SearchNetworking.com E-Guide

Taking Network Configuration and Change Management to the Next Level

Network managers are finally adjusting to the use of change management tools and processes to determine the potential environment caused by a change in order to avoid downtime. Now, as networking pros are being asked to manage virtual machines in their networks, as well as the connection between fluid storage sources and the rest of the network, the demands on change management processes have changed. This series will address implementing configuration and change management in a partially virtual environment, discussing how managers can use change management tools and processes to report on and manage virtual servers as they move between hosts. The series will also look at how changes in physical hosts affect servers. Beyond that, the series will explore how to extend change management processes, including ITIL, to manage upgrades and reconfigurations of the SAN. We will also explore how change management policies can help solve human problems that arise between networking, data center and storage teams when it comes to connecting the three systems.

TechTarget
The Technology Media ROI Experts

SearchNetworking.com E-Guide

Taking Network Configuration and Change Management to the Next Level

Table of Contents:

Network change and configuration management evolves

Network change and configuration management (NCCM) is a strategic approach to minimizing the impact of change on a network or IT ecosystem. The goal is to create a company-wide standardized method to implementing both self-motivated, internal change, such as upgrades and troubleshooting; as well as externally required change, such as government regulations on data. The catch? Networking teams must tackle these changes with zero network downtime.

Configuration management plays a central role in change management since some tools enable networking teams to use software to create detailed maps of the location and configuration of each component and the link or connectivity between them. Network managers can do this either by working through geographical templates provided by the vendor software or in some cases by importing entire images of their networks into the application. These maps work with information from configuration management databases (CMDBs) that contain detailed recordings of the configuration of each component and all updates or changes that have been made along the way. The databases also track the provisioning and function of applications, operating systems patches, previous incidents, etc. That means every time a networking technician updates a configuration or implements something new on the network, they can check the database to be sure there won't be conflicts with existing functions. In turn, technicians are also required to input changes they make into these databases, though some CMDBs track all changes automatically.

Compliance plays an important role in configuration and change management. Mapping tools, CMDBs and network monitoring devices help companies be sure that all changes implemented do not violate government data regulations, such as HIPPA and the Sarbanes-Oxley Act.

Network change and configuration management tools

A multitude of NCCM tools abound on the market. Some tools focus on one element of change and configuration management, such as monitoring or archiving, while others attempt to be an overall solution. Network managers often find themselves patching together a number of applications for the right solution. NCCM tools contain the following features:

- Mapping: The goal is to map as many components, configurations and functions of the network and systems as possible.

- Database (CMDB): A complete, searchable archive of every component configuration and all changes that occur along the way. This database can also track network usage records, applications and service delivery, operating systems and more.

- Documentation: Maintain configuration templates or standardized approach to all network and systems changes.

- Monitoring: These tools monitor the network for the effects of change on performance, as well as for unplanned change. They also seek to ensure regulation compliance, especially on components that have automatic configuration and self-healing mechanisms.

• Reporting: Databases and monitoring tools are used to create user-friendly reports that can generally be accessed via Web interface and viewed in multiple formats.

• Interoperability: Increasingly these tools are being designed to work across network components and software platforms from multiple vendors to gather information.

CMDB Federation Specification and distributed networks

Because some enterprises must manage change across networks, they often require CMDBs that can collect information from a number of management databases. As a result, this year the Distributed Management Task Force (DMTF) created the CMDB Federation Specification (CDMBf). Vendors following the specification will create tools that enable organizations to integrate CMDB data across various products and tool sets.

ITIL for network change and configuration management

IT Infrastructure Library (ITIL) is an internationally recognized set of policies and procedures for managing IT systems and services. It is like a library of industry best practices that offers a standardized approach to everything from cabling infrastructure to computer installation and service management.

Using ITIL policies, IT teams can more easily correlate the relationships between change and network performance. CMDBs are a clear fit for use in ITIL for change and configuration management since they readily provide extensive information for analysis.

Aligning ITIL, configuration management and business processes

Using ITIL best practices and CMDB tools, change management can be applied to business processes and applications in order to avoid service outages. CMDBs and mapping tools track the alignment between network hardware usage and specific business processes and applications. Networking teams generally start by tracking just a few business processes, and then they refine the approach over time. As they add more applications to analyze, chance of outages is reduced.

Human touch: Network change and configuration management policy

Tools can only do so much when it comes to NCCM. Companies must also enforce change and configuration management policy among staff members. That means every IT technician must be required to check and update databases with every change and be cognizant of compliance regulations, etc.

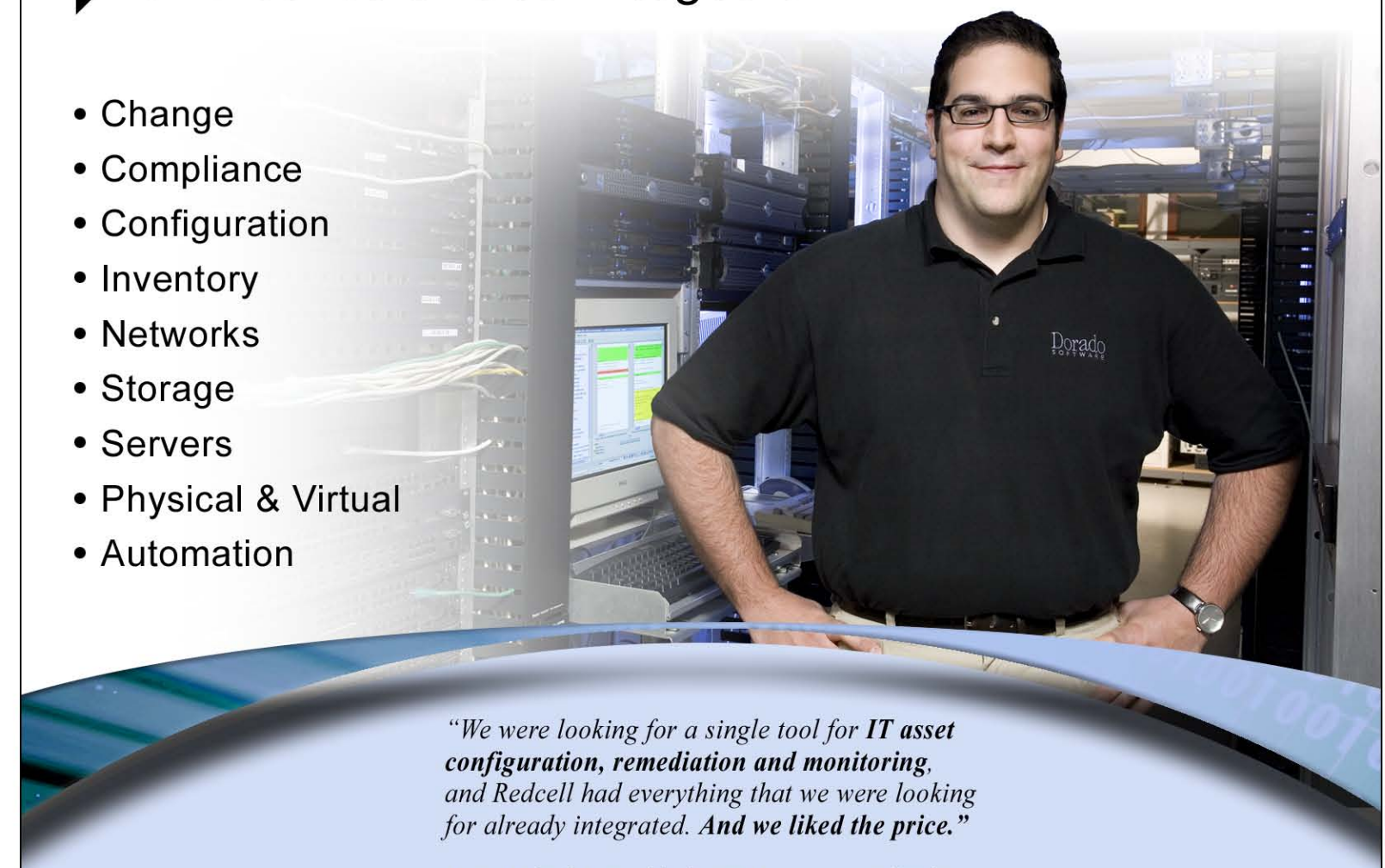
Companies often appoint change advisory boards (CABs) that are charged with setting internal change policy as well as tracking external regulatory updates that will affect internal operations. These boards must be made up of members of various parts of the IT ecosystem, as well as other business units in the enterprise that can provide input on business processes and services.

Next Gen **Configuration & Change** Management

Visit web site for FREE Trial software

One console. Get IT together.

- Change
- Compliance
- Configuration
- Inventory
- Networks
- Storage
- Servers
- Physical & Virtual
- Automation



*"We were looking for a single tool for **IT asset configuration, remediation and monitoring**, and Redcell had everything that we were looking for already integrated. **And we liked the price."***

- Dave Nebral, Network/Telecom Manager - Greatbatch

Take it to the next level with Redcell from Dorado Software. Redcell offers a complete, unified, end-to-end management solution for **network configuration and change management** in next gen data centers. It manages the inherent complexity of next-gen data centers - servers, storage, physical and virtual layers - from a common repository that's way easier to manage.

With Redcell you can FIND, CONFIGURE and MONITOR all the components of your next-gen data center - networks, security, storage, applications, even printers - AND your IT services - from **one integrated system**. You can't get to the next level unless you get it together...on one console from Dorado Software.

for more information

www.doradosoftware.com

info@doradosoftware.com

Dorado SOFTWARE

Why you need to know about virtualization change and configuration management

There is one central belief behind how network change and configuration management (NCCM) works: IT teams must have a basic blueprint of all of the network components, how they are configured, their connectivity and which applications or business processes they are linked to. With that information intact, IT can make informed decisions about implementing change without causing conflicts with existing systems that result in downtime. That whole concept is fully challenged with server and network virtualization.

The beauty of virtualized machines (VMs) is that they are easily migrated between physical hosts according to need. What's more, within a server, memory and space resources are constantly reallocated depending on application demand. That means that NCCM tools, including monitoring devices and databases, must adapt in order to document and archive this fluidity. That's a tall order.

The stakes are higher in virtualization change and configuration management

NCCM is more crucial than ever in a virtualized environment. When change causes outages in a virtualized environment, the ripple effect is much greater than it is in a physical network. After all, if one x86 server (physical host) supporting six virtual application servers goes down, you've lost seven servers rather than one.

In an average network, most outages are not a result of poorly working hardware, but rather of incidents that result from upgrades or troubleshooting. In a virtual environment, approximately 80% of repair time is spent investigating what changed in a system.

Server virtualization challenges the NCCM process, lifecycle management

That's because it's not always easy to monitor an environment with virtual servers. First, VMs are often automatically migrated from one physical host to another. That can cause a range of problems. Movement of virtual machines must be recorded and mapped so that they can be located for troubleshooting. After all, virtual servers need all the same software updates, security patches, hotfixes, memory, CPU and disk upgrades as physical servers.

But it's also important to record the configuration of the new host. That physical server may have a different configuration than the previous one. Network managers must confirm that the configuration of the new host keeps applications in compliance with government regulations and internal policy. That means if an Exchange server is moved to a new host, inbound and outbound messages will still have the same security protection they had on the previous host, for example. This is especially important when servers are hosting databases with health or financial data that must meet HIPAA and Sarbanes-Oxley Act regulations.

The ultimate goal is to create a geographic map of VMs regardless of how often they are moved. That map must be tied to information about the business processes and applications linked to the VMs. Once there is an outage, there is no time to look for this information. VM lifecycle management tools increasingly aim to better control automated provisioning according to policy, and they focus on configuration and change management. Many of these tools are new and evolving.

Should you limit live migration for NCCM in virtualized environments?

While a number of software applications promise to monitor VMs and record their locations as they move, it is questionable how well they keep up in an environment with lots of automatic migration. While live migration of VMs between physical servers is considered one of the most helpful elements to using virtual servers, network managers may want to limit this use until they are sure they have tools that can document changes in real time.

While limiting automatic migration may put a damper on virtualization potential, it helps to simplify the mapping of applications to physical resources and makes troubleshooting and performance management easier.

Tracking resource allocation

In addition to mapping the location of servers, it's also important to archive the allocation of resources -- such as memory -- within physical servers. If, for example, one application demands more memory than others on a specific server, it is common to reallocate resources. A committee often makes allocation decisions -- or at least a staff member is charged with change management using an archive of past changes.

Network virtualization and NCCM strategies

The real problem with NCCM strategies in a virtual environment may actually stem from network virtualization. While network virtualization eases management in some ways, it can be difficult to find end-to-end monitoring and mapping tools that track all of the connectivity and components in a virtual network.

Network virtualization enables the separation of network behavior from the underlying physical network resources. It allows network aggregation and provisioning, combining portions of different physical networks into a single virtual network or breaking a physical network into multiple virtual networks. These can be used as synthetic networks between virtual machines or run as isolated networks.

Network virtualization eases management in that several virtual switches, for example, can be pulled together and managed as one virtual switch. But for NCCM purposes, each of these virtual components, their configuration, their connectivity and the business processes that are linked to them must be mapped and archived. Several software applications promise to do this, but many engineers have found inconsistencies in monitoring tools that offer a holistic view. As a result, there is a long way to go in creating universal policy in relation to virtual networks.

Virtualization change and configuration management tools

The holy grail of NCCM tools for virtualization is a solution that has an end-to-end network view to monitor all virtual servers, network components and data paths. That, of course, would link to a configuration management database (CMDB) that would include configuration information, links to business processes and applications and so on. Also, tools that control VMs would be loaded with policy, ultimately enabling features like automatic migration without causing conflict.

A number of companies claim to have these tools, though users are still testing them to find what really works. Most of the solutions are still evolving as virtualization of servers and the network becomes more prevalent.

Some NCCM tools for virtualization focus on one element, such as virtual server monitoring and control. Others claim to offer a holistic network view and assessment. Either way, ultimately these virtualization monitoring and assessment tools will be integrated into existing CMDBs and other change management applications.

Existing tools generally aim to offer the following features:

- Virtual machine monitoring: These tools monitor specified host servers and their virtual machines. They can track performance of a server and the applications that are tied to these servers.
- Enterprise-wide monitoring: It monitors all virtual servers as well as virtual network devices. This tool checks the health of the physical server as well as each virtual machine, and it monitors the use of virtual resources and provides live reporting.
- Lifecycle management
- Central control of configuration changes
- Monitors for compliance with internal policy and government regulations
- Real time reporting through a Web interface

Understanding the need for SAN change management systems

Server and network virtualization pose complexities to network change and configuration management (NCCM). But implementing change management in storage area networks (SANs) is the mother of all challenges.

That's because mapping, documenting and monitoring SANs is extremely complex. SANs centralize enterprise storage by forming a network between all of the storage devices. The SAN then connects with the data center and on to the rest of the network.

Change management for the SAN means mapping and documenting complex relationships between hundreds (or more) of interconnected servers, as well as switches and storage arrays. SAN change management also involves the intricacies of documenting the relationships between virtual machines and their hosts. Beyond the components, monitoring SANs requires tracking thousands of access paths in real time. In a SAN with only 50 servers, tens of thousands of paths must be documented and monitored.

To add to the complexity, network managers create zones on SAN switches so that servers see only specified applications. This is done for both security and organizational purposes. Also, managers assign storage volumes to specific applications and they must document every change made to any of these configurations.

SAN change management is crucial since application availability relies on functioning storage networks. Approximately 50% of problems in the SAN are related to change.

Ultimately, SAN change and configuration management tools aim to avoid application outages and maintain service-level agreements by managing change implementation more efficiently.

What can SAN change and configuration management tools do?

SAN change management tools generally enable automated component and configuration discovery, mapping, centralized control and reporting. The software also monitors and reports on paths, as well as the health of business processes and applications. Reporting enables network managers to use this information to make decisions about changes they can make without disturbing existing configurations.

While SAN change management applications often fall under the umbrella of SAN provisioning and capacity planning tools, the software must also integrate into existing network change and configuration management. Many SAN change management applications integrate into existing server and network change management databases (CMDBs), offering a single-pane view of the entire network from the core to storage.

Getting to the root-cause with SAN change management tools

While there are similarities in network, server and SAN change management applications, SAN-specific tools often have more complex functions. One of those functions is root-cause analysis.

Root-cause analysis uses information collected either from real-time monitoring or from snapshots of data paths to pinpoint the cause of a problem. The goal is to first create a baseline of what a healthy configuration should look like. Then, when a problem occurs, network managers can quickly compare the previously saved stable configuration to the problematic one to find the root.

With root-cause analysis, managers use information collected to create algorithms for fixing problems. Automated root-cause analysis is one way for storage managers to make sense of the large influx of information that comes in from real-time monitoring alerts.

Predicting the future with SAN change management tools

Some tools also include predictive applications. They model the SAN and then simulate change in order to measure the potential impact on the system.

Some of these applications create simulation in an out-of-band network. Most storage devices include common information model (CIM) agents that managers can use to create a model SAN. Using this model, they can introduce new change and also replay incidents that occurred to examine alternative troubleshooting methods.

ITIL and SAN change management policy

IT Infrastructure Library (ITIL) – the internationally recognized set of policies and procedures for managing IT systems – briefly addresses storage change management. While ITIL is meant to offer a standardized approach to everything from cabling infrastructure to computer installation, the latest version focuses heavily on service management. Because of that, there is a section that addresses storage archiving and policy specifically. ITIL calls for a dedicated team to manage storage. It also outlines how, where and for how long data should be stored.

About the Author: *Rivka Gewirtz Little is the site editor for SearchNetworking.com. She works with editorial staff to develop content aimed at readying businesses for the changing nature of the network, including its infrastructure and applications. Rivka was previously the site editor of www.SearchNetworkingChannel.com and a senior news writer at www.SearchITChannel.com. Rivka has been covering telecommunications and networking since deregulation of the FCC in 1996. She began her career as a daily news reporter in Texas and has been a frequent contributor to The Village Voice, The Houston Chronicle and numerous technology and business publications.*

Resources from Dorado Software

Dorado SOFTWARE

Service Level Monitoring: Real-Time Visibility and Reporting for Mission-Critical IT

'Lights Out' IT Management – Automate Problem Identification & Resolution

The Complete Network Assessment – Improve the Health & Security of Your Network

About Dorado Software

Complete Lifecycle Management of Networks, Systems, Services andApplications

Dorado Software, Inc. is the market leader in infrastructure and service lifecycle management for heterogeneous and multi-technology environments. Dorado gives the power to view, deploy, configure and control resources via a single solution, offering an economical and efficient alternative to the multiple disparate systems traditionally used to manage networks and data centers.

Dorado Software is founded on expertise in the network and system management arena and driven by innovation. Continuously upgrading and building on its extensive suite of products and massive library of "Device Drivers", Dorado keeps ahead of next-generation network-based technologies as they evolve.

Dorado's cost-effective integrated solutions deliver low TCO and rapid ROI, minimizing risk while providing high value. The cost to deploy Redcell is a fraction of expensive Framework-based and OSS solutions yet delivers all the functionality companies need.