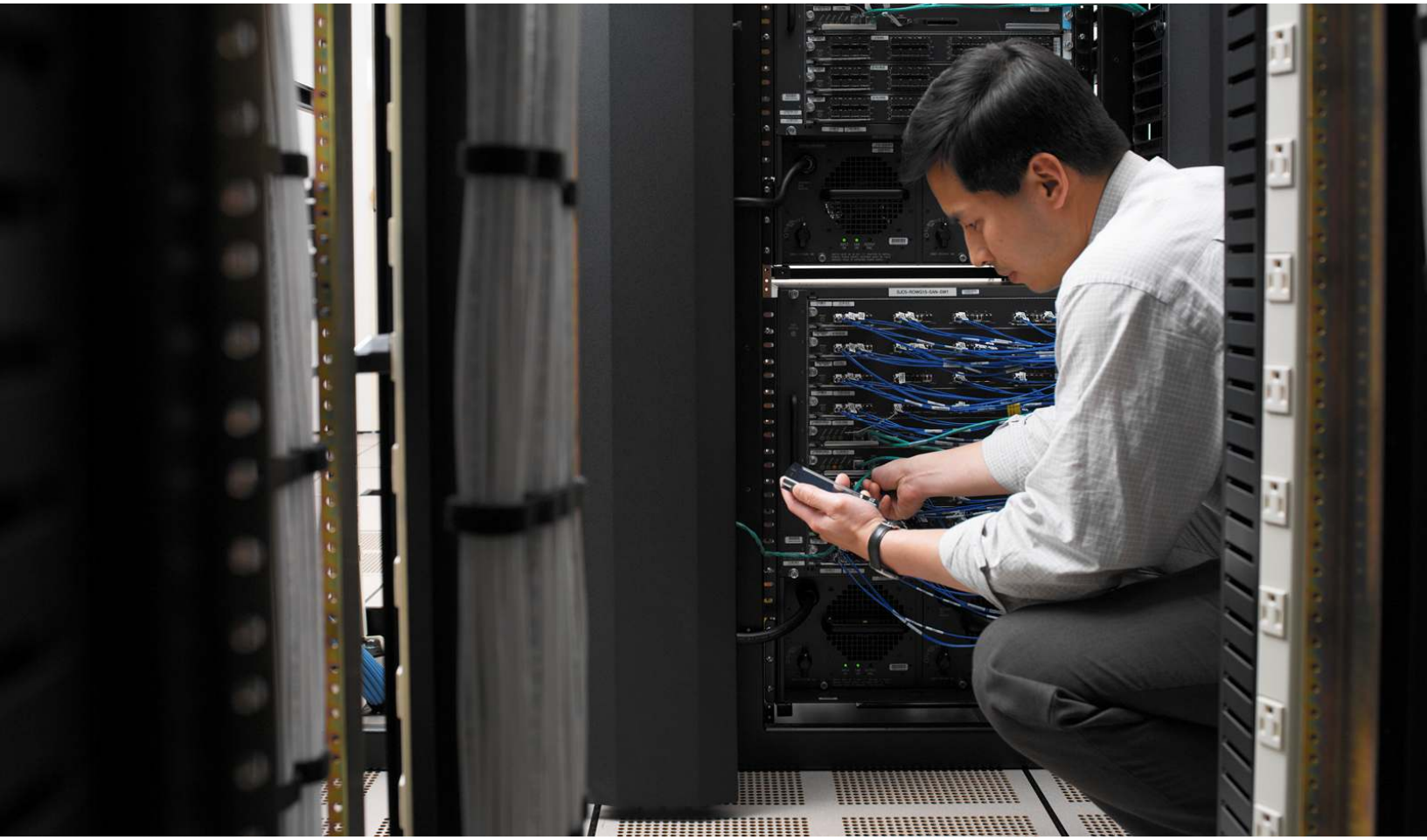
Assurance Management Reference Architecture for Virtualized Data Centers in a Cloud Service Offering



Josh Josyula
Madhukar Wakade
Paul Lam
Tarpley Adams

Contents

Overview

This document provides information on managing a virtualized data center in a cloud service offering. It includes a reference architecture, demonstration cases, and best practices with respect to assurance management (fault and performance) of a data center that is comprisd of network, compute, storage, and applications.

In the past, network management meant managing a network that consisted of network devices. Traditionally, we have used Telecommunications Management Network (TMN) and TeleManagement Forum (TMF) models. Because the network resources in a traditional network are more static, managing them is not as complex an undertaking as it is a virtualized environment. Simply put, it is easier to manage something that is not constantly changing.

Now, more companies (enterprises and service providers) are moving into virtualized and cloud environments, in order to do more with less, cut costs, improve agility, and reduce energy consumption. However, virtualization also presents many challenges for network operations. Now, operations must to deal with not only virtual networks, but also with virtual compute platforms (servers, virtual machines, applications), virtual storage devices, and dynamic mobility, since elements are not static in a virtualized environment.

The term “virtualization” has become synonymous with server virtualization, but it should be understood that servers and applications would not be able to communicate without a network and storage; these also need to be virtualized in order to efficiently realize a cloud environment.

This paper is designed for architects, engineers, and operations personnel with an interest in the design, deployment, and use case testing relating to the management of cloud or virtualized infrastructures. This paper also addresses the solution architecture for managing a cloud or virtualized environment from the assurance perspective. From an assurance perspective, it should not matter whether it is an enterprise or service provider deployment, public or private, or a hybrid cloud. The underlying infrastructure resources (network, compute, storage, and applications) need to be managed for fault and performance, including service-level agreements.

Virtualization and Data Centers in the Cloud

Virtualization is one of the main principles of cloud computing. Virtualization allows us to create many virtualized resources from one physical resource. This form of virtualization allows data centers to maximize resource utilization. In the context of cloud computing, multiple resources (network, compute, and storage) are grouped together to form one “cloud.”

In a cloud environment, the association of network, compute, and storage resources are dynamic to the applications. In other words, whenever a virtual machine (VM) is added on top of a server for new applications, the corresponding virtual network (VLAN, VDC, VIP, etc.) and virtual storage need to be configured dynamically, before the service can be offered to the customers. Also in a cloud environment, the resource usage is tracked at a granular level and billed to the customer on a short interval time basis.

The clouds will hide infrastructure resources and allow control by users, while providing automation to reduce the complexity. The automation allows the cloud infrastructure to be rearranged as needed when a service is ordered or enabled. In a cloud environment, the IT resources and services are abstracted from the underlying infrastructure and provided “on-demand” and “at scale” in a multi-tenant environment.

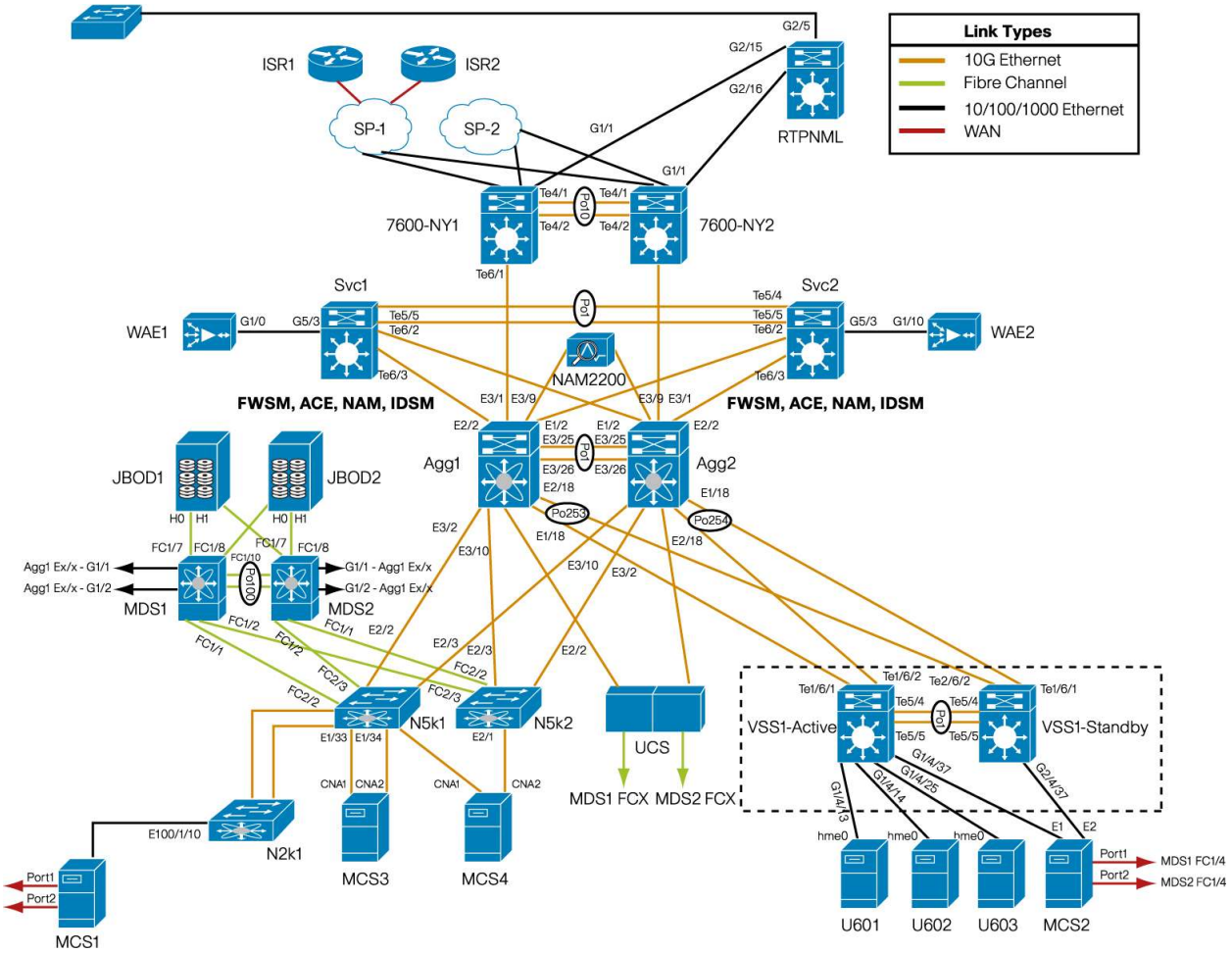
Reference Network for Data Center Assurance Management

The fault and performance management solution was tested in a Cisco laboratory that was built for testing different management solution architectures. This lab is commonly referred to as the Next Generation Data Center (NGDC) Proof of Concept (POC) Lab. The lab also serves as the research center for the Cisco's cloud NMS activities. Figure 1 shows the layout out of the physical infrastructure that the lab used for fault and performance testing in this paper. The multilayered architecture is comprised of core, aggregation, services, and access layers. This architecture allows new modules to be added as demand increases.

3.1 Core Layer

The data center core layer provides high-speed Layer 3 routing for all traffic in and out of the data center. The core layer provides connectivity to multiple aggregation devices and provides a resilient Layer 3 routed fabric with no single point of failure. The core layer is connected to other functional blocks such as Campus, Internet edge, and Wide Area Network (WAN). The core layer consists of Cisco Nexus 7000 Series switches. The switches run on Cisco NX-OS, a modular operating system also designed to operate today's data centers. The Nexus offers unique virtualization features, such as virtual device contexts (VDCs) and virtual port channels (vPCs). In the lab, we used Cisco 7600 Series routers to support the Layer 3 routing. These are shown in Figure 1 as 7600-NY1 and 7600-NY2.

Figure 1. NGDC POC Lab Physical Architecture



3.2 Aggregation Layer

The aggregation layer serves as a boundary between Layers 2 and 3 for the data center infrastructure. It consolidates all Layer 2 traffic and provides platform services, such as firewall and load-balancing services. Layer 2 (the aggregation layer) uses the Cisco Catalyst 6500 Series Virtual Switching System (VSS) and vPC to eliminate the single point of failure in Layer 2 domains. The Nexus and VSS switches can be used in Layer 2; in the lab, the VSS was used with 10 Gigabit Ethernet interfaces. This allows support for a unified fabric architecture supporting combined Fibre Channel over Ethernet (FCoE) and IP traffic on a common infrastructure.

3.3 Services Layer

Network and security services such as firewalls, server load balancers, intrusion prevention and detection systems (IPSs/IDSs), and network analysis modules are typically deployed at the services layer. In the lab, we deployed the Cisco Firewall Services Module (FWSM), Cisco Application Control Engine (ACE), and Cisco Network Analysis Module (NAM) as Cisco Catalyst 6500 Series modules.

3.4 Access Layer

The access layer connects the server farm end nodes in the data center with the aggregation and services layers. The Cisco access layer also provides convergence of storage and IP traffic onto a common physical infrastructure, called a unified fabric. The Cisco Nexus 5000 Series of switches supports storage and IP traffic through support for FCoE switching and 10 Gigabit Ethernet. Server nodes may be deployed with converged network adapters (CNAs) supporting both IP data and FCoE storage traffic, allowing the server to use a single set of cabling and a common network interface. The Nexus 5000 Series also offers native Fibre Channel interfaces to allow these CNA-attached servers to communicate with traditional storage area network (SAN) equipment.

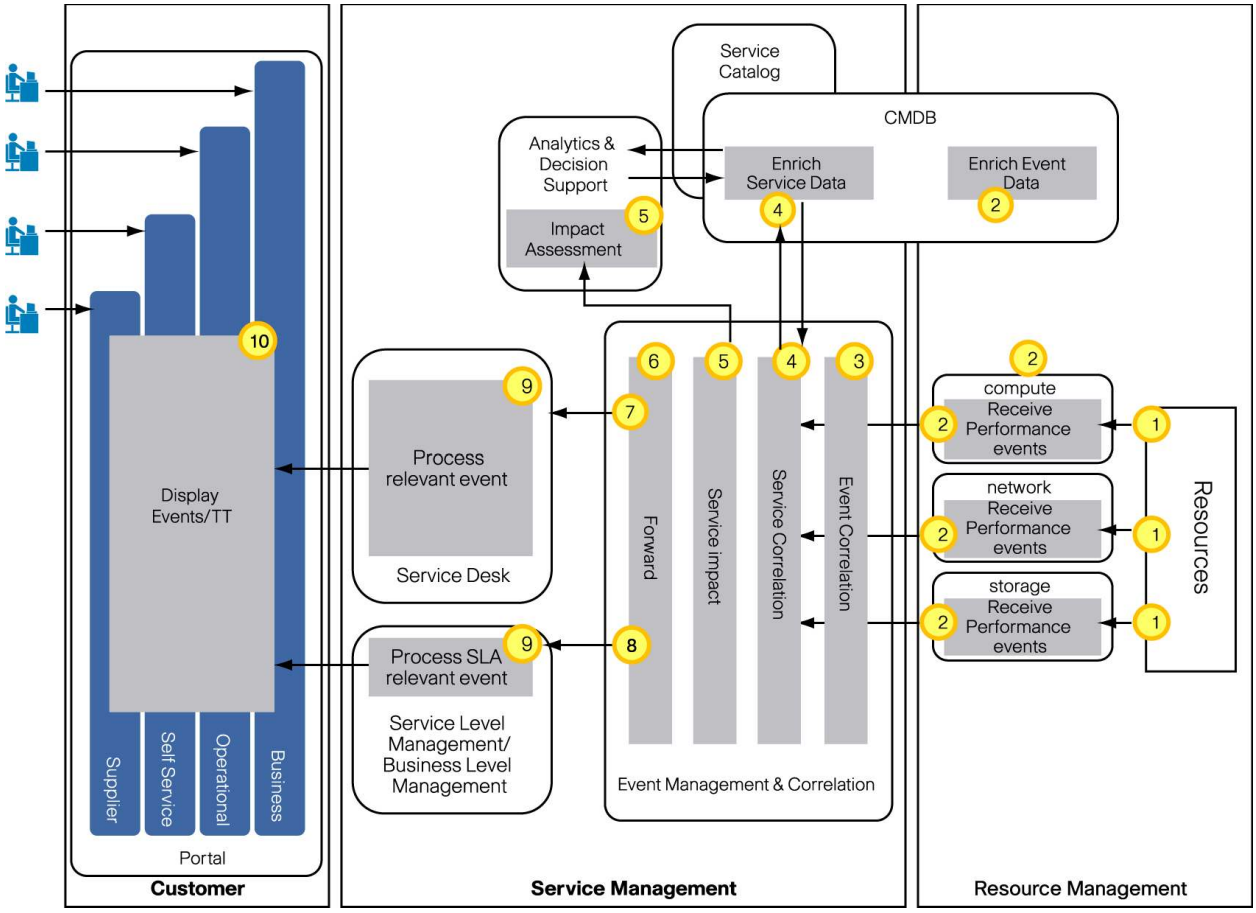
In the lab, we used a new Cisco Unified Computing System (UCS) with four blades for the compute nodes, and Cisco MDS devices for the SAN.

Service Assurance in the Data Center and the Cloud

The data center's assurance process targets the need to monitor and assure the high availability and high quality of the services delivered to the customers. It consists of proactive and reactive maintenance activities, service monitoring, resource status and performance monitoring, and troubleshooting. This includes continuous monitoring to proactively detect possible failures, and the collection of performance data and analysis to identify and resolve potential or real problems.

Figure 2 illustrates the assurance process architecture that is used in data centers to effectively manage compute, network, and storage events.

Figure 2. Assurance Process Flow



The following sections discuss the NMSs chosen to fulfill the assurance process flow, from Figure 2, as well as their integration points and data flows, and include real-world demonstration cases, all from a fault and performance standpoint. The focus is on the collection, reporting, and threshold detection aspects of performance management—we leave capacity management to a future publication.

4.1 Fault Management

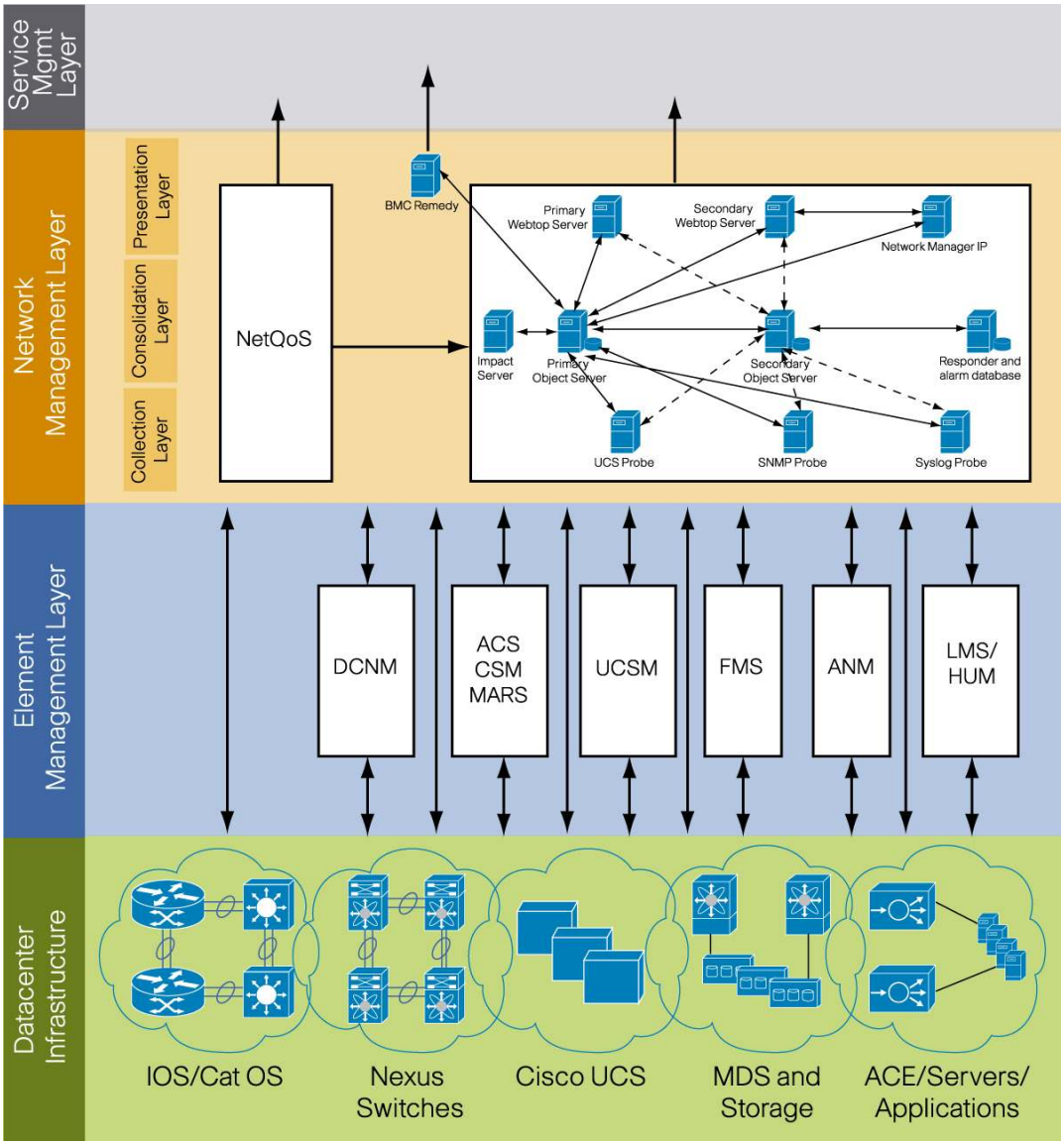
Fault management is a set of functions that enable the detection, isolation, and correction of abnormal operation in the infrastructure devices. Fault management requires collecting faults from the resources in the infrastructure through different methods (polling the devices and events generated by the devices) and different technologies: SNMP traps, XML messages, syslog messages, etc. Once the events are collected by the Network Manager from various sources, either directly from network elements or from an element management system (EMS), they need to be correlated for root cause analysis and normalized (format the events in a consistent way). The number of events that come from devices can be very high; these need to be filtered for any unnecessary/undesired events. Often, the EMS adds value by reducing the volume of event flow, providing value-added events (root causes), and providing localized polling. Please note that the Network Manager used in this paper manages network, compute and storage devices, but is still referred to as a network manager, since this term is commonly used.

The network management systems de-duplicate and correlate the events to determine the root cause of the fault. EMS systems send filtered and correlated events to the top-level NMS. Once the root cause is determined, the faults are displayed for remediation.

4.1.1 Fault Management Architecture

NOCs (Network Operations Centers) frequently need to capture alarms and events from various types of equipment, and then translate that to a standardized alarm format and display the alarm to a user interface. Figure 3 shows our reference fault management architecture, including layers of management functions. More information about the specific products shown in this architecture is provided later in this document.

Figure 3. Fault Management Architecture



The type of fault management architecture that is used depends on the underlying technologies, customer requirements, and operations practices within the customer's environment. The major architectural choice is around the presence and use of the EMSs. The EMSs can reside between the network management layer (NML) systems and the actual managed elements, and offload the NML from polling and event collection responsibilities. The EMSs perform some localized (within their domain) fault reduction, and then forward events and present status to the NML, which conducts further event and status analysis across the entire network.

In practice, EMSs do not always provide sufficient technology to support this architecture, and the NML systems must collect data directly from the managed elements. In this case, the EMSs are typically retained for their customized provisioning UIs, and/or customized fault UIs. Before implementing a fault management architecture in a

customer environment, a fault management assessment must be conducted to determine the appropriate management architecture. Our reference architecture includes a mix of EMS managed domains and direct connections between the NML and the other network elements. Figure 3 illustrates the connections and data flows present in the reference architecture. In our actual implementation and demonstration cases, we have not implemented all the indicated connections due to practical limitations.

For this lab implementation, we have used Cisco Info Center (CIC) in the network management layer of the fault management system. The NML shows three sub-layers: the collection layer, the consolidation layer, and the presentation layer. This layering approach is the best practice because it provides scalability and adoption of multivendor technology. The collection layer would have collection stations, where the events are collected directly from network elements or from the EMS. The number of collection stations depends on the number of devices and the number of messages that are collected.

A note on the presence of NetQoS in our fault architecture: We view the threshold violation events that NetQoS can generate to the fault manager as related to fault, in addition to the traditional performance management function. Threshold violations can be very interesting to NOC operators diagnosing a problem, and to automated fault reduction engines.

4.1.1.1 Element Management Layer

4.1.1.1.1 Cisco DCNM

Cisco Data Center Network Manager (DCNM) is a Cisco management solution for Cisco NX-OS-enabled hardware platforms. Cisco NX-OS provides the foundation for the Cisco Nexus product family. The DCNM server uses the XML management interface of Cisco NX-OS devices to manage and monitor them. The XML management interface is a programmatic method based on the NETCONF protocol that complements the CLI.

4.1.1.1.2 Cisco UCS Manager

Cisco UCS Manager is an embedded device management application that manages the Cisco Unified Computing System as a single logical, highly available entity from end to end. It provides an intuitive GUI, CLI, and XML API.

Cisco UCS Manager resides on a pair of Cisco UCS 6100 Series Fabric Interconnects using a clustered, active-standby configuration for high availability. The UCS Manager participates not only in server provisioning, but also in device discovery, inventory, configuration, diagnostics, monitoring, fault detection, auditing, and statistics collection.

Cisco UCS Manager provides an XML-formatted event stream for forwarding to the top-layer NML. Cisco Info Center receives an event stream on the TCP/IP socket and tokenizes the XML-formatted events for displaying on its webtop. Events are grouped based on UCS modules (e.g., chassis, fabric LAN, fabric SAN, fabric switch, blade, CPU, global systems, etc.).

4.1.1.1.3 Cisco Fabric Manager Server

Cisco Fabric Manager Server (FMS) manages Cisco MDS NX-OS Release 4.2(1) running on Cisco MDS 9000 Family switches. The GUI provides easy configuration of a storage infrastructure. In the future, Fabric Manager capabilities will be ported into DCNM to manage both Nexus and MDS switches.

FMS is used for configuring SNMP, RMON, SPAN, and the Embedded Event Manager (EEM). The SPAN feature is specific to switches in the Cisco MDS 9000 Family. Apart from logging all messages in the form of syslog messages, it supports various MIBs for generating SNMP traps. Also, through a GUI, it allows control over which event will be enabled at the global level or the individual device level.

4.1.1.1.4 Cisco Application Networking Manager

Cisco Application Networking Manager (ANM) enables centralized configuration, operations, and monitoring of Cisco Application Control Engine (ACE) devices, as well as operations management for the Cisco Content Services Switch

(CSS), Cisco Content Switching Module (CSM), Cisco Content Switching Module with SSL (CSM-S), and Cisco ACE Global Site Selector (GSS). ANM also centralizes operation management of virtual IP addresses and DNS rules for GSS devices.

Cisco ANM simplifies Cisco ACE provisioning through forms-based configuration management of Layer 4 through 7 virtualized network devices and services. With Cisco ANM, network managers are able to create, modify, and delete all virtual contexts of the Cisco ACE, as well as control the allocation of resources among the virtual contexts. Within these virtual contexts, Cisco ANM enables configuration of the content networking and Secure Sockets Layer (SSL) services.

4.1.1.2 Network Management Layer

Cisco Info Center (CIC) is used as the network manager to collect events from the infrastructure. The events can be collected either through the Cisco EMSs described in the previous section or directly from the devices. Following is a description of the available Cisco Info Center modules.

4.1.1.2.1 Cisco Info Center Probes

Probes act as event collectors and analyzers for CIC object servers. Probes store and forward the event data from all managed network elements. The object server collects and processes event information in the memory resident database before forwarding it to the reporter server. The probe rules file can be configured to filter and translate upon receipt of certain data.

4.1.1.2.2 Cisco Info Center Object Server

The core component of Cisco Info Center is the object server, which consolidates event information from the infrastructure through event sources such as syslog probe, mttrapd probe, socket probe, etc. The object server is a memory-resident, real-time database that aggregates and de-duplicates fault data and correlates it according to user-defined rules.

4.1.1.2.3 Cisco Info Center Gateways

The gateways link the object servers or other external systems, such as Remedy. They facilitate the propagation of information between servers, systems, and data storage. One of the most significant functions of a Cisco Info Center object server is its ability to support the real-time filtering and distribution of faults and events.

4.1.1.2.4 Cisco Info Center Webtop

Cisco Info Center Webtop is a front-end application that operators see and use locally or remotely connect to object servers. A flow-through interface enables integration with the existing operations support systems (OSSs). Webtop is a web-based operator tool running in a web browser.

4.1.1.2.5 Cisco Info Center Reporter System

The reporter system delivers reporting capabilities and supplements Cisco Info Center's object server for users that want to view network event data after it has been cleared from the real-time object server. The reporter system efficiently captures, stores, analyzes, and displays the Cisco Info Center event data to help network managers and operators understand and enhance network behavior.

4.1.1.2.6 Cisco Info Center Network Manager IP

Network Manager IP automatically discovers IP networks and gathers and maps topology data to deliver a complete picture of Layer 2 and Layer 3 devices. It captures not only the overall inventory, but also the physical, port-to-port connectivity between devices. Network Manager IP captures logical connectivity information, including VPN, VLAN, and Multiprotocol Label Switching (MPLS) services, including Layer 2 and Layer 3 VPNs. Network Manager IP is not used in the lab and in this paper.

4.1.1.2.7 Cisco Info Center Impact

Cisco Info Center Impact is the analysis and correlation engine for Cisco Info Center. Cisco Info Center Impact enables administrators to customize and enhance events by adding features such as advanced event and business data correlation, event enrichment, and event notification. In addition, Cisco Info Center Impact can be integrated with a wide variety of third-party software, including databases, messaging systems, and network inventory applications. Some examples of event enrichments include:

- Information from inventory database (site, building, location, etc.)
- Description of virtual context (not available in SNMP traps or syslog messages)
- Business data information (same device is shared by multiple customer and events are to be identified by customer, active/inactive state of the service, etc.)

4.1.1.3 Event Collection

The following table illustrates how event information can be collected from various parts of the infrastructure.

Table 1. Event Collection from the infrastructure devices

	IOS/Cat OS Devices	Nexus Switches	MDS Switches	UCS Blades and Chassis	ACE Appliances and Blades
Network Management	SNMP traps and Syslog messages are sent to Cisco Info Center. Cisco Info Center will tokenize the messages using the rules file.	Syslog messages are sent to Cisco Info Center. Cisco Info Center will tokenize the syslog messages using the rules file.	Syslog messages are sent to Cisco Info Center. Cisco Info Center will tokenize the syslog messages using the rules file.	The UCS platform provides XML-based event streams for receiving at the TCP socket probe. These events are processed at Cisco Info Center using the rules file.	Syslog messages are sent to Cisco Info Center. Cisco Info Center tokenizes the syslog message using the rules file.
Element Management	LMS is the event management system. It can forward the filtered events to Cisco Info Center using the notification service.	DCNM displays the events and alarms on the DCNM GUI.	FMS displays the events and alarms. (FMS will be merged into DCNM in the future.)	UCS Manager displays the events and alarms on the UCS Manager GUI.	ANM displays the events and alarms on the event browser.

4.1.2 Demonstration Cases

In this section, we will show how we have collected the fault events from the infrastructure devices in the lab (shown in Figure 1), de-duplicated and filtered them, and showed the root cause alarms on Cisco Info Center and on the Webtop.

Table 2. Collection of Fault Events from Network, Compute, and Storage Network Devices

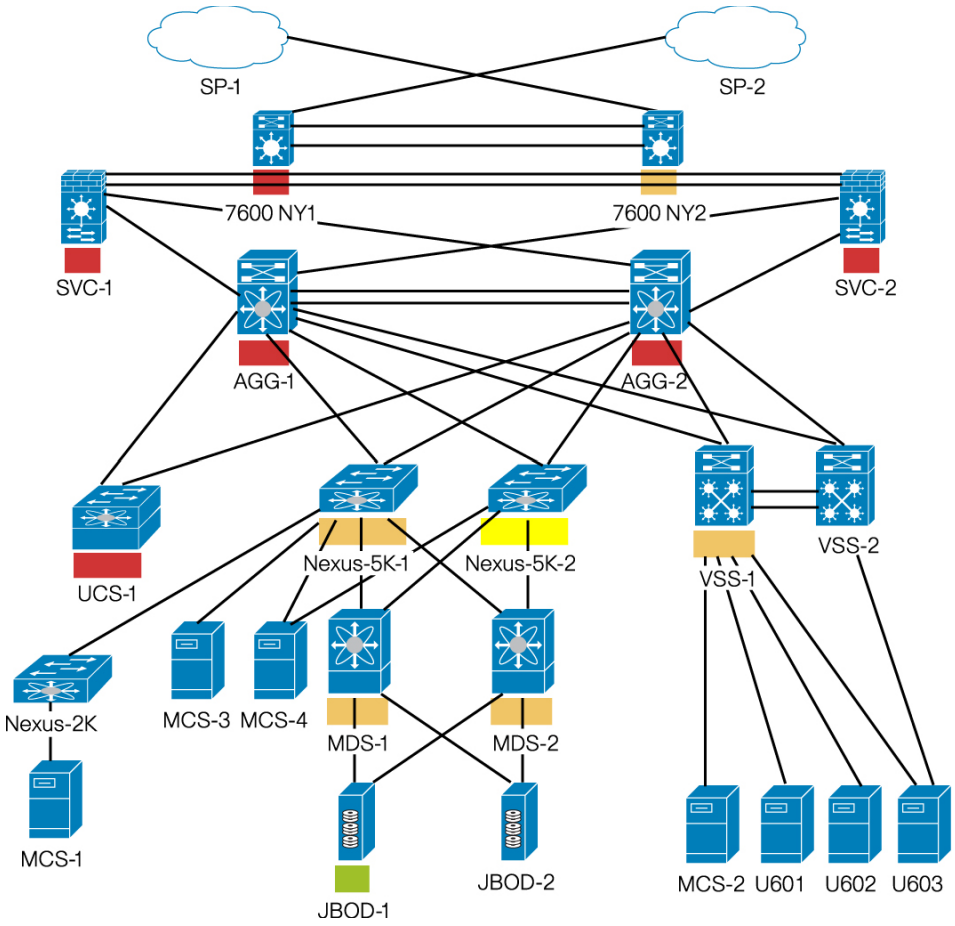
Description	Fault messages forwarded from the lab devices to Cisco Info Center
Requirements	Cisco Info Center and the lab devices as shown in Figure 1
Procedures	• Cisco Info Center receives traps/syslog/XML messages from the lab devices • Network elements and EMSs are configured to receive only important events at Cisco Info Center • Cisco Info Center rules file is configured to de-duplicate the events and do correlation • Event groups are created based on technology and management domain

4.1.2.1 Network Topology Map

The device configuration is retrieved by the configuration management system. This configuration is used for creating the network topology. The EMS uses the device configuration available within the EMS to create the network map or topology. At the network management layer, the network map/topology can be created manually or the EMS map can be launched by integrating the element management and network management layers.

Figure 4 shows the devices that are being monitored by Cisco Info Center. The network devices in the core, aggregation, service, and access layers described in Section 4 are monitored by Cisco Info Center. Also included are the UCS and storage devices (MDS) in the access layer.

Figure 4. Cisco Info Center Webtop Dashboard Showing the Devices and Alarm Information



4.1.2.2 Network Events

Figure 1 describes the core, aggregation, service, and access layers with various network elements. The Nexus platform with NX-OS is relatively new, and not many COTS (Commercially Off-the Shelf) systems are capable of interfacing with these switches. To assist with integration, we have developed Cisco Info Center interfaces to the Nexus platform and to other switches, such as the Cisco Catalyst 6500 Series VSS.

4.1.2.3 Compute Events

Cisco Unified Computing System (UCS) is Cisco's new compute platform. As part of our integration efforts, we have developed Cisco Info Center technology that can monitor the UCS. This technology is able to:

- Confirm events that can be retrieved from UCS
- Identify interested events from the event stream, and retrieve those events
- Map UCS severity events with the existing MOM (Cisco Info Center)
- Create event groups on the basis of managed objects
- Correlate events
- Display events on a dashboard

4.1.2.4 Storage Events

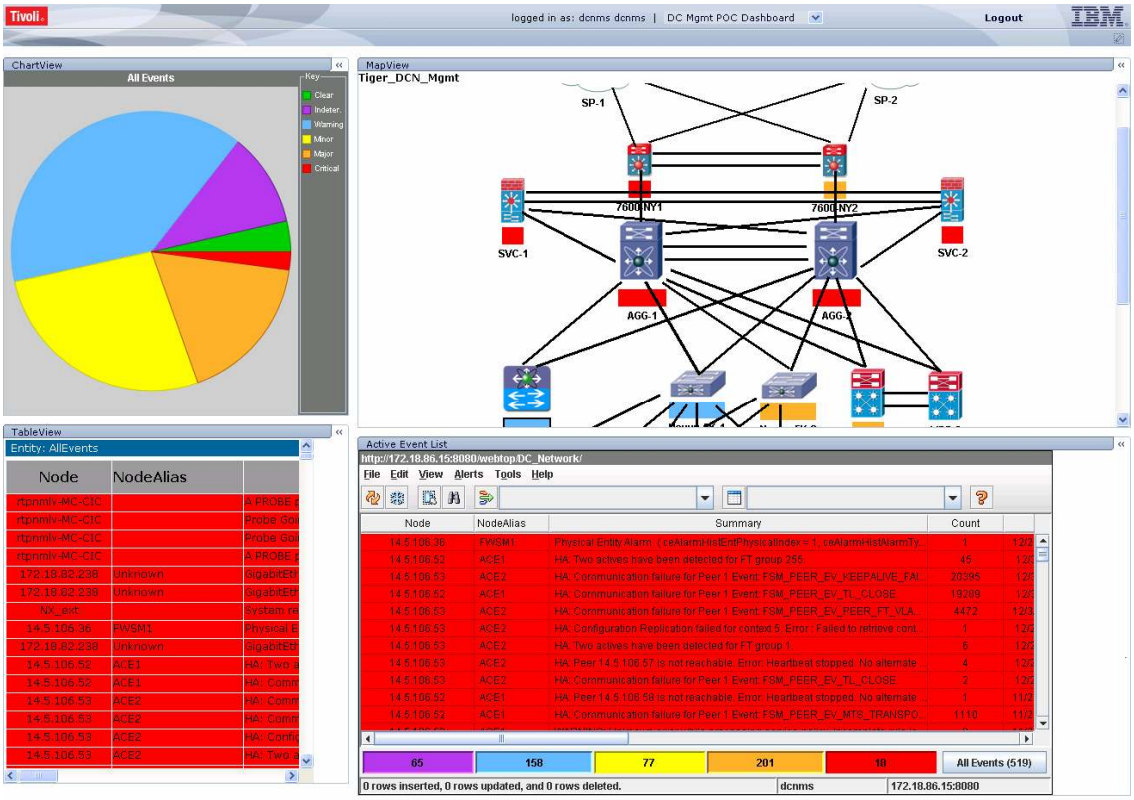
Cisco MDS storage switches are used for the SAN. Since these are new platforms, and have not been managed by network management systems before, we first determined the MIBs that need to be monitored for the network events.

4.1.2.5 Unified Event Display For Fault Management

Generally, the network, compute, and storage fault management may be done separately by disparate systems and separate staff may be used for managing these infrastructures. However, for cloud and virtualized environments, these need to be combined and alarms need to be displayed on a single pane of glass to quickly identify the problem areas for remediation. Consolidating all events from network, compute, and storage and displaying the information on a single pane of glass will provide tremendous value for the operations staff.

Figure 5 shows a consolidated dashboard with alarms from network, compute, and storage. The figure shows four quadrants. The top left quadrant shows a pie chart with cleared events and indeterminate, warning, minor, major, and critical alarms. The bottom left quadrant shows a summary of all NGDC infrastructure events. The same information is also shown on the bottom right quadrant with a more detailed description. The top right quadrant shows the infrastructure with all the devices marked, and the rectangular boxes underneath each device show the color-coded alarm condition. By clicking on these boxes, the detailed alarm condition for a particular device can be displayed in the bottom right quadrant.

Figure 5. Cisco Info Center Dashboard Showing Alarms from the NGDC Infrastructure



Figures 6, 7, and 8 show the alarms from network, compute, and storage platforms. These are obtained by clicking the respective boxes underneath the devices in the dashboard shown in Figure 5.

Figure 6. Cisco Info Center Dashboard Showing Network Alarms

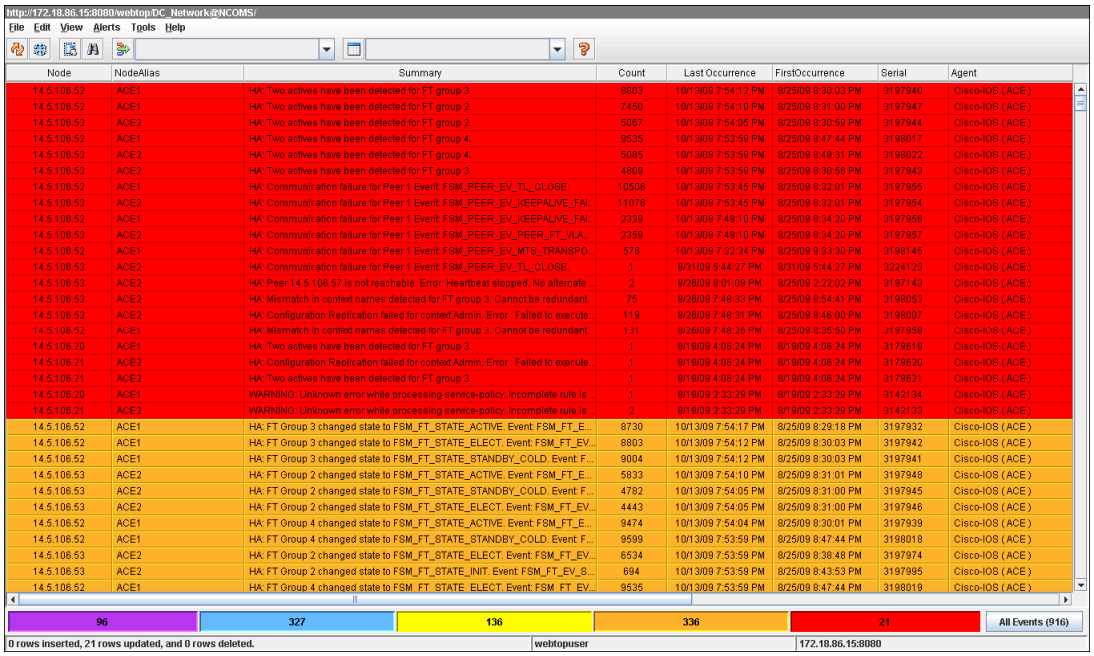


Figure 7. Cisco Info Center Dashboard Showing Storage Network (MDS) Alarms

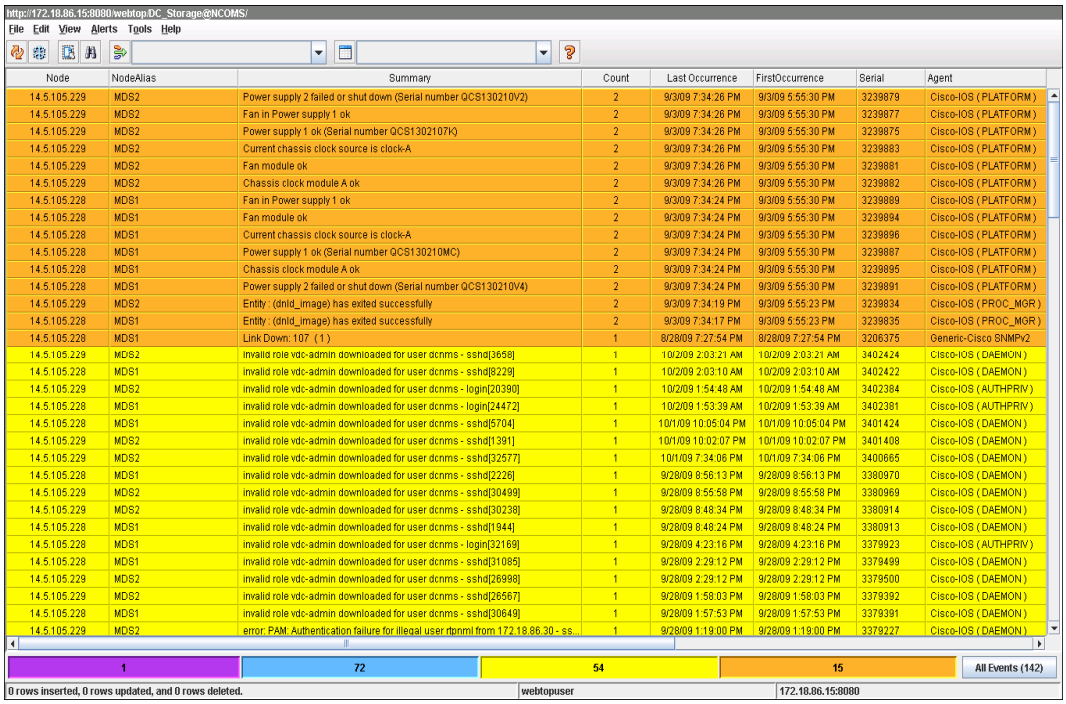
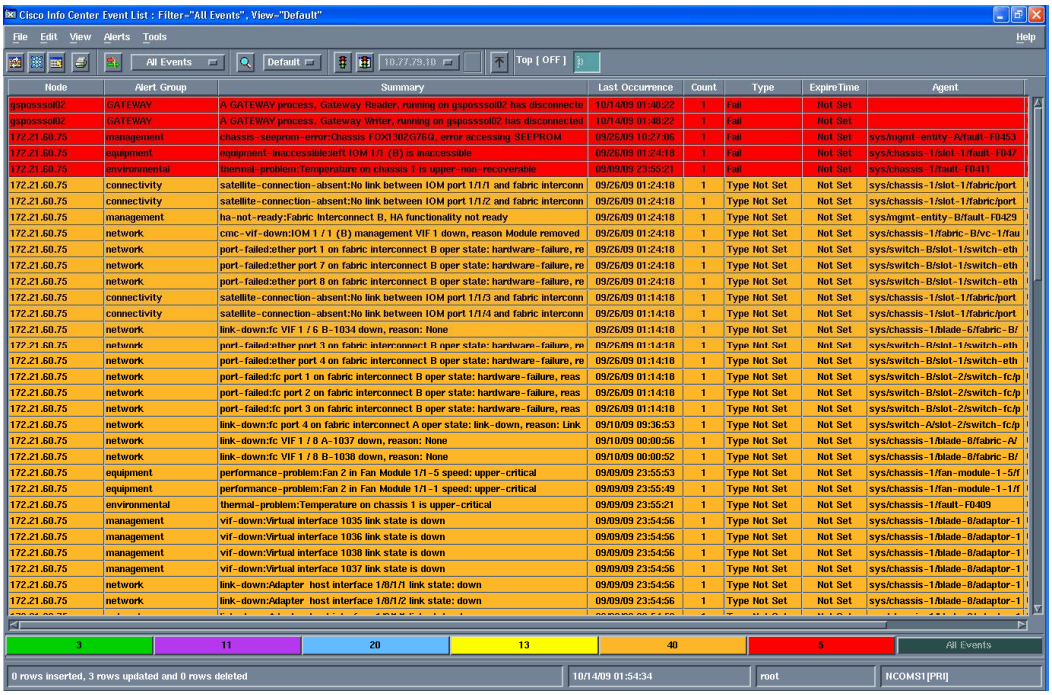


Figure 8. Cisco Info Center Webtop Dashboard Showing Compute (UCS) Alarms



Bridging the space between fault and performance management are threshold crossing alerts. These alerts can be very useful in trouble resolution, so performance systems send these alerts to the fault management systems. This feature is planned for the next iteration of our implementation in the lab.

4.2 Performance Management

Performance Management (PM) for the NGDC covers performance monitoring, data analysis, and performance management processes.

PM manages network devices, platforms, and application key performance indicators (KPIs), and analyzes monitored performance data by providing baseline reports and generating reports on capacity, traffic forecasting, threshold violations, and performance level.

4.2.1 Performance Management Architecture

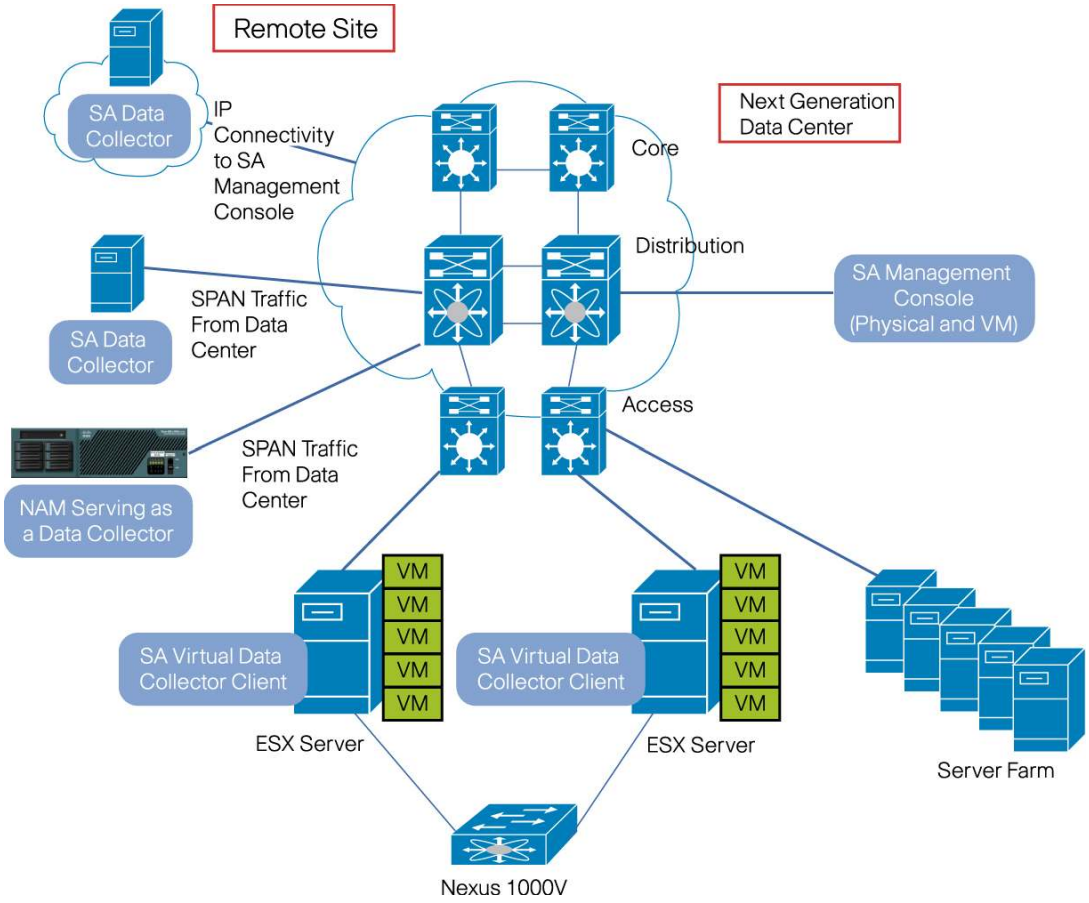
NetQoS, a system for performance mangement, was used in the NGDC POC Lab. Cisco uses other partner products in its performance management architecture, and has tested some of the products, such as SolarWinds and InfoVista. For the purpose of this paper, however, we are showing our strategy and results using the NetQoS tool.

The NetQoS performance management solution being utilized for performance management has three components: NetQoS SuperAgent (SA), NetQoS ReporterAnalyzer (RA), and NetQoS NetVoyant (NV). SA is the end-to-end application performance monitoring and analysis solution using spanned traffic (packets) as a data source. RA is the network traffic analysis solution using NetFlow as a data source. NV is the element management solution using SNMP polling. The following sections describe the NetQoS solution architecture and the NetQoS modules used.

4.2.1.1 NetQoS Super Agent

Figure 9 shows the Super Agent (SA) architecture. The SA solution has two components: the data collector and an SA console. Data collectors capture and store network traffic captured via a SPAN port in the network. The SA management console acquires data from the data collector and generates end-to-end application performance reports. The NetQoS data collector can be a Cisco NAM, or a NetQoS data collector.

Figure 9. Super Agent Architecture

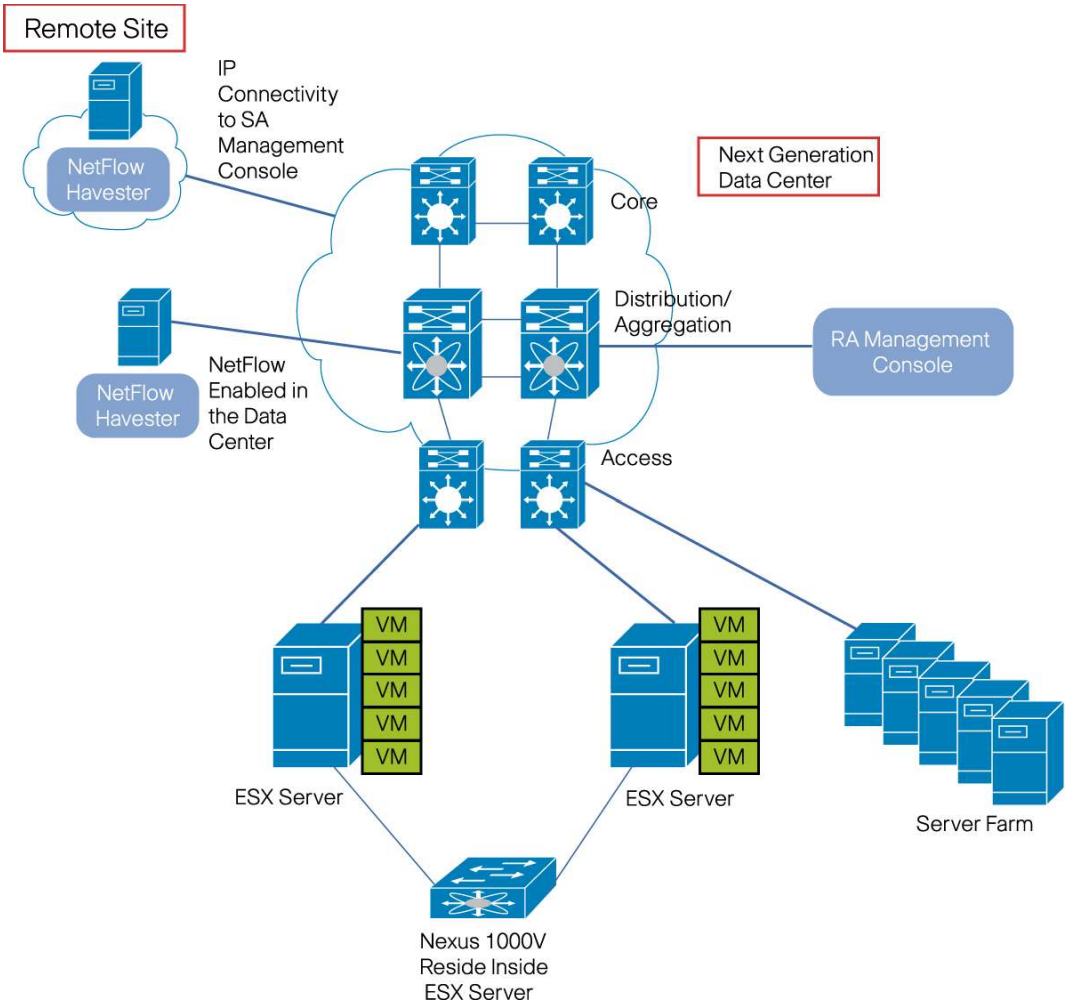


The SA Virtual Data Collector Client resides on the ESX Server and collects performance data from the virtualized switch—the Cisco Nexus 1000V. The Nexus 1000V is a software switch on a VMWare ESX server that delivers the Cisco VN-Link services to virtual machines hosted on that server.

4.2.1.2 NetQoS Reporter Analyzer (RA)

Figure 10 shows an RA architecture. The RA solution uses NetFlow as a data source to monitor and analyze up to one year of network traffic and report flow traffic on the network. RA identifies the source of network bandwidth hogging by pinpointing the application or host that consumed the most bandwidth during a specified timeframe.

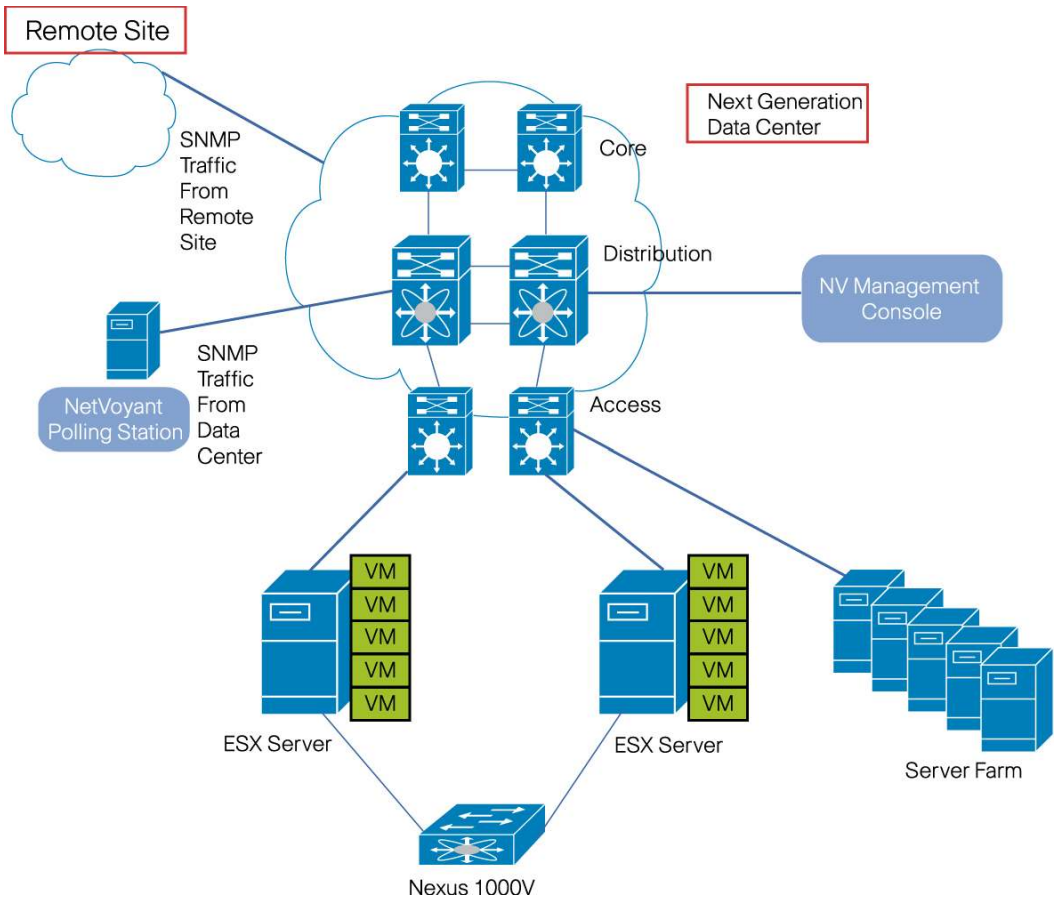
Figure 10. Reporter Analyzer Architecture



4.2.1.3 NetQoS NetVoyant

Figure 11 shows the the NetVoyant (NV) solution. NV uses SNMP polling to manage network devices. NV comes with numerous MIBs precompiled, but any new platform can be supported by adding platform-specific MIBs. NV provides information about packet loss, latency, jitter statistics, device status, and utilization.

Figure 11. NetVoyant Architecture



4.2.1.4 NetQoS Performance Center

NetQoS Performance Center (NPC) is NetQoS's unified web-based console that integrates reports from SA, RA, and NV in a unified view. The NPC server is used as a data source for northbound integration from NetQoS into Cisco Info Center, then from Cisco Info Center to the dashboard.

4.2.2 Demonstration Cases

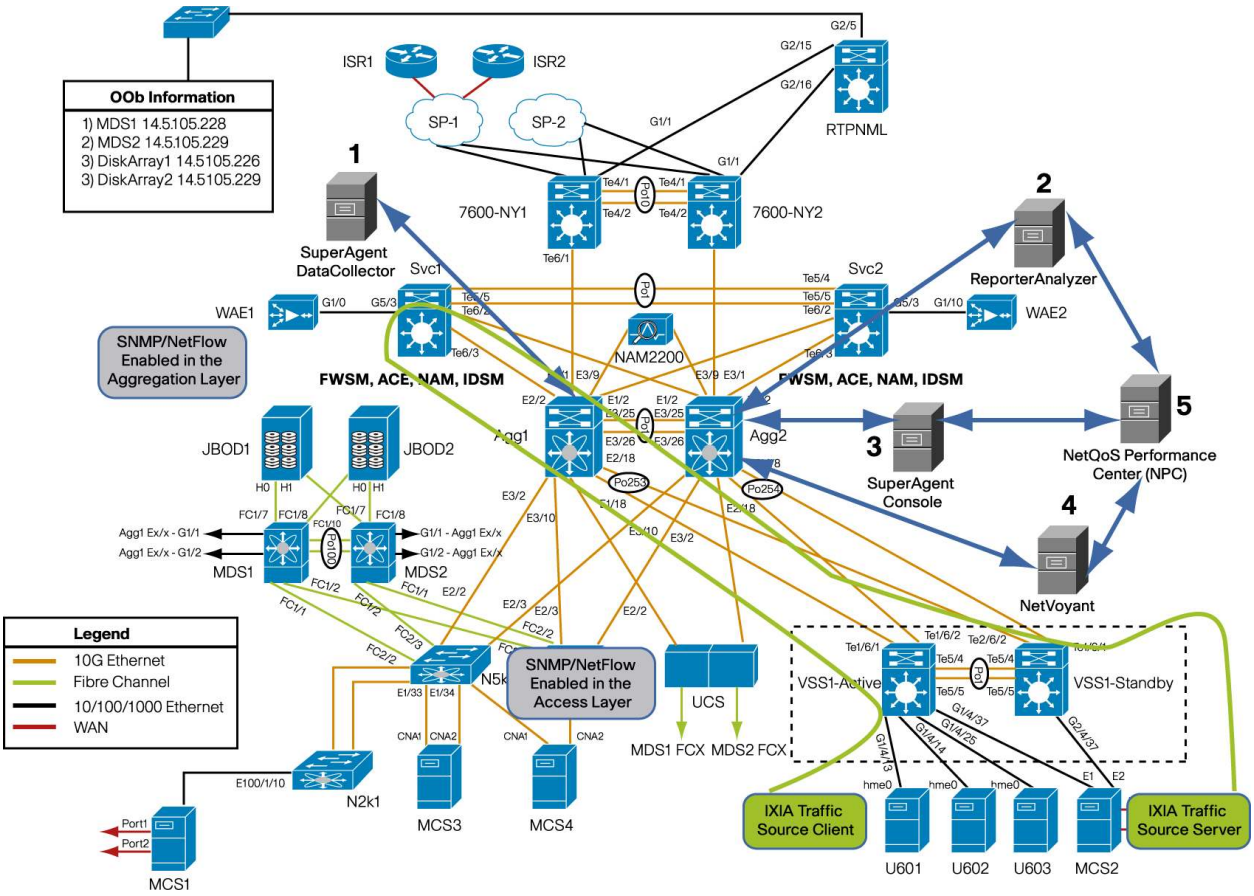
This section details selected cases executed in the NGDC POC Lab. We demonstrate test results for three tests, one from each performance test category: SuperAgent for TCP performance measurement, ReporterAnalyzer for network traffic analysis, and NetVoyant for device management using SNMP polling.

The NetQoS architecture deployed in the lab is the standalone architecture where each appliance (RA and NV) has all components in one appliance. The SuperAgent component requires two appliances: one for data collection and one as a management console.

4.2.2.1 Network Topology

Figure 12 shows NetQoS appliances deployed in the NGDC POC Lab.

Figure 12. NetQoS POC Lab Architecture



Since the SuperAgent component requires end-to-end application packets, the data collector (#1 above) was deployed to SPAN application traffic in the aggregation layer (Agg1 and Agg2 Nexus 7000 Series switches).

NetFlow was enabled in the access and aggregation layers to be forwarded to the ReporterAnalyzer component, which then analyzes and generates network traffic reports.

SNMP polling was also enabled in the access and aggregation layers. The NV component polls and generates device utilization reports.

Each component (RA, SA, and NV: #2, #3, and #4 above) has its own reporting GUI, but all three GUIs can be rolled up to the unified management console—the NPC (#5 above).

The IXIA traffic generator was used to generate application traffic on the network. One port simulates an HTTP client and one port simulates the HTTP server. The green line in the diagram depicts the traffic path. The IXIA client port generated HTTP traffic on the access layer (Cisco Catalyst 6500 Series VSS). HTTP traffic traversed to the aggregation layer (Nexus 7000 Series), and then to the switches (Cisco 7600 Series) where service modules (FWSM and ACE) resided. Once allowed by the service layer, this traffic traverses back to the IXIA server port, completing the round-trip.

4.2.2.2 Performance Test Cases

We have conducted many test cases in the NGDC POC Lab, but the following test cases represent the most salient tests. These tests are conducted using all three NetQoS performance tools, with the devices shown in network diagram Figure 1.

Test 1: Measure network round-trip time.

Test 2: Verify that the RA can receive and process NetFlow data from the Nexus 7000 Series switch.

Test 3: Verify that NV can perform management on the Catalyst 6500 VSS switch.

Test 4: Verify that the RA can receive and process NetFlow data from the Nexus 1000V Series switch.

The test results from these four test cases are shown below with screen shots captured during the tests.

4.2.2.2.1 Network Round-Trip Time

This test verified that the SuperAgent appliance can monitor and measure TCP performance indicators from the NGDC infrastructure as shown in Figure 13 by providing network round-trip time between an HTTP client and an HTTP server.

Table 3. Test Case #1: Network Round-Trip Time

Description	Measure network round-trip time
Requirements	Configure NetQoS to monitor traffic between client and application server
Procedures	• Generate traffic using a traffic generator (IXIA) • Configure SA for to report network round-trip time relative metric

Figure 13. Network Round-Trip Time

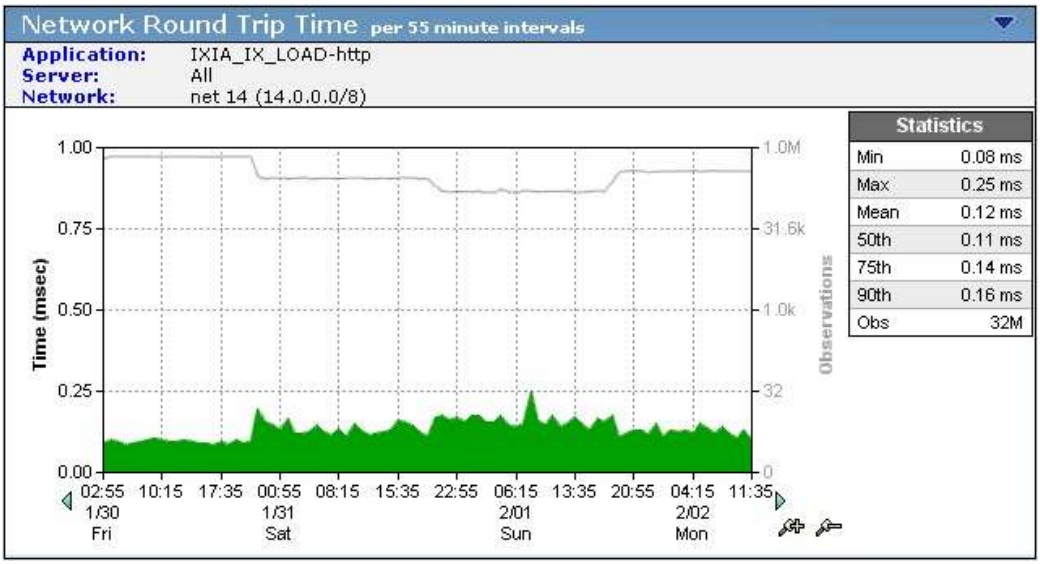


Figure 13 shows:

- An average network round-trip time of 0.12 ms (mean) for the duration of this measurement from Friday 1/30/2009 through Monday 2/2/2009.
- The maximum round-trip time of 0.25 ms occurred on Sunday 2/1/2009.
- There were 32 million “observations”—data points collected and analyzed throughout this timeframe.

4.2.2.2.2 Top talkers in the network

This test verified that the ReporterAnalyzer appliance can receive and process exported NetFlow from the Nexus 7000 device by providing top TCP conversation talkers.

Table 4. Test Case #2: Top Talkers

Description	Verify that the RA can filter and display top talkers in the network
Requirements	NetFlow traffic exported to the RA appliance
Procedures	• Configure the Nexus 7000 Series switch to export NetFlow traffic to the RA • Configure the NetQoS RA to collect, analyze, and report top talkers on the network

Figure 14. Top Talkers

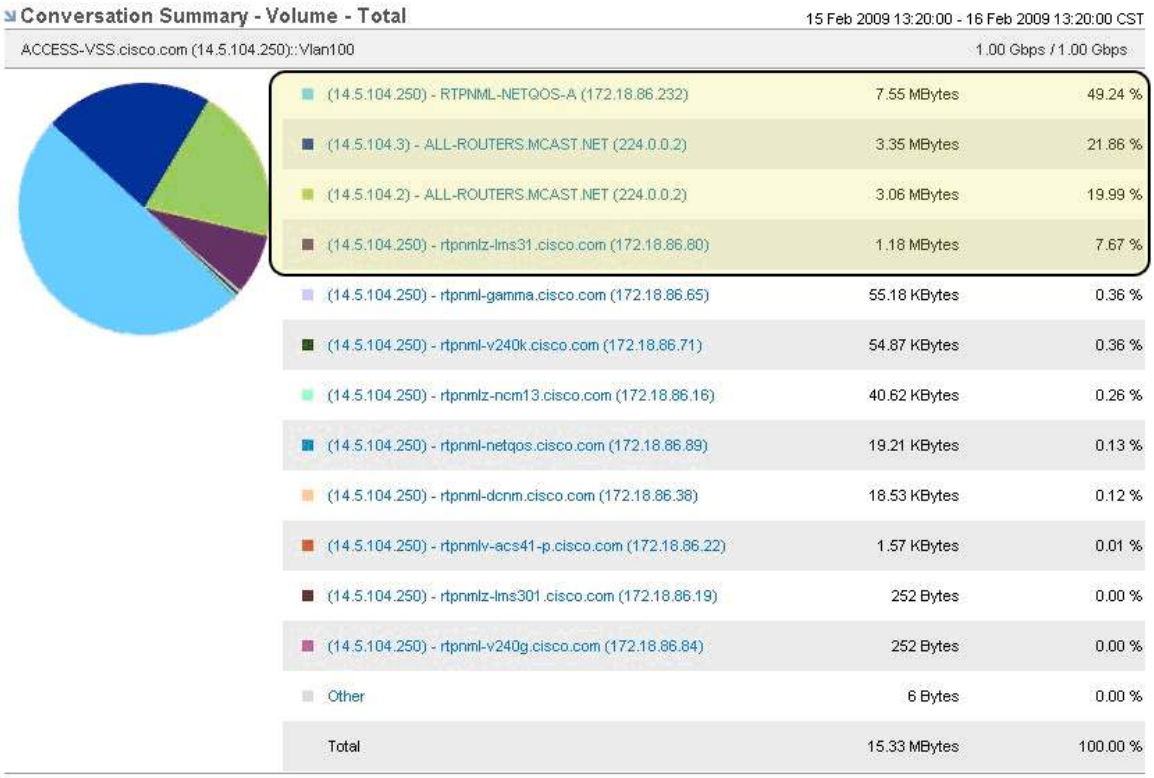
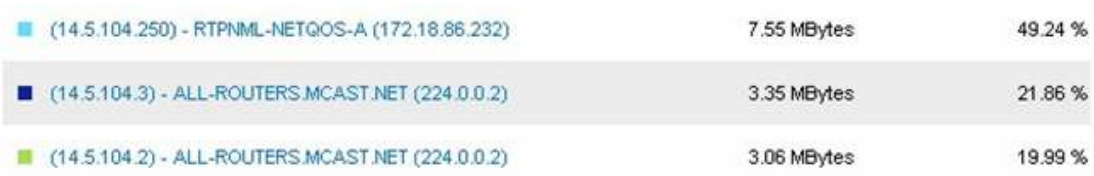


Figure 15. Top Three TCP Conversations Highlighted



These three TCP conversations collectively contributed 91.09% (49.24 + 21.86 + 19.99) of total traffic volume during the analysis period.

4.2.2.2.3 Cisco Catalyst 6500 Series VSS: Link-Related Counter

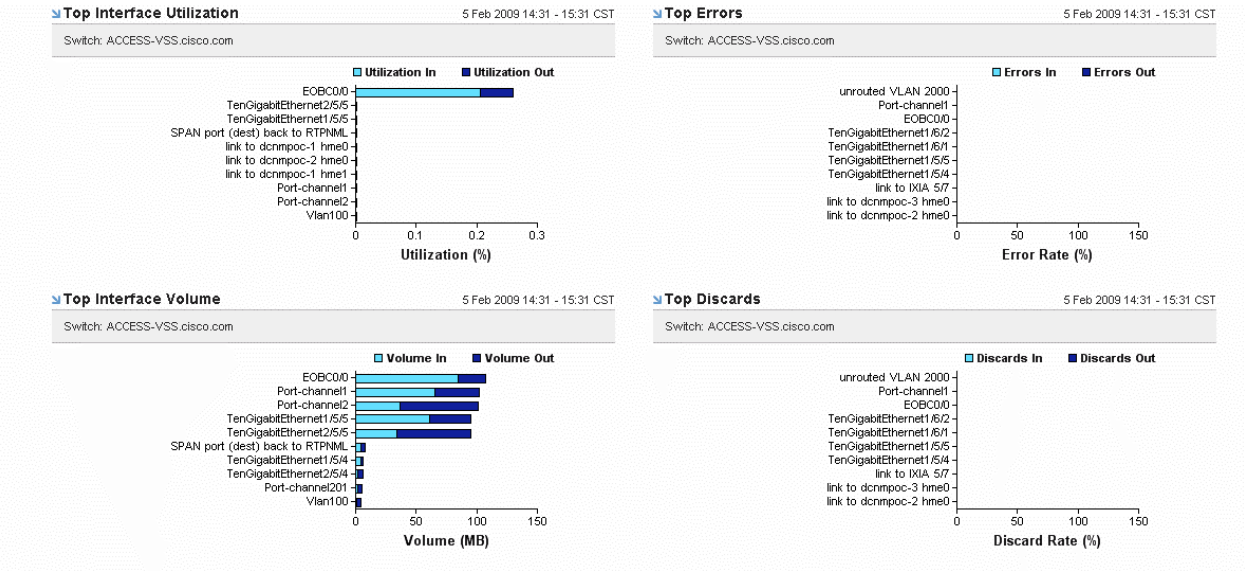
This test verified that the NetVoyant appliance can monitor the Cisco Catalyst 6500 Series VSS device via SNMP by reporting interface utilization percent, interface volume, error, and discards.

Table 5. Test Case #3: Interface MIB

Description	SNMP Poll the CISCO-IF-MIB ifTable
Requirements	• NetQoS NetVoyant • CAT 6500 VSS
Procedures	• Configure SNMP Community strings on Catalyst 6500 Series VSS device • Configure NetQoS NetVoyant to poll the ifTable OID from the IF-MIB

Figure 16 shows that while the port channel and the 10 Gigabit interfaces had traffic passing through, there were no errors or discards.

Figure 16. Top Utilization, Error, Discards

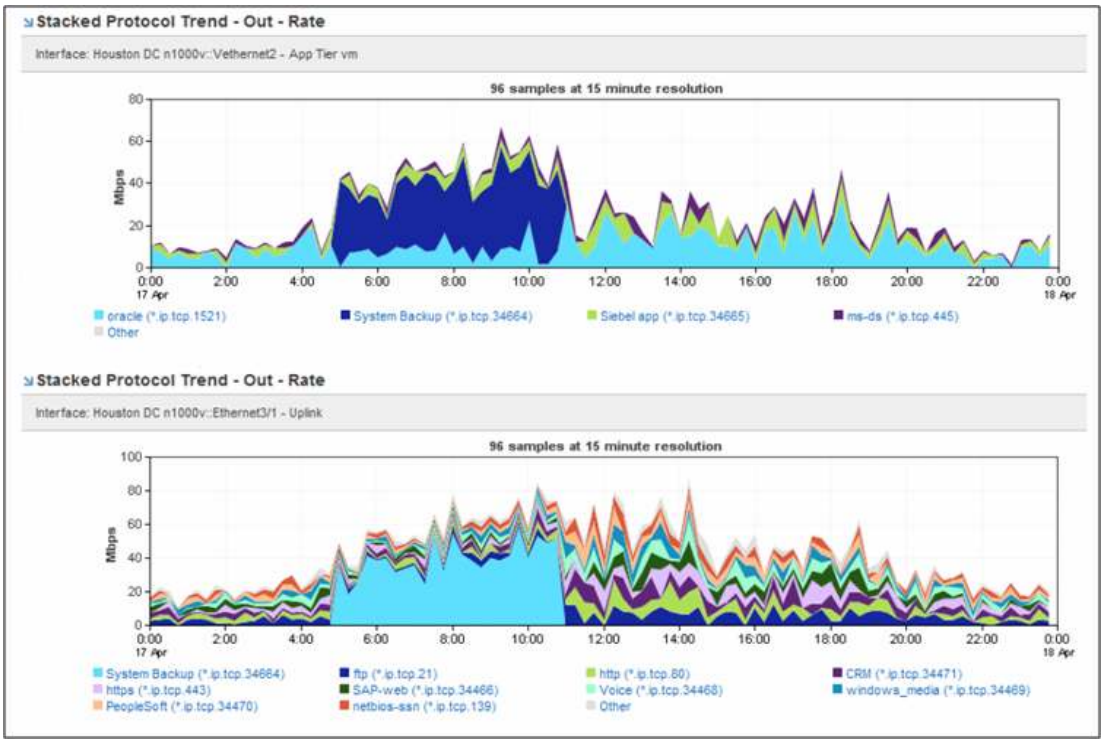


4.2.2.2.4 Nexus 1000V: Top Protocols

The following test result validates the RA's capabilities on the Nexus 1000V Series switch.

Figure 17 shows the outbound network traffic pattern for the Vethernet1 and Vethernet3/1 virtual interfaces. Note the dark blue color on the topmost graph, for the Vethernet2 interface—this represents "system backup" traffic for the VM.

Figure 17. Top Protocols for the Nexus 1000V Series Switch



Summary

To develop unified assurance management (fault management and performance management) for the infrastructure that is comprised of network, compute, and storage applications, we have worked with various ISVs and developed the interfaces to Nexus switches, MDS storage devices, and the Cisco Unified Computing System (UCS).

Several real-world test cases were developed for fault and performance applications, and we have run these test cases in the Next Generation Data Center (NGDC) Lab. The results for fault and performance management are documented. In addition, we have consolidated all fault management alarms on a single pane of glass, which should provide operational value for the NOC operators and eliminate any operational silos.

Cisco Advanced Services provides the consulting services to design, build, and integrate a management platform for virtualized data center operations. By learning how to manage this technology and by partnering with Cisco Advanced Services, customers can reduce the risk associated with managing complex virtualized data centers, and reduce the time and costs associated with deployment of the data center management system.

Acronyms

Table 6. Acronyms

Acronyms	Definition
ANM	Application Networking Manager
CIC	Cisco Info Center
DCNM	Data Center Network Management
FMS	Fabric Management System
ITIL	IT Infrastructure Library
MIB	Management Information Base
NV	NetVoyant (NetQoS Module)
NGDC	Next-Generation Data Center
OSS	Operations Support System
POC	Proof Of Concept
RA	Route Analystics (NetQoS Module)
SA	SuperAgent (NetQoS) Module
SLA	Service-Level Agreements
SNMP	Simple Network Management Protocol
TMF	TeleManagement Forum
TMN	Telecommunications Management Network
VDC	Virtual Data Center (also Virtual Device Context)
VSS	Virtual Switching System
UCS	Unified Computing System

References

1. DCNM
   http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_2/dcnm/release/notes/dcnm_4_2_relnotes.html
2. Fabric Manager
   https://www.cisco.com/en/US/docs/switches/datacenter/mds9000/sw/4_1/release/notes/17675_06fm.html
3. ANM
   http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/application_networking_manager/2.2/user/guide/UG_ports.html
4. UCS Manager
   http://www.cisco.com/en/US/docs/unified_computing/ucs/release/notes/ucs_relnotes_1_0_2.html
5. Cisco Info Center
   http://www.cisco.com/en/US/products/sw/netmgtsw/ps996/products_documentation_roadmap09186a0080805796.html
6. NetQoS
   https://www.cisco.com/en/US/prod/collateral/contnetw/ps5680/ps6870/prod_white_paper0900aecd80693006.html

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 www.cisco.com/go/offices.

Printed in USA C11-575044-00 03/10