0.0 ms	0 %
cur-3725	1 bad call paths	4.34	1.518 ms	2.931 ms	0 %
ew-2951	0 bad call paths	0.00	0.0 ms	0.0 ms	0 %
Syd-2621.syd.lab	1 bad call paths	4.34	2.076 ms	4.08 ms	0 %
Tex-3750.aus.lab	2 bad call paths	4.34	1.634 ms	4.113 ms	0 %
tok-2621	0 bad call paths	0.00	0.0 ms	0.0 ms	0 %
Tok-2811.lab.tok	5 bad call paths	4.34	1.366 ms	3.494 ms	0 %

VoIP CallManagers

	PHONES		GATEWAYS/ENDPOINTS		
HOST	UNREGISTERED	REJECTED	UNREGISTERED	REJECTED	LAST POLL
lab-aus-cucm85.lab.tex	93%	3%	0%	50%	6/14/2012 4:25:15 PM
lab-cucm-71.lab.tex	0%	0%	0%	0%	6/5/2012 1:17:02 AM
ccm-sdk.cisco.com	0%	0%	0%	0%	6/5/2012 1:20:48 PM

VoIP Infrastructure

GROUPED BY VENDOR

- Cisco
- SNMP Research

See the WAN quality statistics.

Top SLA Operations VoIP Call Paths

CALL PATH	MOS	JITTER	LATENCY	PACKET LOSS
bas-2621 -> cur-3725	4.34	1.097 ms	2.5 ms	0 %
bas-2621 -> Tex-3750.aus.lab	4.34	1.536 ms	4.8 ms	0 %
bas-2621 -> Tok-2811.lab.tok	4.34	1.295 ms	3.54 ms	0 %
Syd-2621.syd.lab -> bas-2621	4.34	3.111 ms	5.83 ms	0 %
Syd-2621.syd.lab -> cur-3725	4.34	2.196 ms	3.48 ms	0 %

Calls by Region

LAST 7 DAYS

🟩	Ireland (lab-aus-cucm85.lab.tex)	1494 calls
🟨	Austin (lab-aus-cucm85.lab.tex)	1494 calls
⬜	Austin (lab-cucm-71.lab.tex)	1494 calls
🟧	Chennai (lab-cucm-71.lab.tex)	1494 calls
🟥	Ireland (ccm-sdk.cisco.com)	1494 calls
⬛	Rest	1494 calls
	TOTAL:	8964 calls

Region calls statistics overview.

Top 5 Call Paths

CALL PATH	MOS	CALL PATH	JITTER
Tok-2811.lab.tok -> bas-2621	0.00	Syd-2621.syd.lab -> bas-2621	3.111 ms
Tok-2811.lab.tok -> cur-3725	0.00	Tex-3750.aus.lab -> bas-2621	2.686 ms
Tok-2811.lab.tok -> Syd-2621.syd.lab	0.00	Syd-2621.syd.lab -> cur-3725	2.196 ms
Tok-2811.lab.tok -> Tex-3750.aus.lab	0.00	Syd-2621.syd.lab -> Tex-3750.aus.lab	2.066 ms
Tok-2811.lab.tok -> Tex-3750.aus.lab	0.00	cur-3725 -> Syd-2621.syd.lab	1.948 ms

CALL PATH	LATENCY	CALL PATH	PACKET LOSS
Syd-2621.syd.lab -> bas-2621	5.83 ms	Syd-2621.syd.lab -> bas-2621	0 %
Tex-3750.aus.lab -> bas-2621	5.07 ms	Syd-2621.syd.lab -> cur-3725	0 %
bas-2621 -> Tex-3750.aus.lab	4.8 ms	Syd-2621.syd.lab -> Tex-3750.aus.lab	0 %
Syd-2621.syd.lab -> Tex-3750.aus.lab	4.49 ms	Syd-2621.syd.lab -> Tok-2811.lab.tok	0 %
cur-3725 -> Tex-3750.aus.lab			0 %

Monitor your failed and successful calls.

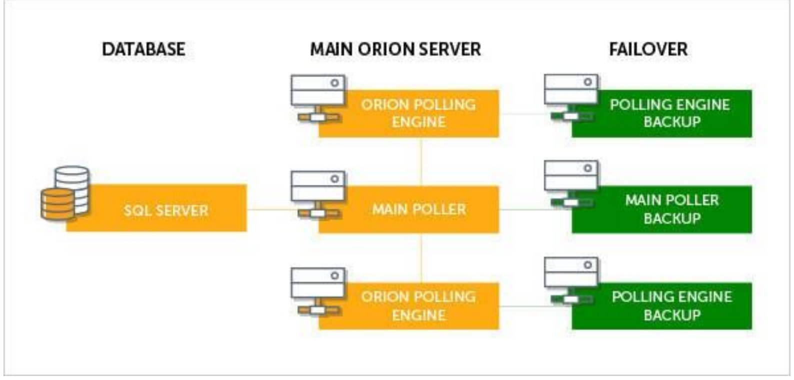
Failed Calls

06/22/2012 01:29:00~06/22/2012 13:29:00

NAM VoIP & Network Quality Manager (VNQM) gives network administrators visibility into a very specific subset of delicate applications. NAM allows for the collection of information about the quality of voice calls on the network. Voice calls have very specific requirements for delay, jitter, and packet loss. NAM integrates with Cisco and Avaya® voice platforms to determine call quality scores based on these criteria and set alerts for calls that have degraded quality.

NAM allows this data to be correlated against Wide Area Network (WAN) performance metrics to determine if call quality is affected by external factors like WAN outages. VNQM can also help test WAN circuit performance by generating synthetic traffic for testing, monitoring for service level performance, and setting alerts for administrators to see when these metrics are suboptimal.

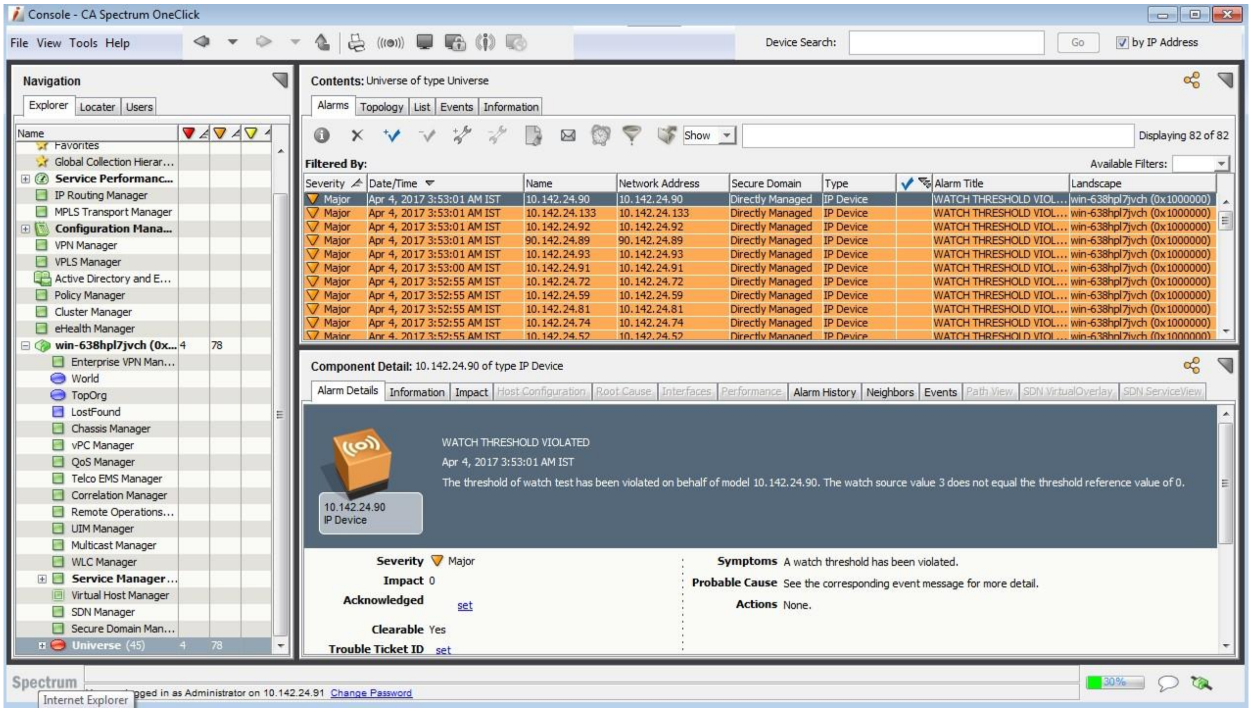
HIGH AVAILABILITY



NAM is based on the reliable SolarWinds Orion® Platform and includes significant High Availability features to help ensure that your networking monitoring system stays up and running in the event of a failure. Polling devices and collection servers can be located across different subnets to help ensure that they are always reachable. The system is also configured so that network monitoring collection gets back on track in typically less than five minutes after a failure.

A public cloud Infrastructure-as-a-Service (IaaS) system can also be configured as a failover point to provide a globally reachable location. NAM allows for automatic failback to a preferred server, so in the event of a failure, you can ensure that your networking monitoring is happening in the location you want as soon as it becomes available again. Customizable failover rules help ensure that everything follows a specific pattern when thresholds are violated or become unavailable, and robust alerting keeps you up-to-date should that occur.

CA SPECTRUM OVERVIEW



Contents: Universe of type Universe

Filtered By:

Severity	Date/Time	Name	Network Address	Secure Domain	Type	✓	Alarm Title	Landscape
Major	Apr 4, 2017 3:53:01 AM IST	10.142.24.90	10.142.24.90	Directly Managed	IP Device		WATCH THRESHOLD VIOL...	win-638hpl7jvch (0x1000000)
Major	Apr 4, 2017 3:53:01 AM IST	10.142.24.133	10.142.24.133	Directly Managed	IP Device		WATCH THRESHOLD VIOL...	win-638hpl7jvch (0x1000000)
Major	Apr 4, 2017 3:53:01 AM IST	10.142.24.92	10.142.24.92	Directly Managed	IP Device		WATCH THRESHOLD VIOL...	win-638hpl7jvch (0x1000000)
Major	Apr 4, 2017 3:53:01 AM IST	90.142.24.89	90.142.24.89	Directly Managed	IP Device		WATCH THRESHOLD VIOL...	win-638hpl7jvch (0x1000000)
Major	Apr 4, 2017 3:53:01 AM IST	10.142.24.93	10.142.24.93	Directly Managed	IP Device		WATCH THRESHOLD VIOL...	win-638hpl7jvch (0x1000000)
Major	Apr 4, 2017 3:53:00 AM IST	10.142.24.91	10.142.24.91	Directly Managed	IP Device		WATCH THRESHOLD VIOL...	win-638hpl7jvch (0x1000000)
Major	Apr 4, 2017 3:52:55 AM IST	10.142.24.72	10.142.24.72	Directly Managed	IP Device		WATCH THRESHOLD VIOL...	win-638hpl7jvch (0x1000000)
Major	Apr 4, 2017 3:52:55 AM IST	10.142.24.59	10.142.24.59	Directly Managed	IP Device		WATCH THRESHOLD VIOL...	win-638hpl7jvch (0x1000000)
Major	Apr 4, 2017 3:52:55 AM IST	10.142.24.81	10.142.24.81	Directly Managed	IP Device		WATCH THRESHOLD VIOL...	win-638hpl7jvch (0x1000000)
Major	Apr 4, 2017 3:52:55 AM IST	10.142.24.74	10.142.24.74	Directly Managed	IP Device		WATCH THRESHOLD VIOL...	win-638hpl7jvch (0x1000000)
Major	Apr 4, 2017 3:52:55 AM IST	10.142.24.52	10.142.24.52	Directly Managed	IP Device		WATCH THRESHOLD VIOL...	win-638hpl7jvch (0x1000000)

Component Detail: 10.142.24.90 of type IP Device

10.142.24.90
IP Device

WATCH THRESHOLD VIOLATED
Apr 4, 2017 3:53:01 AM IST
The threshold of watch test has been violated on behalf of model 10.142.24.90. The watch source value 3 does not equal the threshold reference value of 0.

Severity Major
Impact 0
Acknowledged set
Clearable Yes
Trouble Ticket ID set

Symptoms A watch threshold has been violated.
Probable Cause See the corresponding event message for more detail.
Actions None.

...gged in as Administrator on 10.142.24.91 Change Password

© 2018 CA Technologies. All rights reserved.

CA Spectrum is an enterprise event and network fault management solution. It is a combination of technologies acquired by CA from Concord Communications in 2005 and 3tera in 2010. CA Spectrum can monitor several types of objects, including devices, hosts, applications, and connections.

CA Spectrum manages these objects through a client/server management model. The central repository for this information is SpectroSERVER. This server is an amalgamation of a database server, a device manager, and a modeling engine.

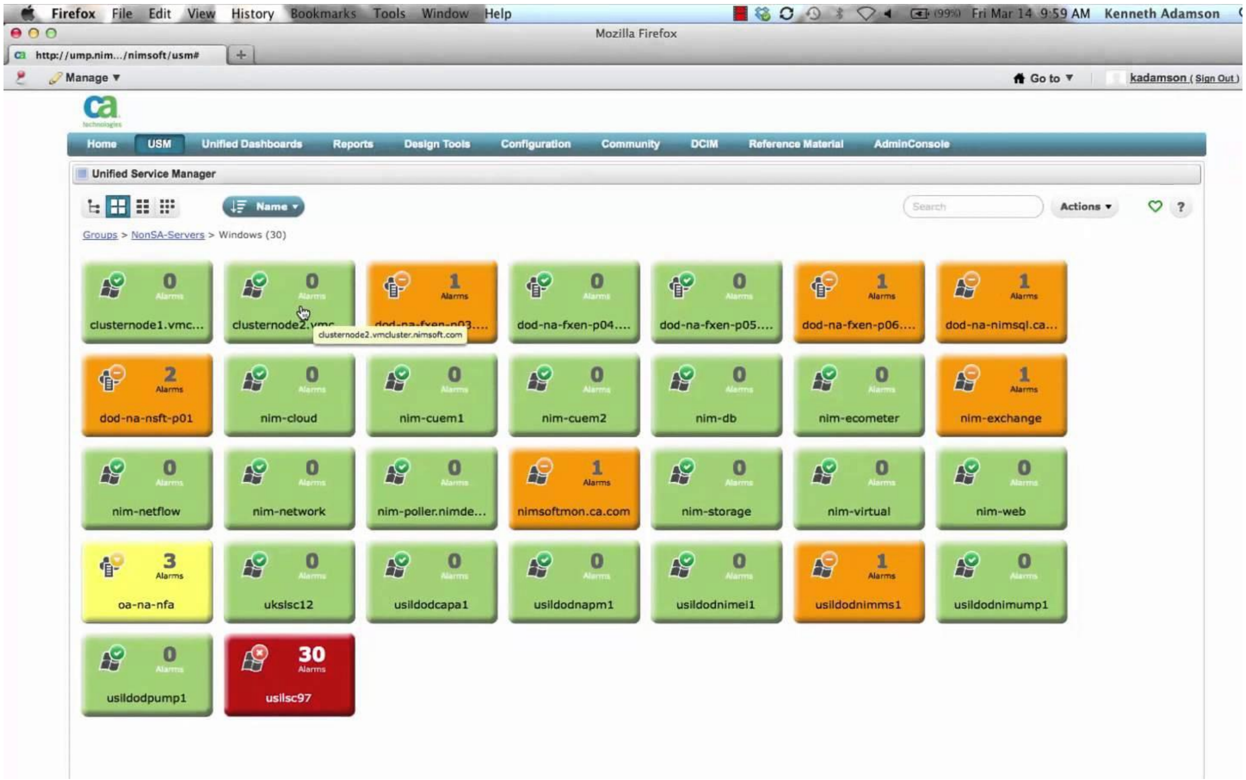
The device manager is a collection of models used to build a topology of the systems that are being monitored. These models can reflect physical devices, such as routers or switches. They can also represent things like network subnets, VPN connections, or quality of service (QoS) policies. These models can be predefined base model types or can be created based on the needs of the users.

The modeling engine builds a picture of the monitored system and networks by taking elements from the modeling catalog and building them into representations of devices. Interface handlers program these models with the characteristics of the devices, such as interfaces and connectivity information. Once all the objects have been built, the final model that is created represents all monitored objects in the system.

CA Spectrum supports automatic discovery of network and systems elements when populating the model database. This automatic discovery has two parts. The first part defines a subnet or group of subnets to search for devices. The discovery process finds these devices and interrogates their capabilities based on SNMP information that you import from a predefined text file.

Once the discovery process has found all the devices, they are imported into the SpectroSERVER for modeling. The modeling process takes the data from the discovery and builds in the configuration of each device as well as the connections to other devices in the system. Once the process is completed, the discovered devices are imported into the main model.

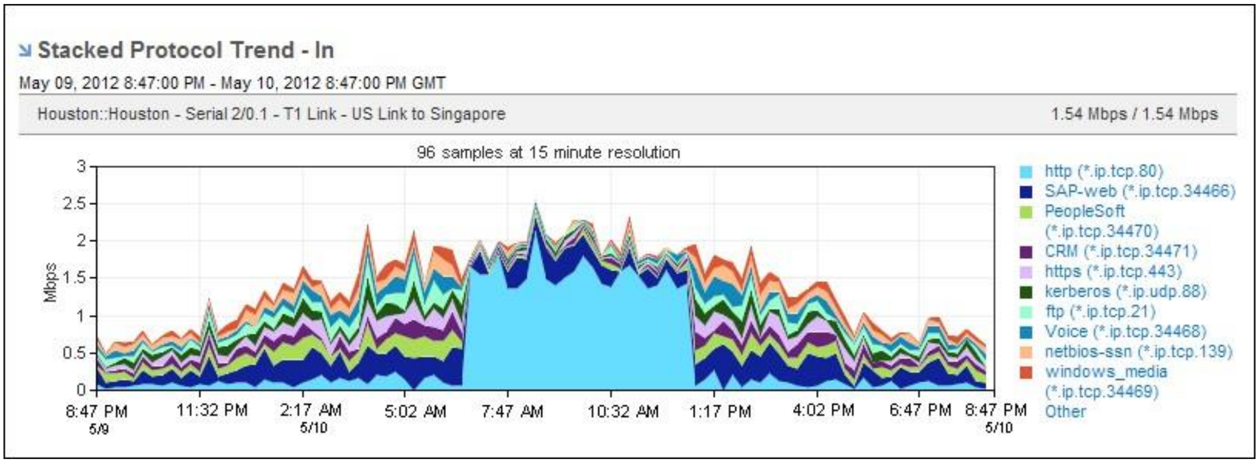
CA SPECTRUM INTEGRATION WITH OTHER CA PLATFORMS


Firefox File Edit View History Bookmarks Tools Window Help
Fri Mar 14 9:59 AM Kenneth Adamson
Mozilla Firefox
http://ump.nim.../nimsoft/usm#
Manage
Go to
kadamson (Sign Out)
Home USM Unified Dashboards Reports Design Tools Configuration Community DCIM Reference Material AdminConsole
Unified Service Manager
Name
Search
Actions
Groups > NonSA-Servers > Windows (30)
0 Alarms clusternode1.vmc...
0 Alarms clusternode2.vmc...
clusternode2.vmcluster.nimsoft.com
1 Alarms dod-na-fxen-p03....
0 Alarms dod-na-fxen-p04....
0 Alarms dod-na-fxen-p05....
1 Alarms dod-na-fxen-p06....
1 Alarms dod-na-nimsql.ca...
2 Alarms dod-na-nsft-p01
0 Alarms nim-cloud
0 Alarms nim-cuem1
0 Alarms nim-cuem2
0 Alarms nim-db
0 Alarms nim-ecometer
1 Alarms nim-exchange
0 Alarms nim-netflow
0 Alarms nim-network
0 Alarms nim-poller.nimde...
1 Alarms nimsoftmon.ca.com
0 Alarms nim-storage
0 Alarms nim-virtual
0 Alarms nim-web
3 Alarms oa-na-nfa
0 Alarms ukslsc12
0 Alarms usildodcapa1
0 Alarms usildodnapm1
0 Alarms usildodnimei1
1 Alarms usildodnimms1
0 Alarms usildodnimump1
0 Alarms usildodpump1
30 Alarms usilsc97

© 2018 CA Technologies. All rights reserved.

CA Spectrum offers additional integration with CA Unified Infrastructure Management (UIM). This solution allows for a unified console to manage alerts from both CA Spectrum and CA UIM. A variety of integration solutions allow alarms to be synchronized between both systems, including SNMP gateways and the Southbound Gateway. There has been a recent change to the integration functionality and now only the Spectrum Gateway is supported. CA UIM is required to integrate CA Spectrum with other CA enterprise infrastructure management tools and requires additional licensing at additional cost.

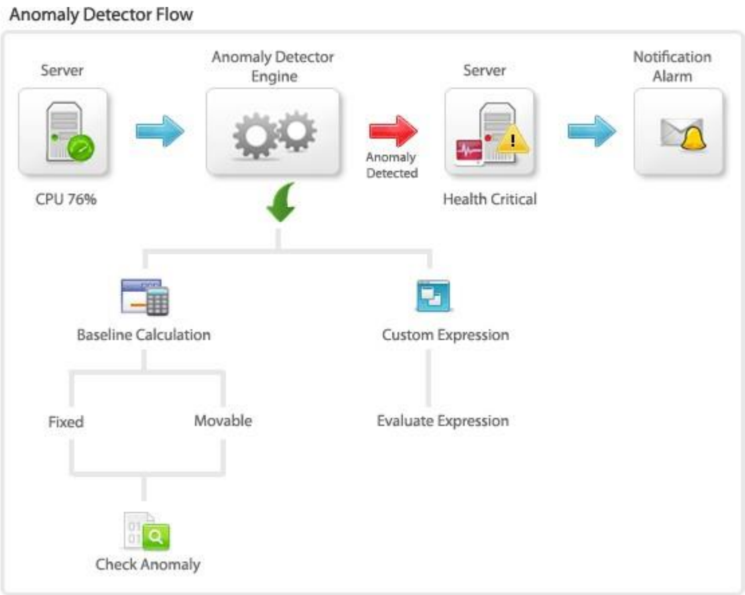
CA NETWORK FLOW ANALYSIS INTRODUCTION



CA Network Flow Analysis is an enterprise traffic monitoring solution designed to give network administrators the ability to monitor traffic based on a variety of criteria. It can also analyze NetFlow and IPFIX information, provide instant information about interfaces with high utilization, and monitor application bandwidth usage across a variety of links, including WAN connections.

CA Network Flow Analysis also retains the collected traffic data, allowing the system to establish baseline trending for interfaces that enables administrators to set thresholds for monitoring. Network Flow Analysis can also analyze trends in applications and hosts to help optimize network settings for application traffic patterns, as well as aiding in capacity planning.

CA ANOMALY DETECTOR



One of the key features of CA Network Analysis is CA Anomaly Detector. This feature uses dynamic algorithms to function like a network-wide monitoring system capable of discovering abnormal network behaviors and profiling them against a variety of known attack vectors, including SYN floods, ICMP floods, and abnormal traffic patterns sourced from unauthorized application servers. Anomaly Detector uses a combination of predictive analysis to reduce the amount of false positive security alerts and correlation of the remaining alerts, helping you build workflows to rapidly react to threats in the network.

One caveat of CA Anomaly Detector is that it requires the installation and configuration of CA Performance Center or CA NetQoS Performance Center. This would incur additional licensing costs for the organization.

CA NETWORK FLOW ANALYSIS INTEGRATION WITH OTHER CA PLATFORMS

CA Network Flow Analysis can integrate with CA Unified Infrastructure Management (UIM). This allows for the import of data collected by CA Network Flow Analysis into a centralized dashboard. CA UIM is required to integrate CA Network Flow Analysis with other CA enterprise infrastructure management tools and requires additional licensing at additional cost.

DIRECT COMPARISON

Both SolarWinds NAM and CA Spectrum are designed to monitor the networks and systems of large organizations. The key differences between the two solutions come down to the way each of them organizes their databases and the upfront costs of implementing each solution. There are also major differences in the amount of functionality provided by each solution as part of the initial package.

CA SPECTRUM

Many reviews of CA Spectrum from IT Central Station highlight the considerable number of features that are very basic. Many of these features seem more oriented toward monitoring systems instead of network devices, such as disk utilization and CPU utilization. There is support for *ping* and SNMP monitoring of devices. Another common issue is that multiple tools are required to unlock additional features, such as adding CA Network Flow Analysis along with CA Spectrum to get similar functionality to NAM, which includes all the tools in one package.

CA Spectrum gets great reviews for their customizability aspects as well as their powerful modeling engine that allows profiling of services. The downside to these features is that they require a considerable time investment to fully utilize. It also requires a good understanding of how the CA object model works to determine how devices and services interact. Building a business policy around these objects and interactions is where the solution shines, according to several of the reviews.

Another drawback for CA Spectrum and Network Flow Analysis is the model-centric view of monitored devices. CA Spectrum is very dependent on the model-driven aspect of the solution to build and monitor the database of devices. The flexibility afforded from storing device information this way gives the CA solutions the ability to add new features or functionality with a simple addition to the device model, but it requires significant training and understanding of the model method to get up and running quickly. This method is much better-suited for large enterprises with a substantial number of devices that need to be managed.

Pricing is also a concern for most organizations. CA Spectrum and Network Flow Analysis are priced per device and require a significant investment to get up and running. These solutions are marketed as "enterprise" focused, so CA may not be the best fit for a small-to-medium enterprise (SME). Many reviews of CA Spectrum cite the need to have multiple tools from CA to complete what administrators are looking to monitor and analyze. If purchasing the entire solution from CA is cost-prohibitive, other less-integrated solutions can be used at the cost of losing enhanced functionality from having a single vendor solution.

CA Spectrum and Network Flow Analysis have no trial offer available. Installation and configuration of the system could involve the use of a systems integrator. According to a publicly available price list from three years ago[1], the list price for a CA Spectrum server is $27,295[2]. The pricing for monitored devices is determined per node. For CA Spectrum, this price is $295 per node.

[1] www.bidsync.com/DPXViewer/ENS_CA,_Inc._Price_List_March_2015.xlsx?ac=view&contid=105022&docid=6215018&usg=AOvVaw1Um8JnsfCQS6S5ZLADXjUd

[2] All prices are shown in USD.

However, because CA Spectrum only includes a subset of the functionality necessary to monitor network traffic, we must also add on the cost of CA Network Flow Analysis to the total price of the solution to be equivalent to SolarWinds NAM. Pricing for CA Network Flow Analysis is $205 per node.

CA device pricing depends entirely on the ability of the device to support SNMP. If the device supports SNMP monitoring, it counts as a single device license. If the device can only be monitored via *ping*, it counts as a device license for every five standard device licenses. For the purposes of this comparison, we will assume that there are 1,000 devices with SNMP enabled. This would mean a total cost of $522,295 for a CA Spectrum server license, and 1,000 device licenses each for CA Spectrum and CA Network Flow Analysis

Integration with CA Unified Infrastructure Management would carry an additional charge for both products.

CA has also introduced a concept known as Gold Key licensing, which supports CA Spectrum and CA Network Flow Analysis running in a licensing mode without restriction. However, the licensing mode still requires that all monitored devices be licensed in the system. This would reduce the cost of the software itself, but still carry a license fee for each monitored device.

SOLARWINDS NAM

SolarWinds NAM offers a lot of tools for the investment. On top of including functionality like performance monitoring and NetFlow traffic analysis in the basic packet, NAM also includes functionality like WAN link quality monitoring, VoIP quality scoring, and IP address management. These are functions that are not available to users of CA Spectrum or CA Network Flow Analysis without purchasing add-on software or third-party offerings.

SolarWinds NAM also offers more simplicity for small- and medium-sized enterprises. The device discovery process and database import system are friendlier for users that are familiar with standard user interfaces for monitoring systems. The devices are imported and configured for monitoring right away without the need to go through the additional steps of the modeling process.

SolarWinds NAM has a pricing model that involves a free 30-day trial. The pricing model for NAM is different than the basic SolarWinds tools that are modeled on a per-interface model. NAM is priced per managed node. Because NAM is targeted at the higher end of the enterprise market, the minimum license package is for 1,000 managed nodes. The list price for NAM for a 1,000-node configuration is $95,000 as of May 2018.

CONCLUSION

Both CA Spectrum and SolarWinds NAM are highly rated enterprise network monitoring solutions. When CA Spectrum is paired with CA Network Flow Analysis and CA UIM, the functionality approaches that of SolarWinds NAM. However, SolarWinds NAM includes more features such as IP address management, VoIP monitoring, and full-featured wireless monitoring and troubleshooting capabilities.

SolarWinds NAM also has an edge on pricing. NAM offers a free trial option to help ensure that all the devices and systems you want to monitor are supported and the cost of the solution at the 1,000-node entry point is much, much lower than that of CA Spectrum alone before bundling in additional products.

While CA Spectrum has a more robust monitoring database thanks to their model-centric view of devices, this type of configuration is overkill for most monitored systems that will be encountered in the real world. CA Spectrum still relies heavily on SNMP to collect and report on data. If SNMP is a requirement, the need for complex modeling is negated in favor of simple device management.

SolarWinds NAM is a unified network monitoring solution with a set of features that are best-of-breed and integrated out of the box, without the need for additional programs or complicated setups. The monitoring aspects of NAM are easy to configure with SNMP out of the box and don’t require text file imports to begin discovering devices on the network. Once configured, SolarWinds has robust reporting features and can be configured to alert on a variety of faults and conditions.

SolarWinds NAM also includes a vast number of tools for the value. While you may not initially think you need to monitor WAN circuits in your enterprise, you may find that it becomes necessary after shifting your workloads to the cloud. With WAN monitoring and path analysis built into NAM, you can increase the monitoring functionality of your organization without increasing the price you pay for the software that monitors it. As your organization grows and changes, so do your monitoring capabilities with SolarWinds NAM.

ABOUT THE AUTHOR

Tom Hollingsworth, CCIE #29213, is a 15-year veteran of the networking industry. He spent over a decade as a Senior Network Engineer for an education-focused reseller, specializing in the implementation and operation of advanced technologies. Tom is well versed in the mechanics of campus and data center networks, voice and collaboration systems, and data center virtualization.

Tom is currently serving as an event lead on the Tech Field Day event series, specializing in Networking and Mobility technologies. He speaks daily with companies on the forefront of exciting innovative ideas and incredible fresh solutions and works with industry influencers to help the greater networking community understand how they work and how networking professionals can take advantage of them in everyday practice.

Tom is also a staff writer for Gestalt IT, where he covers networking, security, and mobility topics in-depth for the community. He has authored many posts about these topics, including several white papers.