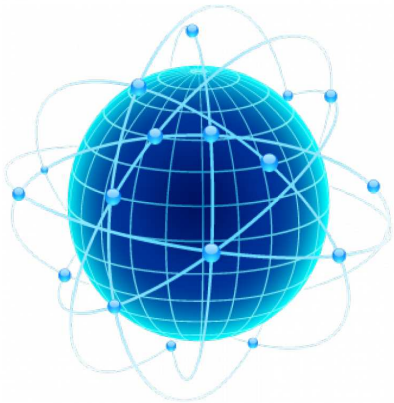
NMSaaS

Best Practices Guide

Top 20 Best Practices for Network Configuration and Change Management.

Contents



1. NCCM Management Overview

Corporation's networks today are expanding exponentially but, more importantly, today's networks are the backbone of a companies' ability to perform its day-to-day business. When network failures occur, businesses cannot operate, revenues are affected, and loss of credibility/customer experience can be catastrophic. Maintaining a consistently high level of service availability is the number one job of any IT organization. However, as you will see, many unplanned outages still plague most IT Networks. These unintended downtimes can cost more than just lost productivity – they can lead to user & customer dissatisfaction which in turn leads to lost customers, lost reputation, and lost revenue.

Enterprise Management Associates reports that 60% of availability and performance issues/errors are the result of misconfigurations. Additionally, industry leading technology research companies (i.e. Gartner & Forrester) report that over 80% of unplanned outages are due to incorrect changes to the corporation's infrastructure by system/network administrators and developers.

A recent Gartner study projected that "Through 2015, 80% of outages impacting mission-critical services will be caused by people and process issues, and more than 40% of those outages will be caused by change/configuration/release integration and hand-off issues." *(Ronni J. Colville and George Spafford Configuration Management for Virtual and Cloud Infrastructure*

Network infrastructures are evolving at an unprecedented rate and, with mixed-vendor environments the norm rather than the exception, management of those systems has become a labor-intensive exercise. Unlike Fault and Performance Management, Network Configuration Change Management (NCCM) has no common harmonized management method or protocols; even first-level engineering teams have to be proficient in numerous different configuration languages and interfaces to perform the simplest of tasks.

An NCCM tool must deliver key functionality in multi-vendor environments to enable common management techniques to be used. Some examples of critical functionality are:

- Real-time configuration backup and restoration to ensure a complete audit trail of changes
- Service continuity and fault/performance analysis
- Process-oriented change management enabling common tasks to be packaged into repeatable processes and for more complex changes to be structured
- Software and firmware upgrade management
- Configuration policy management to enforce corporate/design standards and regulatory requirements
- Vulnerability and EOL (End-of-Life)/EOS (End-of-Sale) tracking for compliance, asset and financial planning

2. Discovery & Network Inventory

When discovering a network it intelligently prioritizes each device it discovers and assigns a weight-value that automatically maps its hierarchical relationship and overall importance within the network topology.

The discovery process includes the capability for extracting all of the devices hardware and software inventory data, including network relationship information.

Best Practices – Discovery & Network Inventory

This section provides guidance for best practices used in the discovery, and continual operational discovery, of an infrastructure environment.

1 – Discover the Current State & Health of the Infrastructure

Understanding the current state and health of the network infrastructure is a fundamental requirement in any infrastructure management environment. What you cannot see you cannot manage, or even understand, so it is paramount for infrastructure stability to have a tool that can constantly discover the state and health of the components in operation.

Simply discovering the network once is not enough as the infrastructure is an ever-changing and evolving environment that needs the best practice processes and tools in place to auto-manage the change and evolution effectively and efficiently.

2 – Manage & Control the Infrastructure Environment

Once you have a fully-discovered network inventory that has the best practice process of an auto-scheduled re-discovery in place you can then start to manage the infrastructure environment in a controlled & secure way. An accurate inventory of the environment's components provide the ability to track hardware, manage end-of-life and end-of-support, hardware threshold management (i.e. Swap-Out device before failure) and effectively manage the environments operating systems and patch management.

The process of recurring auto-scheduled discovery of device hardware and software greatly mitigates any risk against partial or complete hardware failures as you will have all of the knowledge of the hardware and configuration of the failed device in order to be able to replace them exactly. Having this information at your fingertips greatly reduces your risk of prolonged outages, and more importantly, reduces the risk of seriously affecting your business thus maintaining sustained high levels of service availability.

3 – Automate Deployment

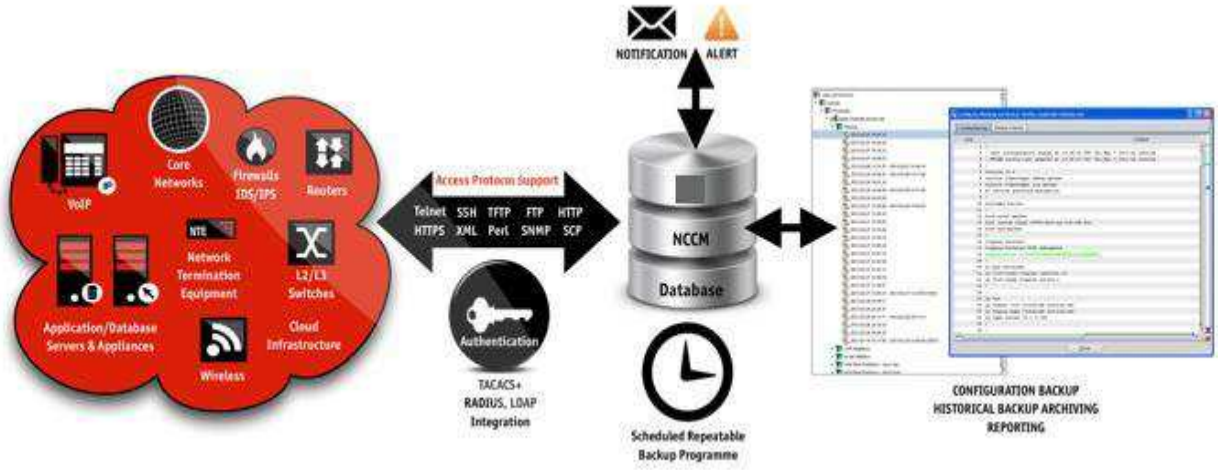
Corporation's today place a lot of emphasis on automation therefore, it is very important that when choosing a tool to operate your infrastructure environment, the tool can integrate seamlessly with your CRM system in order that auto-provisioning of new customer infrastructures, and the expansion of existing infrastructures, can be performed in a repeatable automated way. Having a consistent view of the infrastructure inventory and services will allow repeatable and consistent deployment of hardware and configuration in order to automate service fulfillment and deployment.

3. Device Configuration Backup

Configuration Backup means having a system that supports multi-protocol access for entry into multi-vendor telecom, service provider and enterprise network infrastructures. The majority of system are generally integrated with authentication systems, i.e. TACACS+, Radius, LDAP, where the access credentials are configured for the NCCM platform to gain authenticated access into multi-vendor infrastructures. Scheduled backup jobs are then characteristically setup and structured to fit the backup schedule process you wish to implement.

The scheduled backup jobs would then automatically start at the scheduled date/time to access the infrastructure in order to back up the configuration. Device backup file formats supported must include text-based configuration, typically found on Cisco, Juniper, Brocade, and binary file formats typically found on Ixia, Bluecoat, and F5 infrastructure devices.

The Configuration Backup Structure



Best Practices – Device Configuration Backup

This section provides guidance for best practices used in infrastructure device configuration backup, and continual operational device configuration backup, of an infrastructure environment.

4 – Auto-Discovery Configuration Backup

When discovering the network infrastructure hardware components it is essential that the software IOS image, along with the startup and running configuration files, are backed-up as part of the initial discovery process. The auto-discovery should have the option to include device logon credentials as part of the discovery process. Through the use of your authentication system *i.e. TACACS+, RADIUS,* you can setup a credential profile and auto-logon to devices and auto-backup the configuration as part of discovery.

Having the ability to perform configuration backup is a fundamental requirement of any NCCM system however, having the flexibility to perform additional ‘show’ type commands as part of the configuration backup process to capture current snapshot states of the operating device is of huge benefit as additional device and operational performance data can also be collected and tracked at the same time.

5 – Configuration Backup Automation Alerting

It is essential to know when your infrastructure has been backed-up successfully, or if backups have failed, and more importantly why they have failed. A system must have the capability to send notification updates of backup configuration job successes, failures, and why the job failed. Notifications should be emailed to targeted audiences, alerted via SMS *(providing an SMS gateway is available),* and via any Web & GUI clients. Having up-to-date and current device configuration of your infrastructure is paramount in the mitigation of potential catastrophic failure as it is a key component for the restoration of failed, or misconfigured, infrastructure.

6 – Configuration Backup Scheduling

Once an infrastructure has been discovered and the configuration of that infrastructure estate is backed-up and being operationally managed then you should look to employ a best-practice backup structure and appropriate schedule. For example, the grouping of key devices, or services within your tree-structure, may have elements whereby change to the infrastructure is common place, *i.e. firewall rule-sets, customer LAN switching, etc.* Therefore, it would be common place to ensure daily scheduled backups of these groups are committed. Whereas, the core network components have very little change so weekly scheduled backups may be more appropriate.

It is important to plan a backup schedule for implementation from day 1, and then fine-tune the schedule through the knowledge of the change analytics overtime. Most devices can also send syslog or traps when the configuration is changed, and this event can then automatically trigger a backup process to be initiate.

7 – Configuration Backup Reporting

Reporting and visualization of infrastructure device backup data is a prerequisite for target audiences, for example service management, problem/incident management teams, to understand as part of operational and service health-checking.

Having a daily report of out-of-hours service infrastructure changes is key for firstly, have the knowledge of what has changed so as to correlate the change with a reported service issue, secondly, having established the change is a result of a service issue being able to remediate the change to the previous-known working state, and thirdly, maintaining higher levels of service availability by making better informed decisions on the knowledge of knowing what has been changed.

4. Policy Compliance & Governance

Many organizations today have configuration and security policy rules that require compliance checking to ensure consistency with design standards, processes and directives with internal and external regulators. Using manual processes is not recommended, as it is time intensive, costly, inaccurate and more importantly, your business could be at risk and open to potential attacks through not having the desired real-time visibility.

The policy compliance and governance engine within the an NCCM system must allow corporations to create policies electronically in order to scan/analyze configurations of the infrastructure environment so as to produce accurate and timely compliance and violation reporting analytics. Configuration policies bring together a set of devices and apply a set of rules. This approach means that an entire service type can have specific policies applied so as to ensure consistent service delivery, change and compliance.

These rules can be based on simple text ‘strings’ to finding items present or missing in configuration files; powerful configuration snippets with ‘section’ matching and ‘regular expression’ searching; or advanced scripting languages, *(i.e. XML, Perl)*. The same rule should be able to be created for different vendor hardware using the same identifier, meaning an organization can create a single corporate policy within the NCCM solution to reflect all hardware vendor equipment simplifying reports into a single view.

Whether you need to meet FIPS, PCI, ITIL, FCAPS, ISO27001, SOX, NSA Security Guidelines or other business continuity or regulatory standards a policy checking engine can help greatly with simplifying the process, drastically reduce your risk, and drive compliance consistency throughout your infrastructure ensuring sustained levels of service availability.

Best Practices – Policy Compliance and Governance

This section provides guidance for best practices used in infrastructure policy compliance and governance management and continual operational of policing and governance, of an infrastructure environment.

8 – Regulatory Compliance Policy

Governments and industry regulators require organizations to conform to standard best practices. In order to become compliant with these regulations such as FIPS, PCI, ISO27001, FCAPS, ITIL, SOX, HIPPA, and others, device configuration should conform to these standards. These standards can range from a number of different requirements such as ensuring the presence, or absence, of certain strings, commands, or values.

Any Policy Compliance engine should be able to test for known regulatory compliance requirements and report on out-of-compliance devices & configurations.

9 – Vendor Default Policies

Vendor's ship equipment with default configuration enabled to assist with out-of-the-box implementation. It is known that the default configuration settings are overlooked a lot of the time when the device in question is installed within the organizations infrastructure. Common settings, for example around default username and passwords, or SNMP 'public' and 'private' community strings etc. are not removed, leaving a hole in your security for potential access to attacks.

Therefore, it is a best-practice recommendation that you create policies to scan the configurations of your infrastructure devices to eradicate these potential holes in order that the risk can be mitigated and infrastructure security access is maintained to the highest possible levels. This is also an NSA guideline requirement.

10 – Security Access Policy

Access to infrastructure devices are policed and controlled with the use of AAA *(Authentication, Authorization, Accounting)* TACACS+, RADIUS servers, and ACLs *(Access Control Lists)* so as to increase security access into device operating systems. It is very important therefore that the configuration elements of infrastructure devices have the consistency across the managed estate.

It is highly recommended to create security policies so that the configurations of security access can be policed for consistency and reported on if changed, or vital elements of the configuration are missing.

11 – Service Design Rules Policy

Telco's, ISPs/MSPs and Enterprise organizations have service types that may be pre-defined *i.e. Standard, Enhanced and Premium service types,* or they may have specific *(customized)* services they design for their organizations, customers, internal/external 3rd party interconnects etc. Ensuring service design rules are being applied and policed is usually a manual process and therefore is susceptible to inaccuracies.

Creating design policy rules provides greater control around the service offerings, *i.e. QOS settings for Enhanced service offerings, or a complete End-2-End service type,* and ensures compliancy with the service delivery SLAs *(Service Level Agreements)*.

5. Configuration Change Management

The management of configuration change across large infrastructures is a policing minefield as engineers will argue that ad-hoc changes will always be necessary to bypass issues, or workaround solutions in order to maintain service availability and operation.

Whilst there is an argument around the pro's and con's for 'on-the-fly' changes the simple fact remains that infrastructures today can attribute over 40% of down-time to unauthorized changes. Therefore, organizations need to transform their policies and processes to implement greater secure control around all changes made to the infrastructure.

NCCM is designed to fully meet this transformation whereby greater structure and control of all changes to the configuration of the infrastructure components are executed with the knowledge that the change has been tested and is controlled in a way whereby it can easily be rolled back if problems or performance issues occur.

The bigger picture is that consistent repeatable configurations can be deployed to agreed service fulfillment criteria, large scale complex deployments, or changes to the existing infrastructure environment, can be pre-scheduled guaranteeing carbon-copy execution.

Operating costs will reduce as out-of-hours requirements for change will be automated, and high-level engineering requirements for complex changes will be able to be executed via lower level engineering through the pre-configured auto-scripting functionality. Any change to the system will have a full audit-trail detailing what was changed, who made the change, when the change was executed, and what infrastructure devices the change was executed on.

Best Practices – Configuration Change Management

This section provides guidance for best practices used in infrastructure configuration change management and continual operational configuration change, of an infrastructure environment.

12 – Enabling of Real-Time Configuration Change Detection

Configuration compliance policies for SNMP and Syslog are essential for the assurance of receiving notifications of changes to device configurations. Unauthorized configuration changes are common practice within all sizes of business and so it is extremely important to have the necessary controls in place to notify and audit when a change was committed, what devices the change was committed too, and who performed the change.

By having the ability to perform these key actions you will be able to remediate known changes with ease, control your infrastructure estate with a higher degree of knowledge of what is being changed, correlate actual change configuration with approved change control processes, and maintain a higher level of service availability.

13 – Configuration Change Compare Management

Having visibility of changes to the network infrastructure is essential for any NCCM implementation however, being able to compare configurations from previous-known states is a powerful and quick way of identifying exactly what has changed, or been added, to a device configuration. However, it is not just configuration files, or startup/running configuration comparison visibility that is required.

Having the added capability to execute and backup the output of ‘show’ type commands as part of the configuration backup schedule allows for the tracking of device operational performance analytics with the ability to compare previous and current states.

14 – IOS Feature Set Version Control and Patch Management

Tracking IOS feature types and versions in use across your entire infrastructure is a very important attribute for any NCCM tool capability. It is important to understand the feature sets and versions that are in use for a number of reasons:

1. Infrastructure best practice management design rules will stipulate approved IOS feature sets and versions authorized for use on the infrastructure. Scanning and correlating of the in-use IOS feature sets and versions will ensure design rule compliance.

2. Having full visibility of the IOS feature sets and versions in use will assist in the Vulnerability & Lifecycle scanning process to highlight potential security risks and End-of-Life, -Sale, and -Support of the feature sets and versions in use.

3. Complete IOS patch and upgrade management of the infrastructure feature sets whereby automatic upgrades of IOS can be pre-scheduled and rolled out in a totally automated way.

15 – Central Repository and Knowledge Base

Everyone knows the situation that happens when a network administrator leaves a company. The knowledge has to be transferred, the scripts developed have to be maintained by someone else, and ultimately the new administrator will find it difficult to maintain his predecessor's code and will end up re-writing the scripts in a way whereby he better understands them.

In order to break this cycle - corporations need to employ a tool that has the visibility of the network and can perform repeatable consistent change process that maintains a knowledge base and central repository of the organizations NCCM templates.

Any NCCM tool must have a central knowledge base repository for the organizations NCCM templates to be stored. Based on XML the NMSaaS NCCM templates are easy to maintain, include version control, role-based access, track updates, and provides wider visibility to the service and operational community.

16 – Bulk Configuration Change

Automation is the important task in IT operations nowadays. IT Managers are always looking to automate repetitive and time-consuming tasks in order to reduce operational cost and improve productivity. NCCM tools supports you in this task by automating bulk configuration and change management for network devices. Tasks can be scheduled and configuration changes can be executed for individual or groups of network devices. It is possible to alert on configuration change or policy failures and restore a known good configuration as required.

17 – Configuration Reporting

For assurance purposes it is essential to have accurate reporting on the status of the configuration across the managed infrastructure. Having up-to-date knowledge of infrastructure device configuration changes, backups, failures, knowing what changed on what device(s), and who committed the change is vital for service operations, and service problem and incident management teams.

Visibility of out of hours change activity and rapid identification of what has changed in order that immediate remediation of a change can be restored is vital for maintaining service availability and service level agreements.

18 – Compliance Reporting

Where policies have been applied to govern the configuration and assets within the infrastructure it is necessary that infrastructure compliance reporting is enabled to ensure visibility status. Service problem and incident management teams will need these reports to ensure that compliance is being maintained as changes to the infrastructure occur.

19 – Regulatory Reporting

Governments and industry regulators require organizations to conform to standard best practices. In order to become compliant with these regulations such as PCI, ISO27001, FCAPS, ITIL, SOX, HIPPA, and others, device configuration should conform to these standards.

These standards can range from a number of different requirements such as ensuring the presence, or absence, of certain strings, commands, or values. Reports on policy compliance and violations must be available out-of-the-box.

20 – Vulnerability & Lifecycle Reporting

It is essential to Plan, Maintain, Optimize and focus on upholding accurate vendor updates. Having a process in place whereby announcements are captured and applied to your existing vulnerability and lifecycle data is paramount in maintaining a highly optimized vulnerability and lifecycle management system.

Where policies have been applied to govern the vulnerability and lifecycle of devices within the infrastructure it is necessary that the compliance reporting is enabled, to ensure visibility of the analytics for service incident and problem management teams to certify that compliance is being maintained.

About NMSaaS

NMSaaS is the leader in comprehensive Network Management. The team behind NMSaaS has extensive experience in developing and delivering Network Management solutions to organizations of all sizes.

Our skills and experience have allowed us to identify a major weakness in traditional network management solutions where organizations juggle multiple tools from several vendors, must host and maintain the various products, perform manual software upgrades across their NMS estate and still have substantial gaps in their capabilities and visibility.

The NMSaaS technology platform has been developed for scalability and breadth of coverage across Performance, Fault, and Configuration Management. Users of our platform range from School Districts and Governments to a Global Manufacturing Corporation with 25,000 network devices & an International Retailer with 11,000 stores in 13 countries. Find out more at **www.nmsaas.com**

Disclaimer