

Gigamon[®]

Application Note

System Monitoring and Observability Leveraging Gigamon and VIAVI NITRO AlOps

Introduction

Monitoring systems at service providers and large enterprises have grown to become more complex as networking systems evolve, virtualized and cloud instances become a reality, and sophisticated analytical tools are deployed. These systems have been deployed with multiple vendor solutions and perhaps without integration in terms of managing, operating, and configuring the tools together.

The heart of many of these monitoring systems is a network packet broker provided by partners such as Gigamon. The functionality of the network packet broker is to tap, replicate, aggregate, filter and distribute monitored traffic to multiple probes and data analysis tools. However, a disruption of the monitored traffic from the traffic generating network elements, within the packet broker fabric or to the analytical tools may be difficult to pinpoint.

To integrate, visualize and automate processes associated with monitoring system operations, VIAVI has developed a novel approach to monitoring system observability using NITRO[®] AIOps. The following describes a use case combining the capabilities of NITRO AIOps with a packet broker from Gigamon.

Gigamon with NITRO AlOps from VIAVI

VIAVI plus Gigamon is a combination worth more than the sum of its parts. Gigamon, the leader in deep observability, provides comprehensive visibility across the entire hybrid cloud to amplify the power of performance and service assurance tools like NITRO AIOps. When combined, additional value is unlocked, providing extended visibility into the network and simplified operations.

In the following use case, Gigamon provides APIs to their Fabric Manager, which is a configuration software or element management system for packet brokering equipment. VIAVI created adaptors to the Fabric Manager APIs to show inventory, topology, and a light performance management for in/out traffic.

Additionally, VIAVI uses auto-discovery functions to build a unified inventory and data model from multiple sources (e.g. switches, routers, virtual nodes, cloud instances, firewalls, load balancers, probes, data lakes) which create even deeper end-to-end monitoring observability. The result is a holistic or single-pane-of-glass view of the monitoring fabric, from "tap to GUI."

The following shows a step-by-step outline of the process.

First, network inventory is required to identify all the devices within the network monitoring fabric. The premise is "if you don't see it, then you can't monitor it:"

nventory Overview			IP x 👻 Region	*	B +
		Ros]:	uter 2		
Select All	Operation Status	Region	Device Name	Device ID	Category
TA200E (1)	up	USA	ClusterTD-LS-TA25E-13	10.115.35.39	Active
HC2 (2)	up	USA	ClusterTD-LS-TA200E-6	10.115.35.38	Active
HC1 (2)	up	USA	ClusterTD-LS-HC2P-2	10.115.32.32	Active
TA25 (1)	up	USA	ClusterTD-LS-HC1-8	10.115.32.38	Active
	up	USA	ClusterTD-LS-HC3ccv2-12	10.115.32.92	Active
HC3 (2)	up	USA	ClusterTD-LS-HC3-1	10.115.32.31	Active
TA400 (2)	up	USA	ClusterTD-LS-TA25-7	10.115.32.93	Active
TA200 (1)	up	USA	ClusterTD-LS-TA400-4	10.115.32.94	Active
TA25E (1)	up	USA	ClusterTDLS-TA200-10	10.115.32.90	Active
	up	USA	ClusterTD-LS-TA400-14	10.115.32.34	Active
	up	USA	ClusterTD-LS-HC2P-5	10.115.32.35	Active
	up	USA	ClusterTD-LS-HC1-9	10.115.32.39	Active

Inventory can then be analyzed and reported down to the device level, CPU, memory, and port usage:

Go × +				- 0
A Not secure 10.40.184.101	:30398/#/portal/overview		2 A to 🧔 🤇 🗎 🖬 🦉	L
ed favorites folder 📋 My tools 📋 Project	ts 🙀 Home - Workday 🗶 Sujith Kumar - Pref 🏚	SharePoint 💠 🌰 My files - OneDrive 💿 VM instances -	Co 💥 pve100 - Proxmox 🙆 Google Cloud Deve	>
3			🔍 🛃 🏚 🔡 🖪 📑 Hi, Gigamon	G
iventory Overview		IP × -	v no	
ventory Overview - Router				
				-
Device Summary Device Inv	ventory			
Device ID	10.115.32.38	Discovery Profile Name	-	
Device Name	ClusterTD-LS-HC1-8	Discovery EMS Name	-	
Tower ID	Tower01	Last Discovered Date	-	
Domain	IP	Box ID	8	
Device Type	Router	Chassis ID	H09C9	
Site	Sitel	Hardware Type	GVS-HC100/CHS	
Region	USA	Hardware Revison	DO	
Province	-	Serial Number	H09C9	
Kabupaten/Kodya	-	Product Code	132-00D5	
Kecamatan/District	-	Product Name	GigaVUE-OS	
Desa/Kelurahan	-	Product Version	6.3.00	
Category	Active	System Mode	operational	
Vendor	gigamon	Operation Status	up	
Create Date	06-01-2023 07:56:40		Box ID,Chassis ID,Hardware Type,Hardware	
Last Modify Date	06-01-2023 07:56:40	columnsHeaders	Revison, Serial Number, Product Code, Product	
			indicate in a second of a seco	

In addition, users gain a topology view – where they can visually see the logical interfaces and connections between network devices:



Finally, fault management data can be implemented and displayed for devices to show network device system alarms. Correlation of fault management data from disparate devices can eliminate alarms and generate incidents to reduce the mean time to detect (MTTD) issues. Then, performance KPIs can be overlayed for interfaces in between network devices to show network performance health:



In sum, the procedures described above can create end-to-end, deep observability and help identify anomalous network behavior. This will trigger network orchestration and automation, and ultimately generate closed-loop procedures. Together, Gigamon and VIAVI are helping service providers and large enterprises improve system monitoring resiliency across their networks.

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-level intelligence to amplify the power of observability, performance, security, and service assurance tools. This powerful combination enables IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: modern enterprises and service providers realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit <u>www.gigamon.com</u>.

About NITRO AlOps

The NITRO cloud-native Artificial Intelligence for Network Operations (AIOps) portfolio helps CSPs, DSPs, ISPs, Utilities, and Enterprises accelerate their digital OSS transformation journey by evolving their legacy network operations center (NOC) to a dark NOC. The AIOps End-to-End Service Assurance solution enables the breaking down of silos across network domains to provide a vendor agnostic and holistic view of the entire network. With real-time monitoring, AIOps enables root cause identification of customer experience (CX) impacting issues enabling proactive problem resolution.

NITRO AlOps visualizes, automates, and optimizes digital experiences as well as service and network quality across hybrid telco and IT networks by integrating real-time assurance with closed-loop automation and analytics driven by artificial intelligence/machine learning.

Powered by topology, assurance and analytics suite of applications, NITRO AlOps governs the digital experience as well as service and network quality with intelligence that monitors, detects and heals by leveraging local orchestrators, driving digital transformation initiatives towards autonomic network management.





Contact Us +1 844 GO VIAVI (+1 844 468 4284)

To reach the VIAVI office nearest you, visit viavisolutions.com/contact

© 2023 VIAVI Solutions Inc. Product specifications and descriptions in this document are subject to change without notice. Patented as described at viavisolutions.com/patents gigamon-nitro-aiops-an-xpf-nse-ae 30193867 900 102

viavisolutions.com