Overview

This document describes the best practices in setting up and using Network Configuration Manager in an enterprise network environment. It is intended to offer guidance to TI administrators when they set up the software for use in their production environment.

Best practices in setting up Network Configuration Manager

Mandatory settings

Immediately on installing Network Configuration Manager, launch Network Configuration Manager web interface and ensure that the following settings are configured:

1. **Configure Mail Server Settings** - A valid mail server setting is required for Network Configuration Manager 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. For more details refer to "**Mail Settings**" in help documentation under the "**Admin Operations**" section.

2. **Configure email address of 'admin' user** - The fresh installation of Network Configuration Manager has a default user account named 'admin'. The 'admin' is the 'root' user for Network Configuration Manager. The default email id for this user is admin@manageengine.com. You need to change it to reflect in your admin id. To change this, navigate to **Settings >> User Management** page, click on the user account to be edited 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:

1. **Configure Proxy Settings** - In case you wish to report any issues encountered with the product to Network Configuration Manager 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. For more details refer to the section on "**Proxy Settings**" in help documentation under the "**Admin**

Operations" section.

2. **Configure options for Disaster Recovery** - In the rare event of something going wrong with Network Configuration Manager, it is important to have a backup of device configuration to recover from the disaster. Network Configuration Manager provides the option of backing up the device configuration files. Once you have the backup, it is easy to achieve a quick disaster recovery. For more details, refer to the "**Disaster Recovery**" section in help documentation.

Best Practices in using Network Configuration Manager

After setting up Network Configuration Manager, you can carry out the following:

Create credential rules

Network Configuration Manager already has a feature know as Credential Profiles, where the user can set up a profile with all the required credential parameters for different protocols and then the credential profile can be associated with the devices and based on the protocol selected in device credentials, appropriate credentials will be applied to the device automatically. To configure this, navigate to **Config Automation >> Credentials >> Credential Rules**. For more details, refer to the "**Credential Rule**" section in help documentation.

Use 'Discovery' to add your devices

If your devices are SNMP-enabled, use 'Discover' option in **Settings > Discovery** page to discover your devices add them to the inventory. This option has several advantages, including the following:

1. You can discover and add many devices at one go.

2. Three simple ways of device addition - you can select any one of these options and click on discover to discover new devices:
(a) IP/ Host Name
(b) IP Range
(c) CSV File Import

For more details, refer to "**Discover Devices**" in help documentation under the "**Adding Devices**" section.

Group your devices

When you have a lot of devices in your environment, grouping the devices based on some logical criteria will come in handy for carrying out operations in bulk. For example, you can create a group containing all Cisco routers or a group containing 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. Refer to the "**Grouping Devices**" section in the help documentation for more details.

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, Network Configuration Manager 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 "**Providing Credentials for Devices**" section in help documentation.

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 in real time to set things right. Network Configuration Manager enables you to detect configuration changes in real time. Many devices generate syslog messages whenever their configuration undergoes a change. By listening to these messages, it is possible to detect any configuration change in the device. Network Configuration Manager leverages this change notification feature of devices to provide real-time change detection and tracking. Refer to the "**Real-time Change detection**" section in help documentation for more details.

Define change management rules

Monitoring the changes done to the configuration is a crucial function in configuration management. Network Configuration Manager 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 rollback the changes. Network Configuration Manager helps in sending notifications in the following ways:

1. Sending email
2. Sending SNMP Traps
3. Using Syslog
4. Generating trouble Tickets

There is also the 5th option of "**Rollback**", which allows you to rollback either to the previous version or to the stable version, whichever selected, whenever a change is made to the associated devices.

And these notifications can be sent whenever there happens a change in

1. Startup or running configuration
2. Startup configuration alone
3 .Running configuration alone

You can define change management rules to suit your needs. Refer to the "**Change management and notification**" section in help documentation for more details.

Enforce standards by defining compliance policies

Government and industry regulations require TI organizations to conform to some standard practices. To become compliant with the regulations such as SOX, HIPAA, PCI, and Cisco IOS, device configurations should conform to the standards specified. The standards could be anything - ensuring the presence or absence of certain strings, commands or values. Network Configuration Manager helps in automatically checking for compliance to the rules defined. Reports on policy compliance and violations are generated. Refer to the "**Companies Policies**" section in help documentation for more details.

Create scheduled tasks

If you have a large number of devices carrying out operations such as backup, upload etc., it becomes 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.

Tasks such as:

1. Configuration backup
2. Report generation and
3. Compliance check

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. Refer to the "**Adding Schedules**" section in help documentation for more details.

Automate configuration tasks

Quite often, there arises a need to carry out changes to the running configuration of devices and at times, the 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. Network Configuration Manager provides a simple solution for this by way of 'configuration templates' and 'scripts'. Refer to the "**Automation using Configlets and scripts**" section in help documentation for more details.

Label configurations

Network Configuration Manager helps in backing up device configurations. The backed up configurations are properly versioned and stored in the Network Configuration Manager 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 remembering the version number of a particular good configuration. To avoid that, you can associate the version with a label for easy identification. For details, refer to the section "**Viewing Device configuration details**" in help documentation.

Impose Role-Based Access Control (RBAC)

Network Configuration Manager 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. Network Configuration Manager provides Role-Based Access Control (RBAC) to achieve this. By default, you can define any of the following two roles - Administrator and Operator and define access rules. Refer to the "**Role-based access control**" section in help documentation for more details.

ZOHO Corp.
4141, Hacienda Drive.,
Pleasanton, CA 94588, USA
Phone: +1-925-924-9500
Fax: +1-925-924-9600