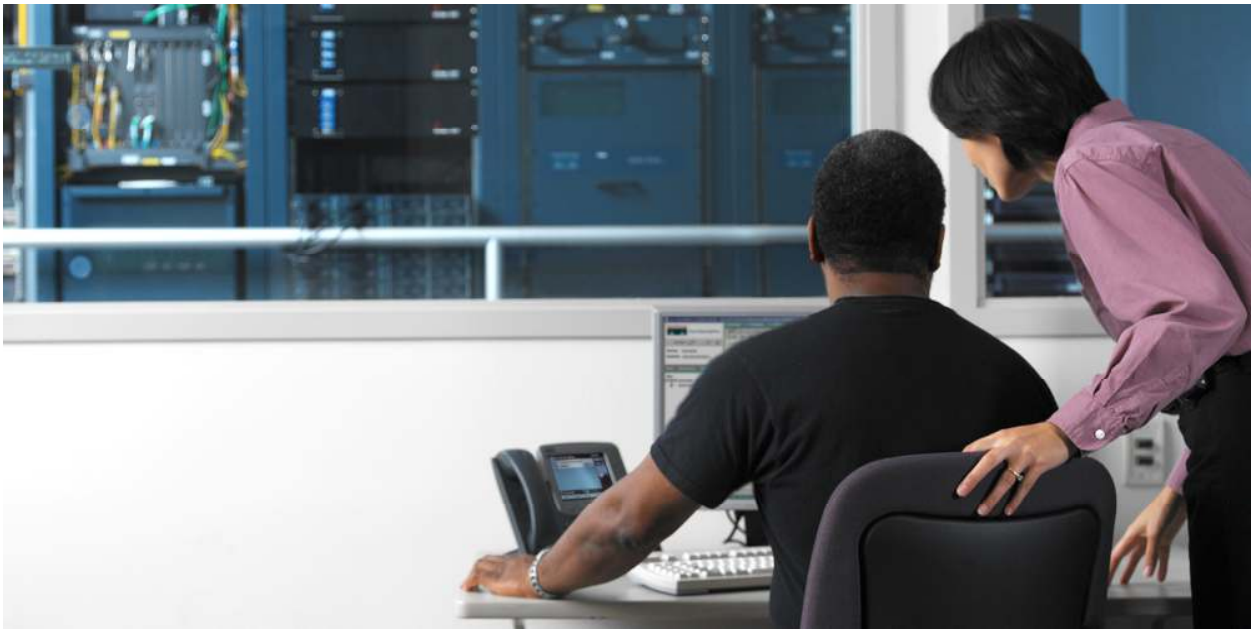
Cisco Fabric Manager 5.0: Visibility and Control for the Unified Data Center



Product Overview

Cisco® Fabric Manager is the management tool for storage networking across all Cisco SAN and unified fabrics.

Cisco Fabric Manager provides comprehensive visibility for improved management and control of Cisco storage networks (2-, 4-, and 8-Gbps Fibre Channel and Fibre Channel over Ethernet [FCoE]). Cisco Fabric Manager helps reduce overall total cost of ownership (TCO) and complexity through unified discovery of all Cisco Data Center 3.0 devices and through task automation and detailed reporting.

The Cisco Data Center 3.0 strategy helps increase IT efficiency, responsiveness, and resilience by optimizing existing data center network assets for mission-critical workloads, and also by laying the foundation for the next-generation data center to more efficiently meet the demands placed on IT for greater collaboration, quicker access to applications and information, and compliance with ever-stricter regulatory requirements.

Visibility and control in the Cisco storage network enables service providers and IT departments to optimize for the quality-of-service (QoS) levels required to meet service-level agreements (SLAs) for internal and external customers.

Cisco Fabric Manager provides centralized Cisco MDS 9000 Family and Cisco Nexus® Family storage network management services, performance monitoring, federated reporting, troubleshooting tools, discovery, and configuration automation for today's and tomorrow's data center.

Features and Benefits

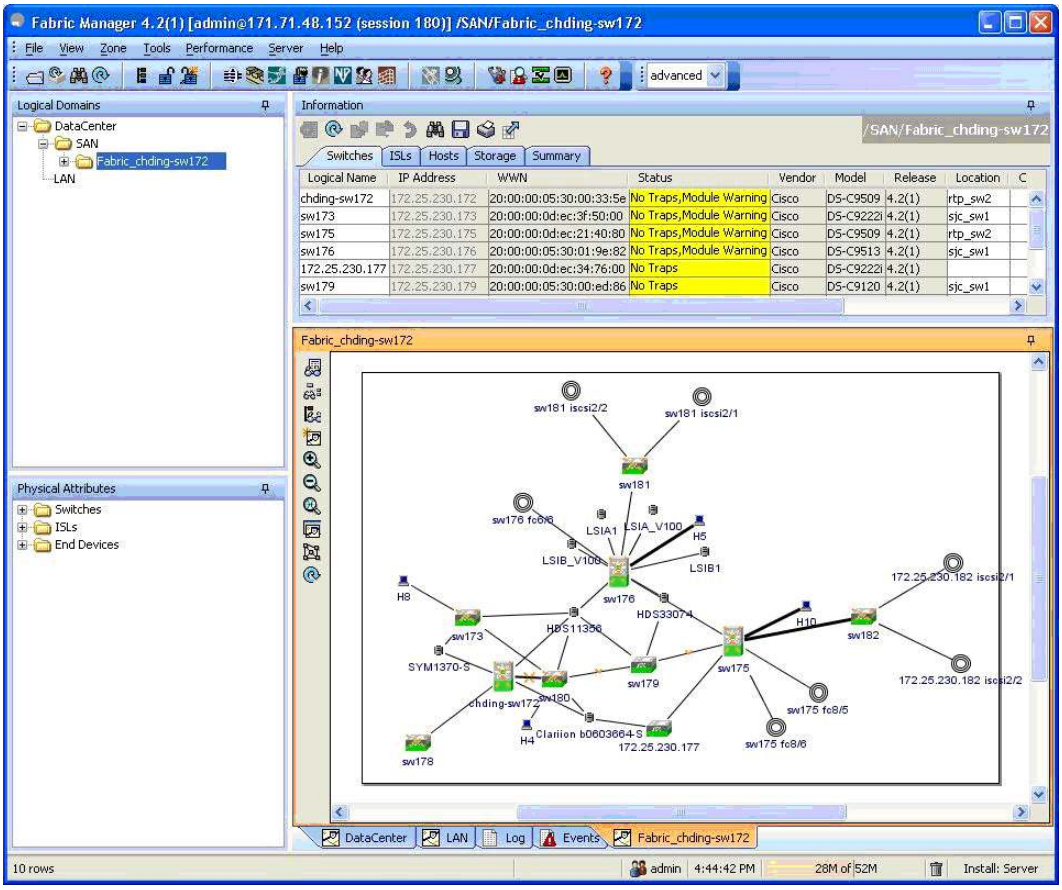
Table 1 summarizes the main features and benefits of Cisco Fabric Manager.

Table 1. Main Cisco Fabric Manager Features

Feature	Description	Benefits
Federation	• Federation of up to 10 Cisco Fabric Manager servers to manage and report on a large number of fabrics using a single management pane	• Scalability and improved response time for discovery and reporting tasks
Discovery	• Cisco Discovery Protocol, Fibre Channel Generic Services (FC-GS), Fabric Shortest Path First (FSPF), and Small Computer System Interface 3 (SCSI-3) for discovery of devices and interconnects on one or more fabrics	• Discovery and topology map for all Cisco Data Center 3.0 devices (Cisco MDS 9000 Family, Cisco Nexus Family, and Cisco Catalyst® Family) and interconnects (Ethernet, Fibre Channel, and FCoE) • Discovery of Cisco LAN attributes • Limits on the scope of discovery by VSAN for large fabrics
Automation	• Configuration checking, helping simplify resolution of problems, perform successful fabric merges, and resolve configuration inconsistencies automatically • Multiple-switch feature configuration across all managed devices in a selected domain • Wizards for zone configuration, inter-VSAN routing (IVR), PortChannels, Fibre Channel over IP (FCIP) tunnels, and IP access control lists (ACLs) • Cisco MDS 9000 Configuration Analysis Tool	• Reduced human errors through automation • Simplification and automation of routine tasks • Consistency maintained among multiple fabrics • Reduced time spent managing storage networks • Detailed switch configuration management (compare switch configurations, schedule periodic backups of running switch configuration, and analyze and identify configuration differences)
Reporting and analysis	• Real-time statistics and historical performance monitoring and reporting • Visibility into the entire Cisco storage network through Cisco Fabric Manager server federation	• Visibility into performance, utilization, topology, and configuration details for more efficient planning and provisioning

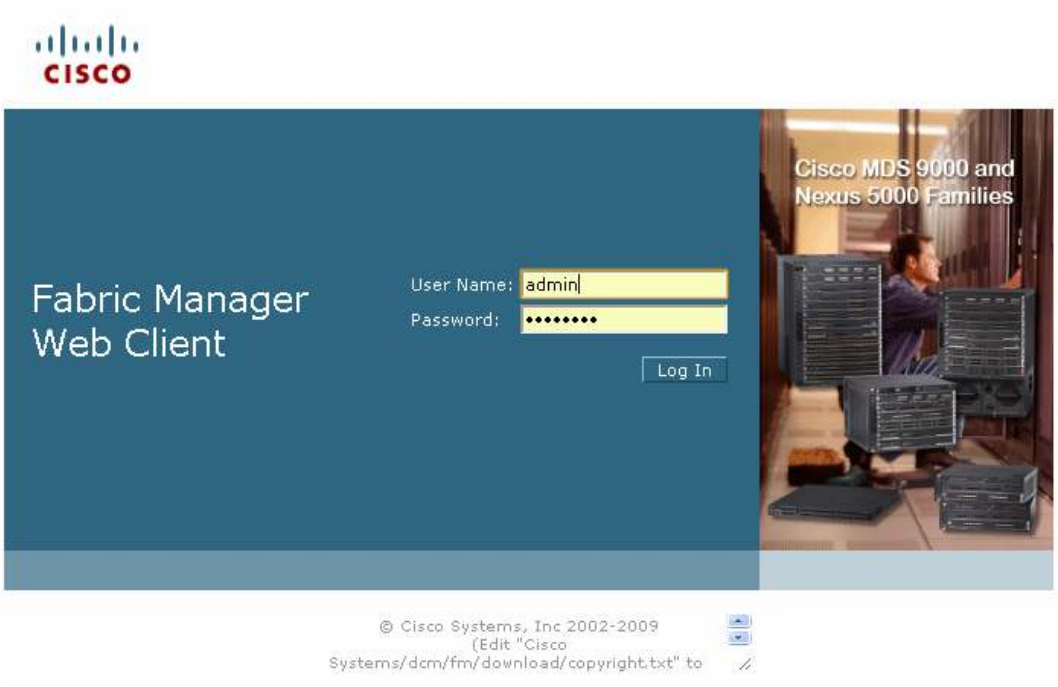
The Cisco Fabric Manager Client can be used by data center administrators for fabricwide provisioning and to represent the storage network topology map (Figure 1).

Figure 1. Cisco Fabric Manager Client



The Cisco Fabric Manager Web Client can be used for fabricwide federated reporting and Cisco Storage Media Encryption (SME) configuration (Figure 2).

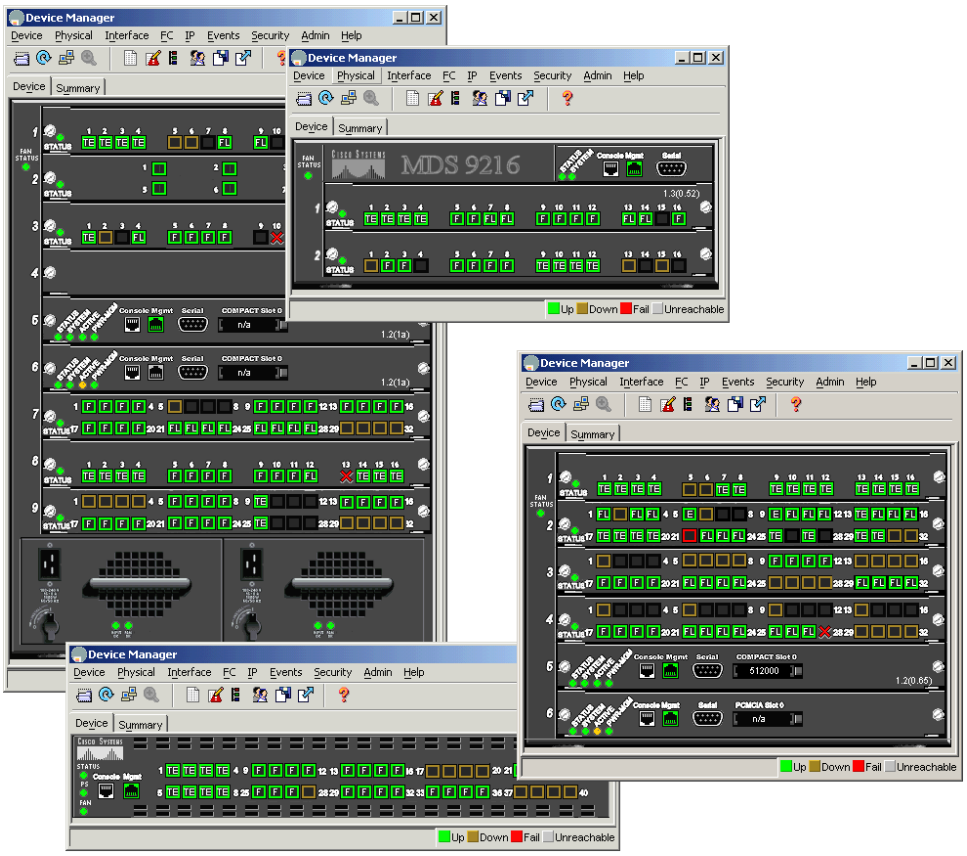
Figure 2. Cisco Fabric Manager Web Client



Storage Network Device Manager

Cisco Device Manager can be used for detailed switch provisioning and provides a graphical representation of each Cisco MDS 9000 Family switch chassis or Cisco Nexus 5000 Series Switch chassis, including the installed switching modules, the supervisor modules, the status of each port within each module, the power supplies, and the fan assemblies (Figure 3).

Figure 3. Cisco Device Manager



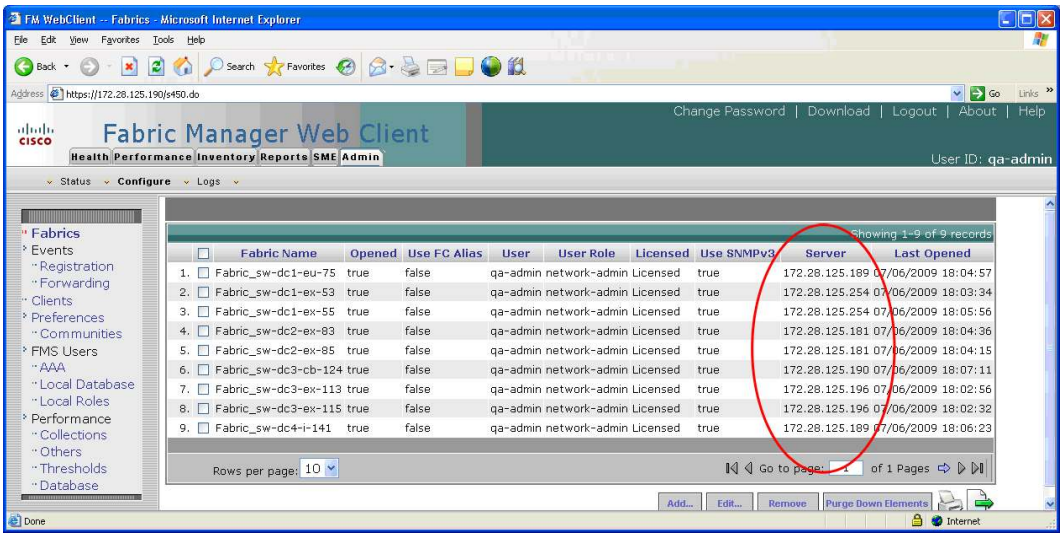
Use the Device view to perform switch-level configuration, including the following:

- Configuring physical Fibre Channel interfaces
- Configuring virtual Fibre Channel interfaces
- Configuring FCoE features
- Configuring zones for multiple VSANs
- Managing ports, PortChannels, trunking, and oversubscription
- Managing Simple Network Management Protocol Version 3 (SNMPv3) security access to switches
- Managing command-line interface (CLI) security access to the switch
- Managing alarms, events, and notifications
- Saving and copying configuration files and software image
- Viewing hardware configuration
- Viewing chassis, module, port status, and statistics

Storage Network Management Scalability

A group of two or more Cisco Fabric Manager servers can work together in a federation to provide a higher level of scalability, availability, and reliability for automated data center fabric management tasks. Federation distributes data center fabric management responsibility among the Cisco Fabric Manager servers (Figure 4).

Figure 4. Manage All Fabrics Discovered in the Federation



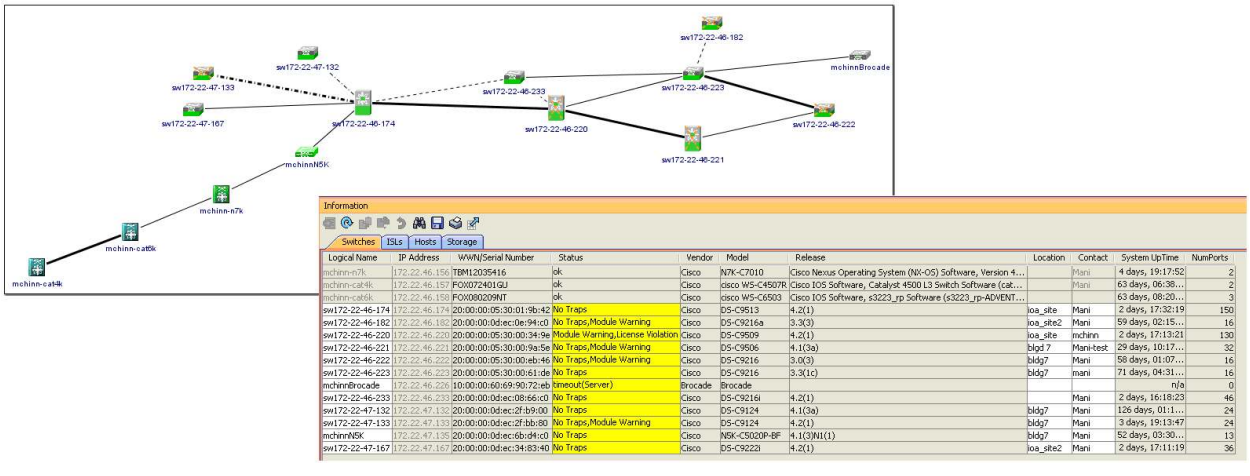
Federation uses a central database to persist data and share common information among all servers, with each physical server mapped as a logical entity in the federation. With the capability to move fabrics across the federation, the storage administrator can load-balance Cisco Fabric Manager server workloads and increase overall storage network management scalability, availability, and reliability.

Federation of Cisco Fabric Manager servers allows comprehensive reporting across all fabrics distributed among the servers in the federation.

Storage Network Discovery and Topology Mapping

Cisco Fabric Manager Web Client displays and maps real-time views of Cisco storage networks (Fibre Channel and FCoE), including Cisco Nexus 5000 Series Switches and Cisco MDS 9000 Family switches as well as third-party network switches, hosts, and storage arrays (Figure 5).

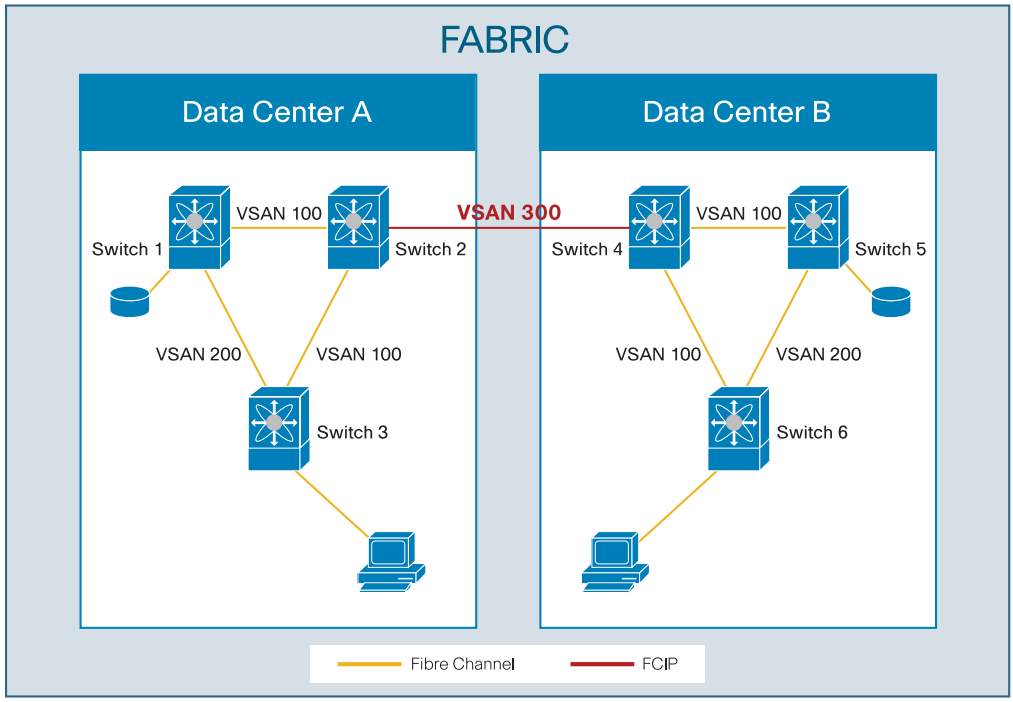
Figure 5. Discovery of Cisco Storage Networks for Reporting and Analysis



The Cisco Discovery Protocol is a device discovery protocol that runs on the Cisco MDS 9000 Family, Cisco Nexus Family, and Cisco Catalyst Family products. In addition to Cisco Discovery Protocol, Cisco Fabric Manager uses standards-based discovery protocols, including FC-GS, FSPF, and SCSI-3, for discovery of devices and interconnects on one or more fabrics.

For large enterprises, a SAN fabric can span multiple geographical regions consisting of hundreds of VSANs and switches, and thousands of ports. VSAN scoping allows data center administrators to discover switch ports and end devices attached to VSANs specific to a geographic region. VSAN scoped discovery limits which VSAN within a fabric can be discovered and viewed (Figure 6).

Figure 6. VSAN Scoped Discovery and View of Fabric

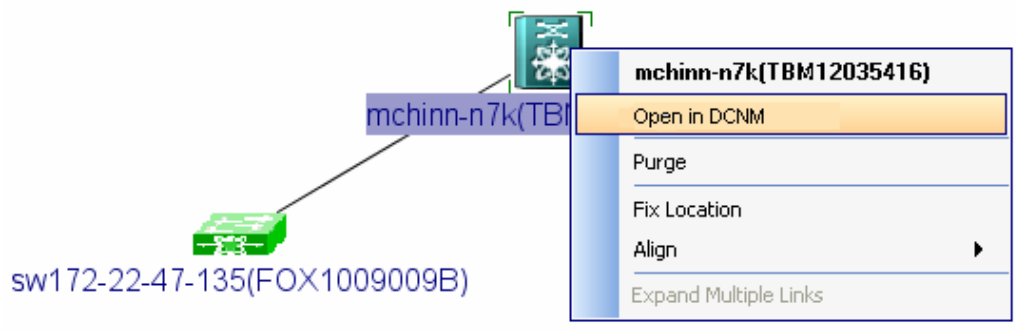


Data Center Integration

Cisco's end-to-end data center vision enables data center administrators to fully integrate Cisco management tools across the Cisco MDS 9000 Family, Cisco Nexus Family, and Cisco Unified Computing System™ to provide cohesive end-to-end visibility and configuration capabilities. Integrating Cisco Fabric Manager for the Cisco MDS 9000 Family, Cisco Data Center Network Manager (DCNM) for the Cisco Nexus 7000 Series Switches, and Cisco UCS Manager for the Cisco Unified Computing System significantly simplifies provisioning and monitoring operations in Cisco next-generation data centers. Data Center administrators can extend their management scope from the SAN to incorporate LANs relevant to storage networking paths over Ethernet networks.

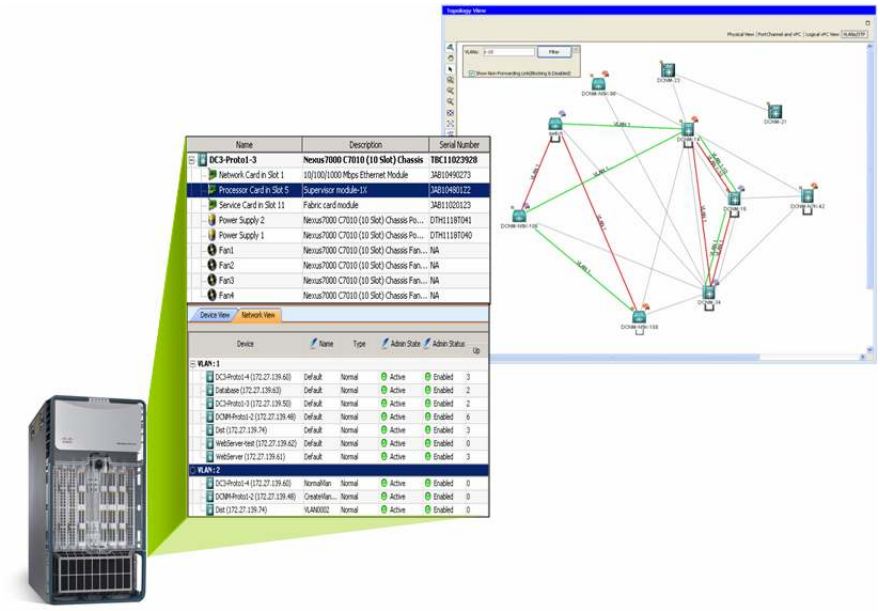
Cisco Fabric Manager and DCNM clients can be launched from the respective switch icon in Cisco Fabric Manager or DCNM topology maps. For example, in Cisco Fabric Manager, the Cisco Nexus Family switch icon allows users to launch Cisco DCNM by double-clicking or by choosing Open in DCNM from the context menu (Figure 7).

Figure 7. Select the Cisco Nexus 7000 Series Switch to Launch Cisco DCNM Client



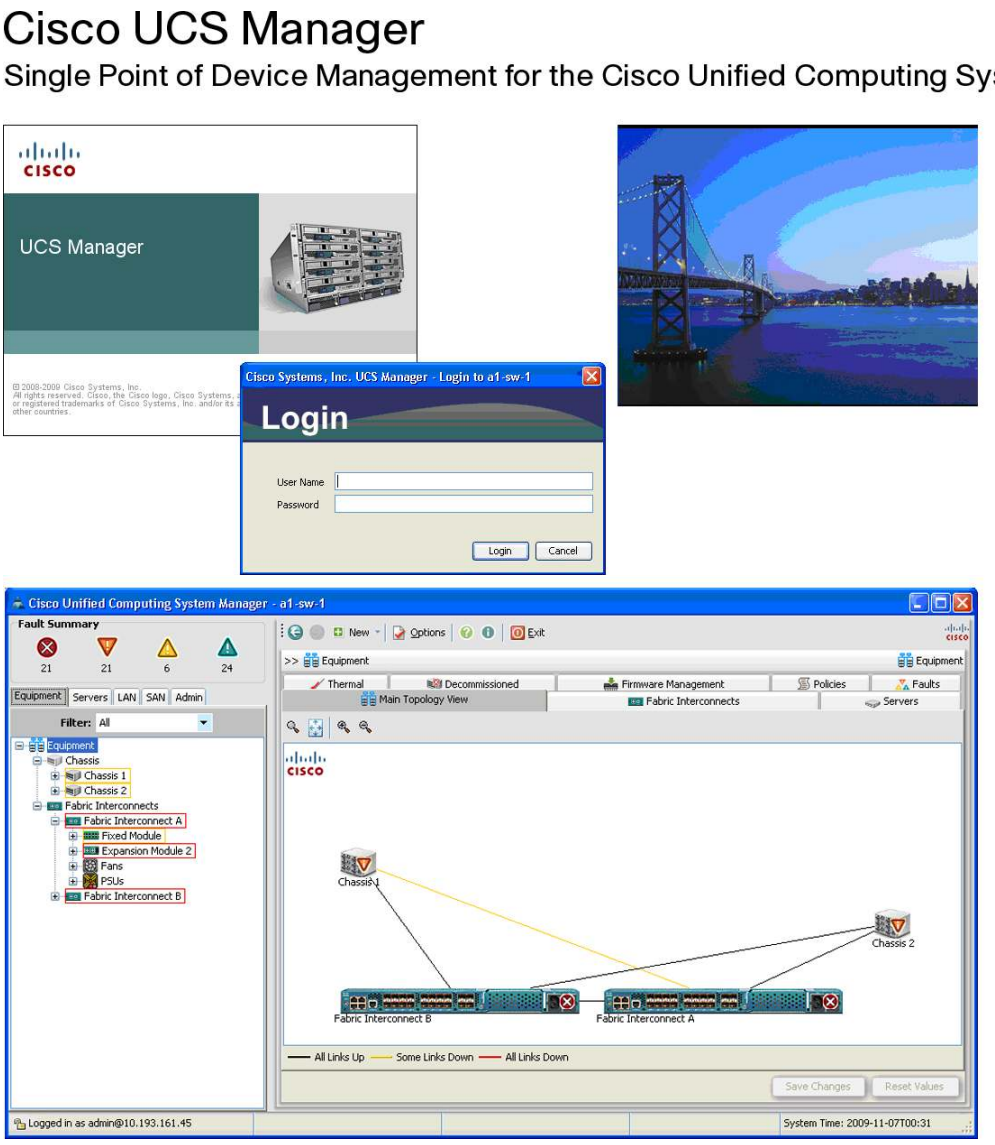
Cisco DCNM is a multiprotocol-aware, data center–class, comprehensive administration solution for the Cisco Nexus 7000 Series dedicated to network operations for Ethernet, IP, and network security management (Figure 8).

Figure 8. Cisco DCNM Interface for Cisco Nexus 7000 Series



Cisco UCS Manager provides centralized management capabilities, creates a unified management domain, and serves as the central nervous system of the Cisco Unified Computing System (Figure 9). Cisco UCS Manager is embedded device-management software that manages the system from end to end as a single logical entity through an intuitive GUI, a CLI, or an XML API. Cisco UCS Manager implements role- and policy-based management using service profiles and templates. Autodiscovery allows Cisco UCS Manager to detect, inventory, manage, and provision any system component that is added or changed. When present in the data center, and when Cisco UCS Manager is installed, Cisco UCS Manager can be launched in context from the Cisco Fabric Manager topology map.

Figure 9. Cisco UCS Manager Interface



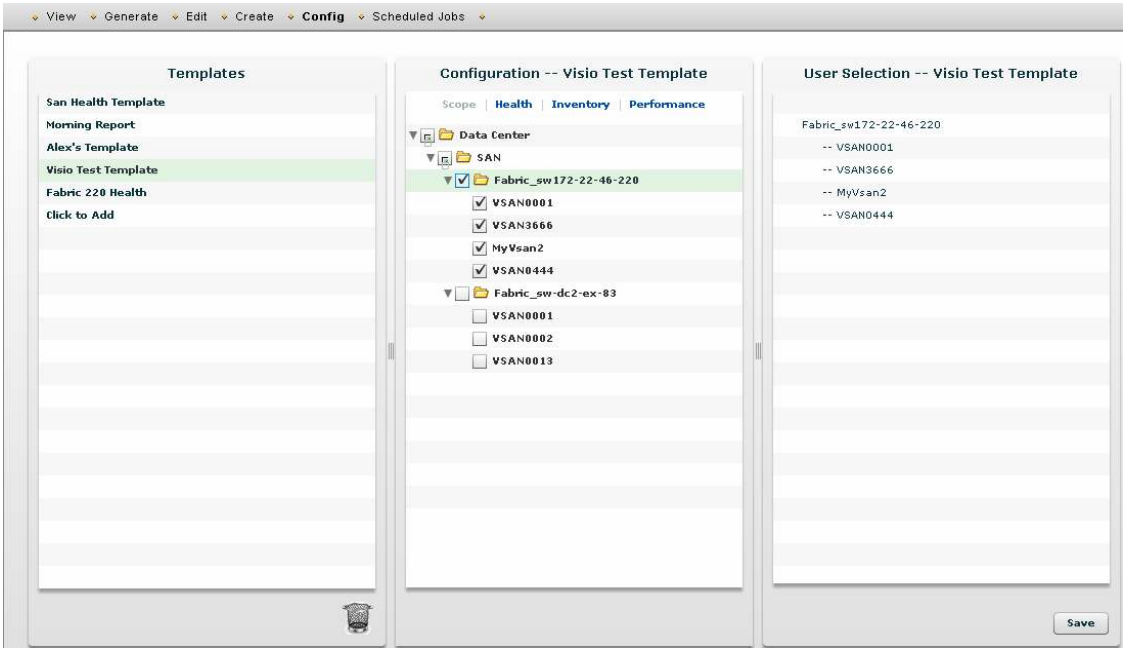
Storage Network Reporting

To help design for network resource optimization, Cisco Fabric Manager provides input for SLA planning, provisioning, and advanced reporting tools (Figure 10). Device-level visualization provides high-level and detailed views for:

- Overall fabric health (switch health status and monitoring, thresholds and event alerting, path connectivity status, zone discrepancies, etc.)
- Performance (utilization for devices, Inter-Switch Links (ISLs), end devices, flows, switch bandwidth, etc.)
- Inventory details (device count, port use, and licensing details)
- Zones, VSANs, N-port virtualization (NPV), F-port trunks, and flows
- Device-level details (switches, modules, and end devices)

A template configuration engine for custom report generation enables the creation, configuration, and deletion of default and custom report templates. Default SAN health and daily status reports can be customized to help data center administrators with day-to-day operational tasks and reporting requirements.

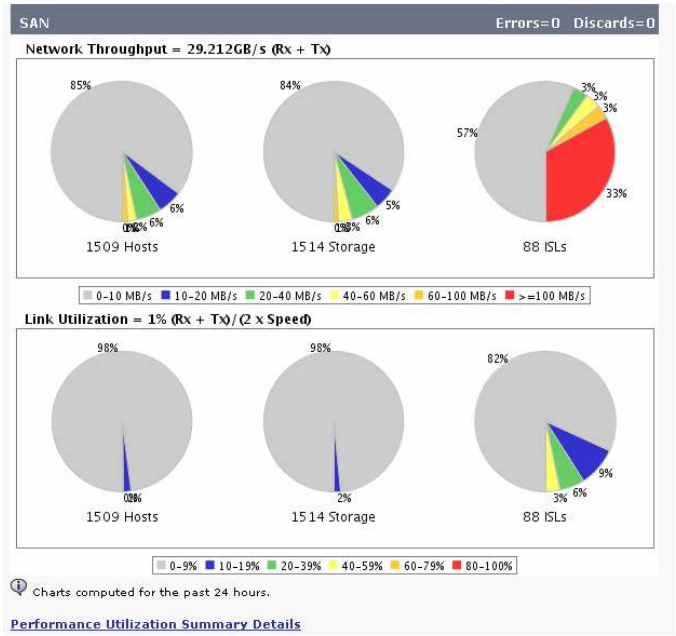
Figure 10. Customize Existing Report Templates



Cisco Fabric Manager and Device Manager enable comprehensive real-time and historical performance monitoring across all fabrics in the federation.

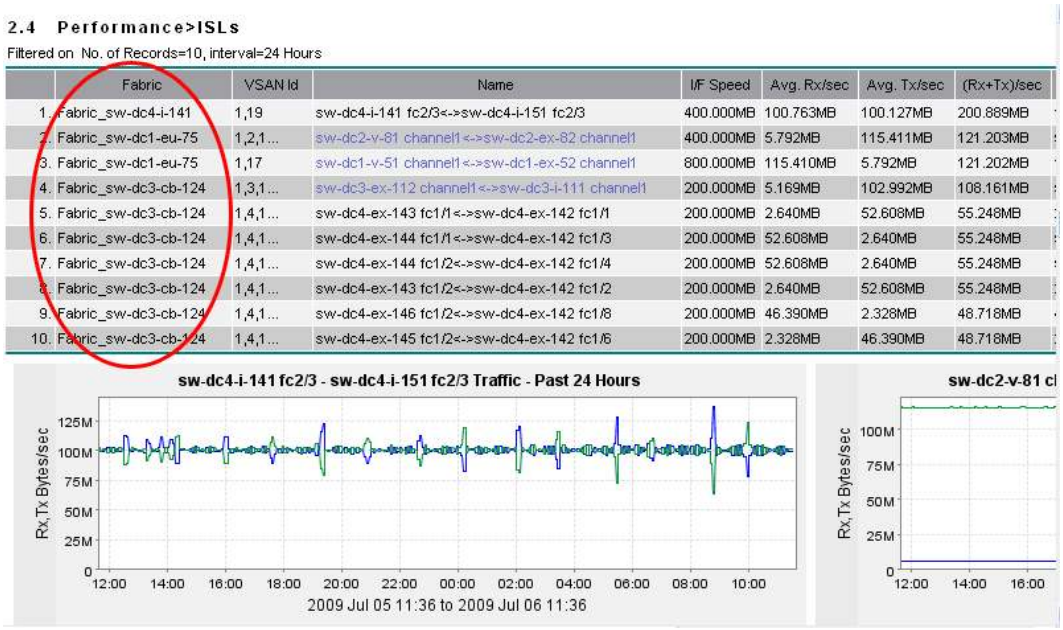
Cisco Performance Manager monitors performance and provides statistics for end devices (host and storage port traffic and errors), ISLs, NPV links, flows (host-to-storage traffic), and Ethernet (Ethernet and FCIP traffic); it provides average and peak throughput data and hot links for all Fibre Channel and Gigabit Ethernet interfaces and interconnections across the federation (Figure 11). Traffic Analyzer provides detailed Switched Port Analyzer (SPAN) port traffic statistics. Future link utilization and performance predictions can be configured from Cisco Fabric Manager Web Client.

Figure 11. Performance and Utilization Statistics



Using Cisco Performance Manager, storage administrators can step through the process of creating performance collections on fabric flows using configuration files, in which collections are defined for one or all VSANs in the fabric (Figure 12).

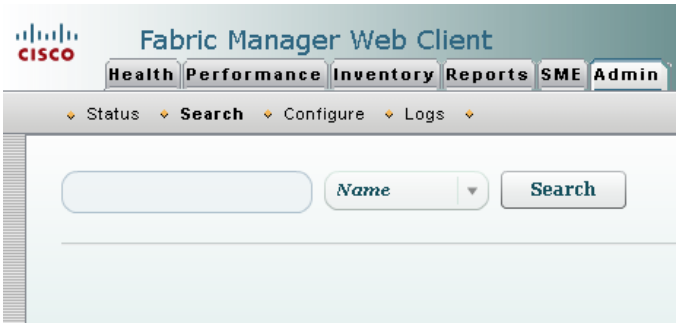
Figure 12. Generate Reports Across Fabrics Discovered on Different Cisco Fabric Manager Servers in a Federation



Search

Using the Cisco Fabric Manager search engine, specific management objects (entities) can be quickly accessed through a query for the entity's common name, IP address, world wide name (WWN), or alias (Figure 13).

Figure 13. Cisco Fabric Manager Search Tool Bar



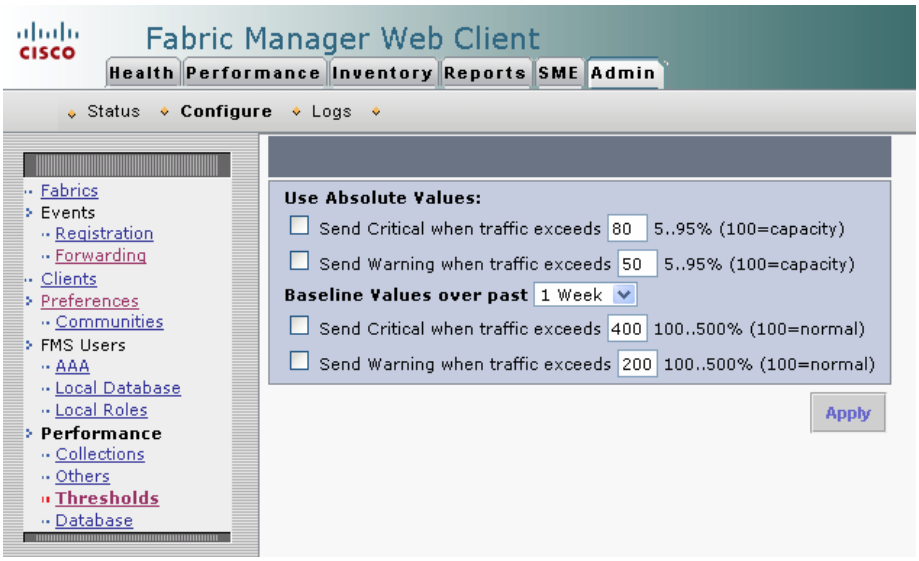
Flexible Monitoring and Alerts

Cisco Fabric Manager Web Client provides storage administrators with real-time and historical performance-monitoring statistics in tabular and graphical formats. Performance-monitoring thresholds and configuration of threshold-based alerts, including Call Home, facilitate rapid response to exception conditions.

Alert Thresholds and Event Forwarding

Use Cisco Fabric Manager Web Client to configure thresholds across multiple fabrics and forward threshold violation events through email or SNMP traps to third-party applications (Figure 14).

Figure 14. Set Thresholds and Baseline Values for Alerts and Warning Messages



Storage Network Administration Automation

Cisco Fabric Manager greatly reduces operating costs and complexities associated with mission-critical IT environments by offering powerful configuration automation capabilities for installing switches, tuning the fabric after it is operational, and setting up zones, ISLs, network security, and VSANs.

Cisco Fabric Manager includes automated tools that provide configuration analysis and parallel switch Cisco NX-OS Software upgrades (Figure 15). The Fabric Configuration Analysis tool allows administrators to compare, reference, and clone switch configurations (Figure 16). Multiple-switch feature configuration allows the storage administrator to automatically apply Cisco MDS 9000 Family configuration settings and policies across selected devices in the management domain.

Figure 15. Automate Parallel Cisco NX-OS Upgrades and Versioning

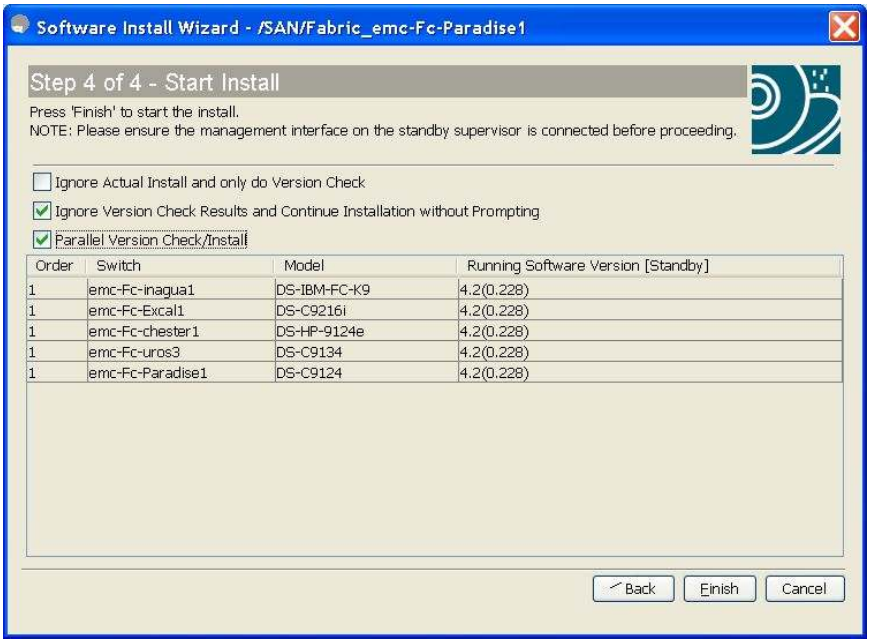
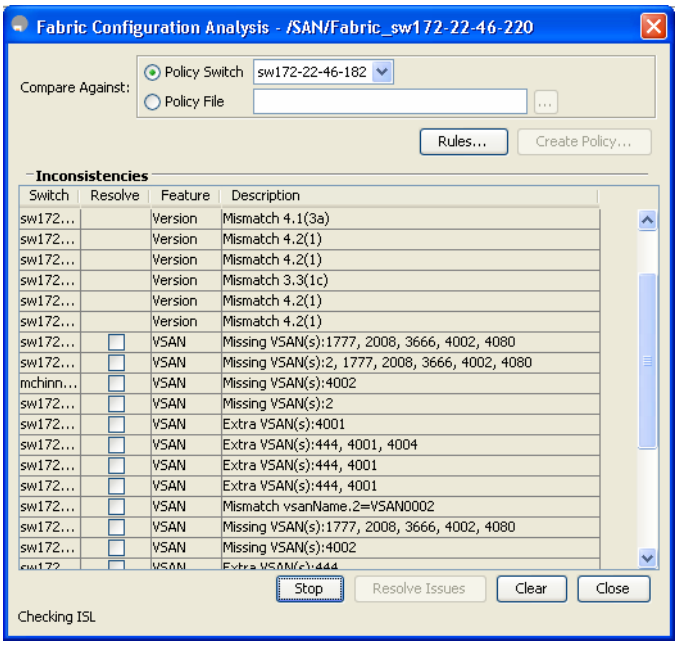
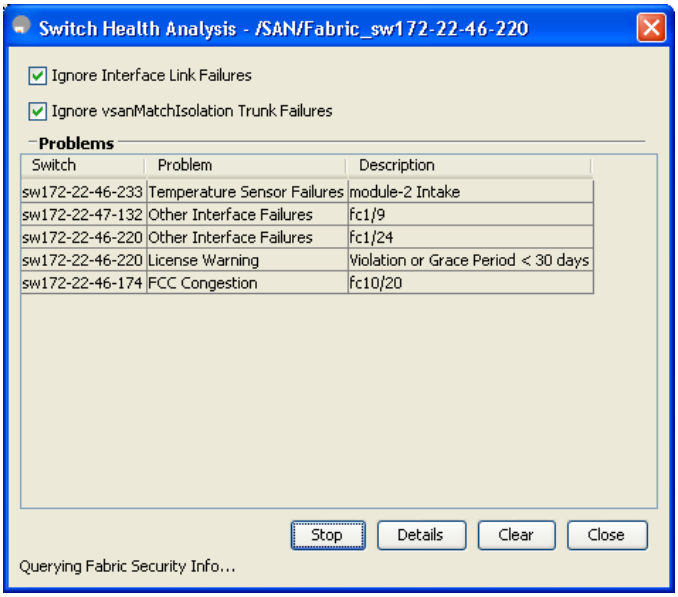


Figure 16. MDS Fabric Configuration Analysis Tool



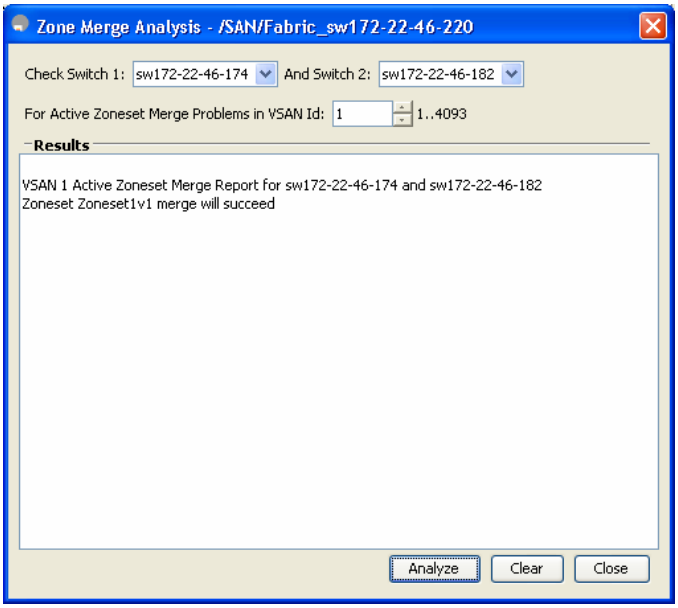
With the Cisco Fabric Manager intuitive GUI, data center administrators can compare switch configurations side by side, perform configuration policy checks across switches, set alarm thresholds to report to third-party fault-management applications, view individual device and aggregate statistics in real time, and analyze historical performance statistics. In addition, using the Cisco MDS Configuration Analysis Tool (Figure 17), data center administrators can schedule periodic backups of running switch configurations and analyze and identify configuration differences over a specified period of time and filter on the basis of the management object of interest (VSAN, zone, interface, IVR, etc.).

Figure 17. The Cisco Fabric Manager Switch Health Analysis Tool Allows the Storage Administrator to Scan for Operational and Configuration Problems as well as the Operational Heatlh of the Switch in the Fabric to Help Identify Physical and Logical Failures



The Cisco Fabric Manager Zone Merge Analysis Tool identifies specific configurations that would prevent a successful merge when fabrics are combined (Figure 18).

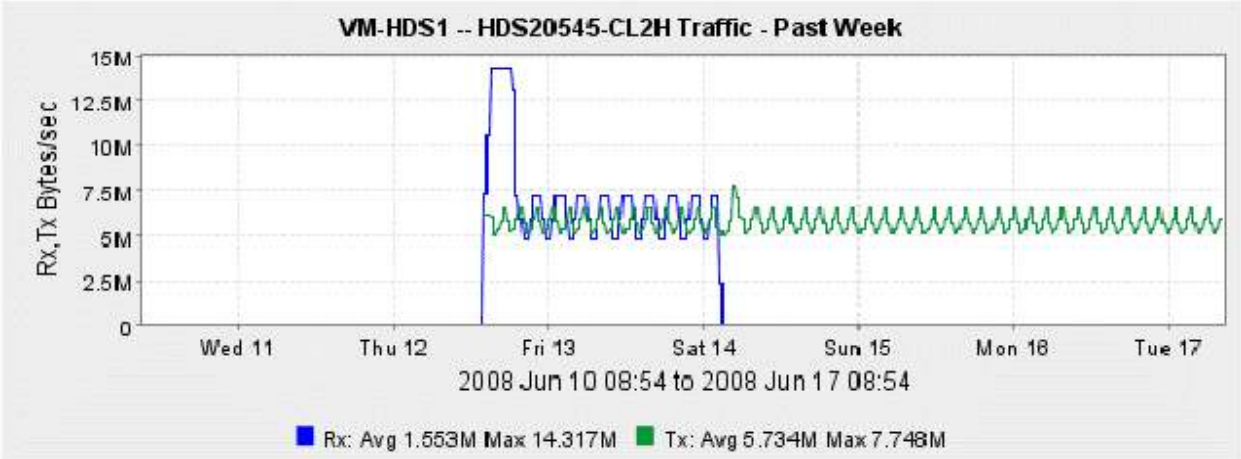
Figure 18. By Running the Zone Merge Analysis Tool Before Combining Fabrics, Problems with Active Zone Set Naming and Zone Membership Can Be Resolved Proactively



Control and Monitoring of Virtual Machines Using N-Port ID Virtualization

Cisco Fabric Manager supports the industry-standard N-port ID virtualization (NPIV) technology. NPIV assigns multiple Fibre Channel IDs (FCIDs) on the same physical F-port on the switch. Designed for virtual server environments, NPIV gives virtual servers a storage network identity (port WWN [pWWN]). In addition, NPIV support in Cisco Fabric Manager gives the storage network administrator virtual machine–level control through the zoning wizard, logical unit number (LUN) masking, and end-to-end traffic-flow QoS specification. These capabilities provide better utilization of server network connectivity and enable the administrator to monitor I/O performance using Cisco Performance Manager to provide flow statistics for each virtual machine (Figure 19).

Figure 19. The Same Capabilities Available for Monitoring the Performance of Physical Devices Are Available for Monitoring I/O Performance and Utilization of Individual NPIV-Enabled Virtual Machines



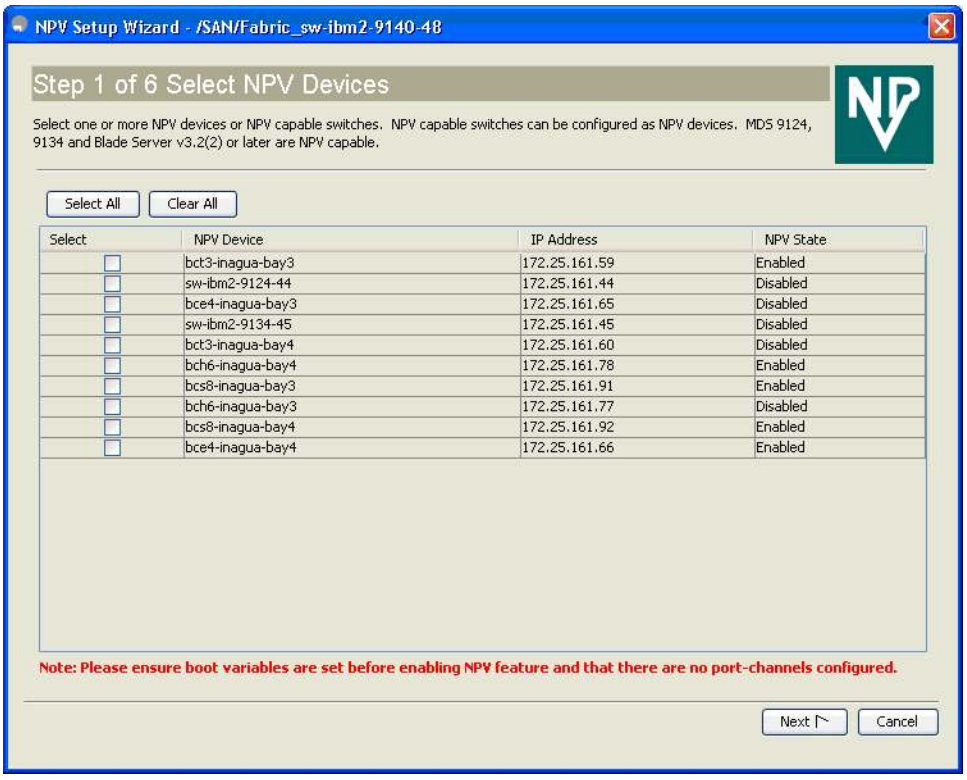
Server Consolidation Using Cisco N-Port Virtualizer

Server consolidation using blade and fabric switches increases the number of switches and hence the number domains in the network. It also increases the management associated with the increased number of Fibre Channel switches. NPV addresses both management and domain ID scalability concerns using standards-based NPIV technology. NPV converts a Fibre Channel blade switch to a host bus adapter (HBA), which does not use a Fibre Channel domain ID. The HBA gets FCIDs for attached devices from the SAN core switch to which it is connected.

When the Cisco blade switch is used in NPV mode, the SAN fabric does not see the blade switch as a switch but instead as an HBA aggregator. NPV relies on the core switch to run NPIV. The Cisco blade switch is VSAN aware. Traffic from all servers connected to a particular VSAN is uplinked to the core on N-ports that carry that VSAN. NPV offers significant configuration flexibility, with advanced traffic management capabilities.

The NPV Setup Wizard, which is part of Cisco Fabric Manager, simplifies large-scale blade deployments by guiding users through tasks (such as uplink selection, VSAN specification, and pairing of NPV switches with the correct SAN cores) that are required for batch deployment of a large number of blade switches (Figure 20). Cisco Fabric Manager also provides configuration and monitoring tools for building and managing large-scale storage networks.

Figure 20. NPV Setup Wizard



Storage Network Security

Cisco Fabric Manager provides comprehensive network security by protecting against unauthorized access and snooping through the use of the following security applications, protocols, and methods:

- FIPS activation and switch self-test
- Role- and profile-based authorization
- VSAN policies
- Cisco Secure Access Control Server (ACS) 3.1 and 4.0

- Cisco PIX® Firewall Software
- IP tables
- Fibre Channel Security Protocol (FC-SP) and Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP)
- Switch port security
- Fabric binding
- Certificate authority and digital certificate support through Public Key Infrastructure (PKI) (IP Security [IPsec] and Internet Key Exchange [IKE], and Secure Shell [SSH])
- SSHv2
- Authentication, authorization, and accounting (AAA) protocols: TACACS and RADIUS
- Globally enforced SNMP privacy encryption
- HTTPS
- SNMPv1, v2c, and v3
- CLI and SNMP user synchronization
- Advanced Encryption Standard (AES) encryption-based privacy

Intelligent Network Services Support

The Cisco MDS 9000 Family services nodes (Cisco MDS 9000 18/4-Port Multiservice Module, MDS 9222i Multiservice Modular Switch, MDS 9000 16-Port Storage Services Node, and MDS 9000 Storage Services Modules) provide intelligent network-hosted services to Cisco storage networks, including such services as Cisco SAN Extension over IP, I/O Accelerator (IOA), SME, Data Mobility Manager (DMM), and Secure Erase for storage LUNs.

Network-assisted applications are enabled through the open Cisco intelligent services API (ISAPI). Cisco makes the ISAPI development platform available to original storage manufacturers (OSMs) and independent software vendors (ISVs) that want to develop storage applications on the Cisco storage network platform. Cisco delivers the data path software architecture, and the OSM or ISV provides the control-path software architecture and applications.

Major Intelligent Applications

- Cisco IOA accelerates I/O over metropolitan area networks (MANs) and WANs using proven Cisco SCSI acceleration technology. Cisco IOA can also be used to enable remote tape backup and restore operations over long distances without significant throughput degradation (Figure 21).
- Cisco DMM provides transparent online data migration across heterogeneous storage arrays without the need for host agents (Figure 22).

Figure 21. Cisco IOA Configuration

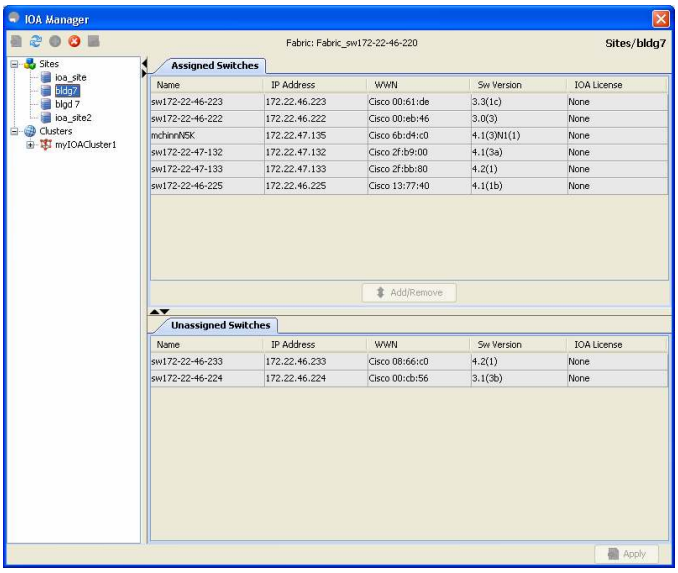
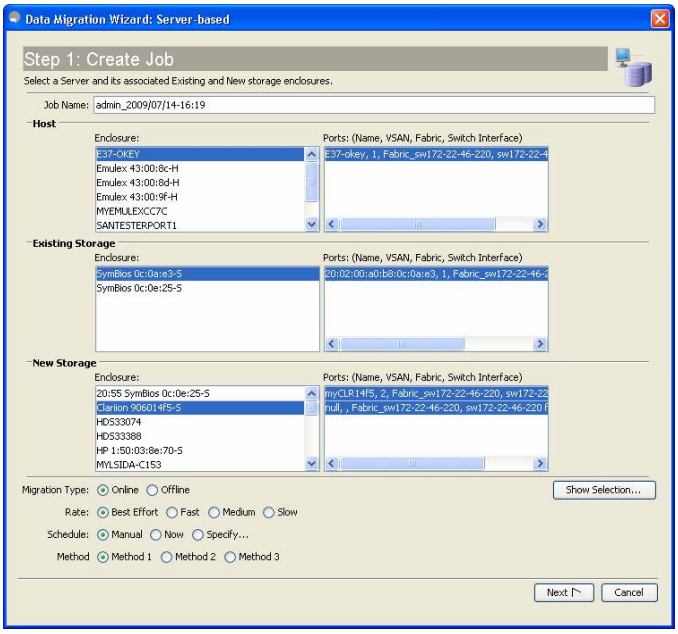
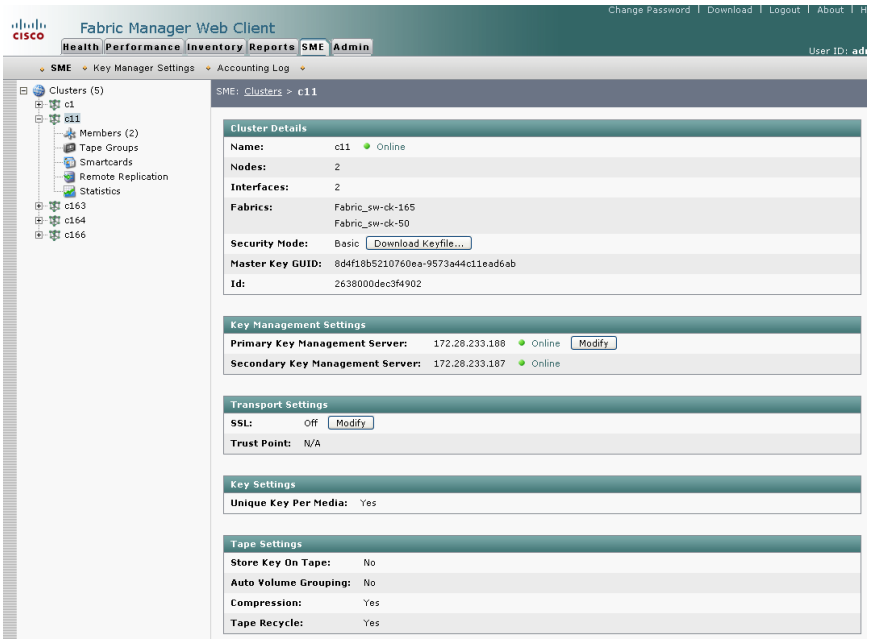


Figure 22. Cisco DMM Configuration



Cisco SME provides a secure solution for encrypting data at rest on SAN-attached storage devices and includes comprehensive key management functions (Figure 23).

Figure 23. Cisco SME Configuration



Third-Party Software Integration

Cisco Fabric Manager provides a web service API (Simple Object Access Protocol [SOAP]) for third-party application integration to enable the discovery of fabrics and retrieval of related inventory details (VSANs, zones, end devices, ISLs, etc.).

Cisco Fabric Manager Web Services (FMWS) enables third-party vendors to access Cisco Fabric Manager core software functions as remote procedure calls. Cisco FMWS extends the World Wide Web (WWW) infrastructure to provide a method for interoperating with third-party software applications. Applications access Cisco FMWS using many protocols and data formats, such as HTTP, HTTPS, XML, and SOAP. Cisco FMWS combines the best aspects of component-based development and the web. Cisco FMWS makes Cisco Fabric Manager an enterprise-class application, allowing it to interoperate with other software platforms.

Resource Requirements

Table 2 lists the minimum resources (disk, memory, and CPU) required for both the server and client for Cisco Fabric Manager to operate satisfactorily.

Table 2. Resource Requirements

Size	Small	Medium	Large
Port count	Up to 2000	Up to 5,000	Up to 15,000
Disk space (includes Cisco Performance Manager Round-Robin Database [RRD] files)			
Client	100 MB	100 MB	100 MB
Server (plus PostgreSQL)	1 GB	10 GB	20 GB
Server (plus Oracle Express Edition)	3 GB	15 GB	30 GB
Memory			
Client	500 MB	1 GB	2 GB
Server (plus PostgreSQL)	2 GB	4 GB	8 GB
Server (plus Oracle)	2 GB	4 GB	8 GB

CPU: Client			
Microsoft Windows	2.0-GHz processor	2.0-GHz c	2.0-GHz processor
Linux	2.0-GHz processor	2.0-GHz processor	2.0-GHz processor
Solaris	Ultra 45 1.6 GHz	Ultra 45 1.6 GHz	Ultra 45 1.6 GHz
CPU: Server			
Microsoft Windows	2.0-GHz processor	Dual processors: 2.0 GHz	Dual processors: 2.0 GHz
Linux	2.0-GHz processor	Dual processors: 2.0 GHz.	Dual processor: 2.0 GHz
Solaris	SunFire Version 240 2x 1.6 GHz	SunFire Version 440 4x 1.6 GHz	SunFire Version 440 4x 1.6 GHz

For More Information

For more information about Cisco Fabric Manager, please see the Cisco MDS 9000 Family Fabric Manager Configuration Guide, Release 4.0 (http://www.cisco.com/en/US/docs/switches/datacenter/mds9000/sw/4_1/configuration/guides/fm_4_1/fmguide.html) or the release notes for Cisco MDS 9000 Family Fabric Manager (http://www.cisco.com/en/US/products/ps5989/prod_release_notes_list.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 C78-384070-07 01/10