Overview

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

Best Practices in Setting Up NCM

Mandatory Settings

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

1 Configure Mail Server Settings - A valid mail server setting is required for NCM to send various notifications to users. To configure this, navigate to Admin >> General Settings >> Mail Settings page and provide values corresponding to the SMTP server running in your network. For more details refer to the **"Mail Settings"** in Help Documentation.

2 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 Admin -> User Management page, 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:

1. 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 Admin -> Proxy Settings page and configure the settings appropriately. For more details refer to the section on **“Proxy Settings”** in Help Documentation.
2. 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. For more details, refer to the **“disaster recovery”** section in Help Documentation.

Best Practices in Using NCM

After setting up NCM, you can carry out the following

Use 'Discovery' to add your Devices

If your devices are SNMP-enabled, use 'Discover Devices' option to discover and your devices to the inventory. This option has several advantages including the following:

1. You can discover and add many devices at one go.
2. 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.

For more details, refer to the **“Discover Devices”** section in Help Documentation.

Group your Devices

When you have 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 may 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 section **"Grouping Devices"** in the Help Documentation for 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, 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 **“Credential Profiles"** 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 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 these messages, it is possible to detect any configuration change in the device. NCM leverages this change notification feature of devices to provide real-time change detection and tracking. Refer to the section **"Real-time Configuration Change Detection"** for more details.

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:

1. Sending Email
2. Sending SNMP Traps
3. Generating trouble Tickets

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 section **"Change Management & Notification"** for more details.

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, CISP, PCI, Sarbanes-Oxley 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 **"Companies Policies"** for more details.

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.

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 section **"Schedules"** 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, 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.

Label Configurations

NCm helps in backing up device configurations. The backedup 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. For details, refer to the section **"Viewing Device Details"** in Help Documentation.

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.