ManageEngine

BEST PRACTICES

Network Configuration Manager

www.networkconfigurationmanager.com

Overview

ManageEngine Network Configuration Manager offers a simple, comprehensive and elegant solution for easy Network Change and Configuration Management (NCCM). It offers multi-vendor network device configuration, continuous monitoring of configuration changes, configuration backup, notifications on respective changes, detailed operation audit and trails, easy and safe recovery to trusted configurations, automation of configuration tasks and insightful reporting.

This document describes the best practices in setting up and using Network Configuration Manager (NCM) in an enterprise network environment. It is intended to offer guidance to IT administrators when they set up the application in their network environment to manage their network configurations.

- ➤ System requirements of Network Configuration Manager (NCM)
- ➤ Database Management
- ➤ Best practices in configuring Network Configuration Manager
- ➤ Best practices in using Network Configuration Manager

System requirements of Network Configuration Manager

Network Configuration Manager comes bundled with PostgreSQL database and also supports MS SQL database. Network Configuration Manager works on both Windows and Linux. The minimum hardware requirements for Network Configuration Manager are found below:

Parameter	Professional Edition	Enterprise Edition
Processor	2 GHz Dual-core, or more	2.5 GHz Dual-core, or more
RAM	4 GB RAM	16 GB
Hard disk space	100 GB	100 GB hard disk space

The system requirements shown above apply for an environment consisting of 50 devices only. If your environment consists of more than 50 devices, click here.

OS supported	Web-client supported	protocols
Windows ● Windows XP Professional ● Windows XP 64 bit ● Windows Vista ● Windows Server 2008 ● Windows Server 2008 R1 & R2 ● Windows Server 2012 ● Windows Server 2012 R1 & R2 ● Windows 7 ● Windows 8 ● Windows 10 ● Windows Server 16	HTML client requires one of the following browsers** to be installed in the system: ● IE 10 and above (on Windows) ● Latest version of Firefox ● Latest version of Chrome ● Latest version of Safari ● Microsoft Edge ** Network Configuration Manager is optimized for 1024 x 768 resolution and above.	SNMP v1/v2/v3, Telnet, SSH v1/v2, and TFTP
Linux ● RedHat Linux 6.0 and above ● RedHat Linux Advanced Server 2.1 & 3.0 ● RedHat Enterprise Server 2.1 & 3.0 ● Debian version 6.0 and above ● Debian GNU/Linux 3.0 (Woody) ● Mandrake Linux 10.0		

● SUSE 10 and above ● Cent OS 6.0 and above ● Fedora 18 and above ● Ubuntu 12 and above		

The following ports are used by Network Configuration Manager:

Port number	Usage
32000-32999	Wrapper
31000-31999	JVM (To Connect Wrapper)
13306	Database port
22	SCP Port
69	TFTP port
8060	Web Client port
514	Syslog Server port

Learn step-by-step installation of Network Configuration Manager >>
https://download.manageengine.com/network-configuration-manager/ncm-installation-and-getting-started.pdf

Database Management

Database supported: MS SQL 2008, 2012,2014,2016,2017 and PostgreSQL (bundled with Network Configuration Manager). In case, you wish to use MSSQL databases, follow the steps detailed below:

Important Note:

- MSSQL backend is supported from Network Configuration Manager version 5500 only. Earlier versions do not have provision to run with MSSQL
- At present, data migration from MySQL to MSSQL is not supported. You need to start afresh only. This means, if you already using MySQL and wish to switch to MSSQL, the current configurations, settings and other data cannot be migrated to MSSQL.

Steps to Change to MSSQL

1. Stop Network Configuration Manager Server, if running.
2. Open a console and navigate to <deviceexpert_home>/bin directory (as root user).
3. In Windows, execute the batch file "ChangeDB.bat". In Linux, execute the script "sh ChangeDB.sh".
4. The DB Configuration window pops up. Select MSSQL option. Configure the following information:
    - DB Host: The name or the IP address of the machine where MSSQL is installed.
    - Port: The port number in which Network Configuration Manager must connect with the database. Default is 1433.
    - User Name and Password: The user name and password with which Network Configuration Manager needs to connect to the database.
    - Click 'OK'
    - Start Network Configuration Manager. It will run with MSSQL.

Best Practices in configuring NCM

Mandatory Settings

Immediately on installing NCM, launch the web interface and ensure that the following settings are configured.

Configure Mail Server Settings

A valid mail server setting is required for NCM to send various notifications to users.
To configure this, navigate to *Settings>> general Settings >> Mail Server Settings page* and provide values corresponding to the SMTP server running in your network.

Configure Email address of 'admin' user - The fresh installation of NCM has a default user account named 'admin'.

The 'admin' is a 'root' user for NCM. The default email id for this user is admin@adventnet.com. You need to change it to reflect your admin ID. To change this, navigate to *Settings -> User Management -> Users, click the 'Edit User' icon* in the RHS and provide a suitable email address.

Optional Settings

In addition to the above mandatory settings, it is good to carry out the following optional settings:

Configure Proxy Settings

In case, you wish to report any issues encountered with the product to to NCM Support, internet access is required to upload debug logs. If your enterprise network setup is such that you have to go through a proxy server to access the internet, you need to provide the username and password required for internet access. To do this, navigate to **Settings -> General Settings -> Proxy Server Settings** page and configure the settings appropriately.

Configure options for Disaster Recovery - In the rare event of something going wrong with NCM, it is important to have a backup of device configuration to recover from the disaster. NCM provides two utilities to achieve this - backing up the device configuration files or backing up the entire database. Once you have the backup, it is easy to achieve a quick disaster recovery.

Best Practices in Using NCM

After setting up NCM, you can carry out the following:

1. Discover devices

You can discover devices in NCM by going to **Settings->Discovery->Network Discovery.**

SNMP addition: If your devices are SNMP-enabled, use 'Discover Devices' option to discover and your devices to the inventory. This option will help you add multiple devices in one go.

Manual addition: This is a very simple way of device addition - all the you need to provide is the hostname or IP or IP range of devices to be discovered.

Import CSV file: You can also export a CSV file containing IP address, host names, series and model and discover devices.

Refer "Device addition" for more details.

2. Create Credential-Profiles

In practical applications, you may find that the same set of credentials could well be applied 'as they are' to many devices. In such cases, to avoid the cumbersome task of entering the credentials for each device separately, NCM offers the flexibility of creating common credentials and sharing the common credentials among multiple devices. This is called as “Credential Profile”. For more details, refer to the section “CredentialProfiles" in Help Documentation.

3. Backup network configurations

After setting up the devices and providing credentials, the first operation that would be performed is backing up the device configuration. Backup could be done anytime on demand for a single device or a group of devices in bulk. It can also be automated by creating scheduled tasks. Refer "Backup Operations".

4. Group your Devices

When you have a lot of devices in your network infrastructure, grouping them based on some logical criteria will come in handy for carrying out operations in bulk. For example, you may create a group containing all cisco routers, or all cisco switches etc., This would help in carrying out certain common operations with ease.

A group can be created based on some criteria or it could be just a random collection of devices. You can create groups by going to Inventory -> Groups. Refer "Grouping" for more info.

5. Enable Real-time Configuration Change Detection

Unauthorized configuration changes often wreak havoc to the business continuity and hence detecting changes is a crucial task. Detection should be real-time to set things right. NCM enables you to detect configuration changes in real-time.

Many devices generate syslog messages whenever their configuration undergoes a change. By listening to possible to detect any configuration change in the device. NCM leverages this change notification feature real-time change detection and tracking. Refer to the section "Real-time Configuration Change Detection".

6. Define Change Management Rules

Monitoring the changes done to the configuration is a crucial function in Configuration Management. NCM provides convenient change management options. Once the configuration change in a device is detected, it is important that notifications are sent to those responsible for change management. It also provides option to roll-back the changes. NCM helps in sending notifications in the following ways:

- Sending Email
- Sending SNMP Traps
- Generating trouble Tickets
- Sending syslog messages
- Rolling back configurations

7. Enforce Standards by Defining Compliance Policies

Government and industry regulations require IT organizations conform to some standard practices. To become compliant with the regulations such as SOX, HIPAA, PCI, Cisco IOS policy and others, device configurations should conform to the standards specified.

The standards could be anything - ensuring the presence or absence of certain strings, commands or values. NCM helps in automatically checking for compliance to the rules defined. Reports on policy compliance and violations are generated. Refer to the section "Compliance Policies" for more details.

8. Create Scheduled Tasks

If you have a large number of devices, carrying out operations such as backup, upload etc., become monotonous, if they are to be done manually. You might also require to perform certain operations at regular intervals. Execution of these operations can be automated - that is they can be scheduled for execution at the required time automatically. The following operations can be scheduled:

- Configuration backup
- Report generation
- Compliance check
- Configlets
- Device discovery
- Configuration sync
- PCI review

For a specific device or group of devices could be scheduled for execution at a future point of time. These tasks can be scheduled for automatic execution at periodic intervals or for an one-time execution.

9. Automate Configuration Tasks

Quite often, there arises a need to carry out changes to the running configuration of devices and at times, same set of changes need to be applied to multiple devices. Though network administrators can very well edit the configuration manually, the task can prove to be arduous due to the volume of changes and the repetitive nature of the work.

NCM provides a simple solution for this by way of 'Configuration Templates' and 'Scripts'. Refer to the section "Automation using Templates & Scripts" for more details.

10. Label Configurations

NCM helps in backing up device configurations. The backed up configurations are properly versioned and stored in the NCM database. For any version of configuration, you can associate a label - that is, a unique tag. As configuration versions keep on changing, you will have difficulty in remembering the version number of a particular good configuration. To avoid that, you can associate the version with a label for easy identification.

11. Impose Role-Based Access Control

NCM deals with the sensitive configuration files of devices and in a multi-member work environment, it becomes necessary to restrict access to sensitive information. Fine-grained access restrictions are critical for the secure usage of the product.

NCM provides role-based access control to achieve this. By default, you can define any of the following three roles – Administrator, Power User and Operator and define access rules. Refer to the section "Role-based Access Control" of our Help Documentation for details.

12. Assess firmware vulnerabilities

With NCM, you can now identify potential vulnerabilities in your network devices and take action. Network Configuration Manager works in accordance with NIST (National Institute of Standards and Technology) by fetching firmware vulnerability data and correlating it with the network devices which are currently managed in your infrastructure. At present, Network Configuration Manager helps to manage firmware vulnerability for Cisco IOS, Cisco ASA, Cisco Nexus and Juniper devices. Refer "Firmware Vulnerabilities" for more info.

Contact Details

- Write to us at ncm-support@manageengine.com or fill the Support form
- Forum for discussion: https://forums.manageengine.com/network-configuration-manager
- Live online demo: https://demo.networkconfigurationmanager.com/
- Help docs: https://www.manageengine.com/network-configuration-manager/help/
- E books: https://www.manageengine.com/network-configuration-manager/ncm-ebooks.html
- Tech videos: https://www.youtube.com/channel/UCHLusaahd4nS9esD3xBVeUQ