Page Title: adding-devices-for-network-configuration-management

On this page

Adding Devices for Network Configuration Management

In Motadata AIOps, the process of adding devices for Network Configuration Management (NCM) is integrated with the discovery of the network device for monitoring. When you complete the discovery of a network device

or a

wireless device

in Motadata AIOps, the device is not only configured as a

Monitor

but it is also setup in the

NCM device inventory

Any network device that is configured as a monitor in Motadata AIOps will be listed in the

NCM device inventory

but that does not necessarily mean that it is enabled for configuration management.

The monitor will be available for configuration management only when the

Enable NCM

option is enabled for that monitor either during device discovery or later on through the the

Manage NCM Status

option in the

NCM device inventory

.

Let us understand the two ways how the device can be enabled for Network Configuration Management in Motadata AIOps.

1. Enable NCM during Device Discovery

â€‹

To enable a network device for Network Configuration Management, you can opt to configure the device as an NCM device during the discovery process of that device for monitoring. This is facilitated through the discovery profile configuration, which includes an option to

Enable NCM

. By using this toggle button, you can initiate the discovery of the device as an NCM device after it is configured as a monitor in Motadata AIOps.

The eligibility of a monitor for network configuration management depends on the status of the

Enable NCM

button during discovery. If the

Enable NCM

button is activated, a specific discovery runs in the back end to enable NCM for that monitor. Once the initial backup for this monitor is successfully completed, it is available for analysis in the

NCM Explorer

In case the

Credential Status

for a particular monitor listed in NCM device inventory shows as

Failed

, it signifies that the discovery for monitoring is completed, but the NCM discovery encountered credential-related failures. Administrators can pinpoint the exact stage of failure by clicking on

Failed

under the column

Credential Status

and subsequently update the credentials accordingly.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

The list of all the created discovery profiles is now displayed on this screen.

Steps to Enable NCM during Discovery

â€‹

Refer

Adding Network devices for Monitoring

for details on how to enable a network device for Network Configuration Management. The same steps need to be followed while creating a credential profile for a wireless device to enable then for Network Configuration Management.

2. Enable NCM from Device Inventory

â€‹

Once a network device is successfully discovered and configured as a Monitor, it becomes a part of the NCM device inventory. In case you did not opt for the

Enable NCM

option during the discovery of the network device as explained in the first option but later on you want to enable NCM for that device in Motadata AIOps, you can do it from the NCM Device Inventory.

If the "Enable NCM" button is deactivated during device discovery, the device remains part of the NCM device inventory but is not eligible for network configuration management. To enable NCM

functionalities for such a device, administrators can click on the "

Manage NCM Status

" button in the NCM device inventory screen. However, the device will only be present in the NCM Explorer and accessible for other functionalities after the first backup is completed.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, select

Network Config Settings

. Select

Device Inventory

. The list of all the network monitors is displayed on the screen.

Steps to Enable NCM from Device Inventory

â€‹

Here, you can see a column

Manage NCM Status

with a toggle button. You can switch ON the toggle button to enable the network configuration management for that device.

Once you switch the toggle button ON, the monitor will now be enabled for network configuration management and the NCM discovery for that device will run in the backend. Once the initial backup for this device is successfully completed, it is available for analysis in the

NCM Explorer

The integration of NCM discovery with discovery for monitoring ensures a smooth transition from monitoring to comprehensive network configuration management in Motadata AIOps. Administrators

gain fine-grained control over NCM settings, allowing them to harness the full potential of configuration management, backup, and restore capabilities.

Page Title: backup-restore-ncm-devices

On this page

Backup and Restore for NCM device

Efficient backup and restore processes are integral components of Network Configuration Management (NCM) in Motadata AIOps. This section outlines how administrators can schedule backups, attach storage profiles, and restore configurations for individual devices or perform bulk restores.

NCM Device Backup

â€‹

Go to Menu. Select

Settings

. After that, select

Network Config Settings

. Select

Device Inventory

. Navigate to the device for which you want to schedule the backup. From the

Actions

tab, select

Schedule Backup

.

A tab to schedule the backup is displayed.

Enter the details in the scheduler to schedule the backup as per your requirement.

Select

Schedule

to schedule the Backup as per the details you specified.

Scheduling Backup to External Server

â€‹

Apart from the local NCM device backup, you can also ensure data redundancy by taking the backup on a external server. Attach a

Storage Profile

to the NCM device if you wish to store backups externally.This external server can be configured in addition to local backups on the Motadata AIOps server.

Go to Menu. Select

Settings

. After that, select

Network Config Settings

. Select

Device Inventory

. Navigate to the device for which you want to attach Storage Profile. From the

Actions

tab, select

Attach Storage Profile

.

Next, select the Storage Profile that you wish to assign to the NCM device. Once the scheduled backup for the NCM device is completed, the same backup will also be taken in the

Storage Destination

mentioned in the

Storage Profile

.

Bulk Backup of NCM Devices

â€‹

You can backup the devices in bulk from the NCM Explorer instantly.

Select the devices that you want to backup using the checkbox in front of all the devices in the NCM explorer as shown below. In case you want to take backup of all the devices instantly, select the checkbox at the top of all the devices as shown in the diagram below.

Once you have selected the devices that you want to backup, select the

button at the top of the screen besides the

Compare

button and select

Backup Now

.

The Backup process will start in the backend and you can view the status of the backup of all devices in the

Last Backup Status

column.

NCM Device Restore

â€‹

Go to Menu. Select

NCM

. After that, select the tab

Explorer

. Navigate to the device for which you want to restore the configuration to a previous version. From the

Actions

tab, select

Restore

.

The system prompts you to select the file you want to restore to the running config of the NCM device.

Field

Description

Config File Type

Specify the source configuration file type (Running config or Startup config) from which you want to restore the configuration.

Version

Select the version of the config file you wish to restore.

Bulk Restore of NCM Devices

â€‹

You can restore the devices in bulk from the NCM Explorer instantly.

Select the devices that you want to restore using the checkbox in front of all the devices in the NCM explorer. In case you want to restore all the devices instantly, select the checkbox at the top of the list of NCM devices in the NCM Explorer.

Once you have selected the devices that you want to backup, select the

button at the top of the screen besides the

Compare

button and select

Restore

.

Select

Baseline

if you want to restore the running config of all the NCM devices to the baseline version of the

running config.

Select

Latest Version

if you want to restore the running config of the NCM devices to the latest version of the running config.

After selecting the

Config File Type

, select the

Restore

button to bulk restore the NCM devices as per your selection.

NCM in Motadata AIOps provides a user-friendly interface for scheduling backups and restoring configurations. Whether working on individual devices or streamlining bulk restores, administrators gain precise control over version selection and configuration file types, ensuring the integrity of network configurations.

Page Title: firmware-upgrade

On this page

NCM Firmware Upgrade

Firmware Upgrade in Motadata AIOps NCM

â€‹

A firmware upgrade for a network device involves updating the device's embedded software to improve functionality, enhance security, or fix bugs.

Motadata AIOps NCM (Network Configuration Manager) supports end-to-end firmware upgrades for network devices using associated

NCM device templates

. These templates contain the sequence of commands required to perform the firmware upgrade.

Enabling Firmware Upgrade

â€‹

Enabling Firmware Upgrade in the NCM Device Template:

Once a device is available in the

NCM Explorer

and the

Firmware Upgrade

option is enabled in the corresponding

NCM device template

, the

Firmware Upgrade

button will be enabled for that device in the NCM Explorer.

Navigation

Navigate to the

NCM Explorer

. Click on the

Firmware Upgrade

option against the device to initiate the upgrade process.

Firmware File Selection:

A pop-up window will appear asking for the firmware upgrade file.

You can select an existing firmware file or upload a new firmware upgrade file through the UI.

Starting the Upgrade:

Once the firmware file is selected or uploaded, click the

Upgrade

button to start the upgrade process.

The progress and status of the upgrade will be monitored by the system.

Completion and Status:

After the upgrade is successfully completed, the

Last Performed Action

column in the NCM Explorer will display

Firmware Upgrade Successful

.

If any errors occur during the upgrade, they will be indicated in the

Last Performed Action

column. Users can click on the action to view detailed information about where the upgrade process failed.

Firmware Upgrade Option Unavailable

â€‹

If the

Firmware Upgrade

option is not available for a device, this typically indicates that:

The firmware upgrade option is not enabled for the device in the NCM Device Template.

Motadata AIOps relies on the commands specified in the associated NCM device template to perform the upgrade. If these commands are missing, the firmware upgrade option will not be enabled for that device. Users must ensure that the commands related to the firmware upgrade are included in the template.

Working with NCM Device Templates

â€‹

Pre-Defined NCM Device Templates

â€‹

If the device is associated with a pre-defined (inbuilt) device template, you cannot directly edit the template to add the firmware upgrade commands.

In this case, you need to

Clone

the existing template, add the necessary firmware upgrade commands, and then associate the cloned template with the device.

The required commands for the firmware upgrade may already be available in the built-in device template attached to the device. If so, the firmware upgrade option will be enabled without further action.

Custom NCM Device Templates

â€‹

If the device is associated with a custom-created template, you can directly add the necessary commands for the firmware upgrade if not already added beforehand.

After adding the commands, save the template to enable the firmware upgrade option for the NCM device.

By following these guidelines, users can effectively manage and execute firmware upgrades for their network devices within Motadata AIOps, ensuring their network infrastructure remains up-to-date and secure.

Now, let us look into how to

add the firmware upgrade commands

to a

custom created NCM device template

.

Page Title: firmware-upgrade-commands-ncm-template

On this page

Adding Firmware Upgrade Commands to a Device Template

Motadata AIOps provides a comprehensive solution for managing firmware upgrades on network devices. This feature enables you to define and execute a sequence of commands necessary to upgrade a device's firmware, ensuring enhanced performance and security. The commands are configured within the associated NCM device template, which dictates the entire firmware upgrade process. Below, we outline the steps involved in configuring firmware upgrade commands, followed by an example specific to upgrading the firmware of a Cisco device.

You can add firmware upgrade commands to a NCM device template in any of the following situations:

When you create a new NCM device template . Go to Menu. Select

Settings

. After that, select

Network Config Settings

. Select

Device Template

and then select

Create Template

button to create a custom template.

You can clone a pre-defined device template in the NCM device template screen and add firmware upgrade commands to it.

You can add the firmware upgrade commands to an already created custom NCM device template.

Firmware Upgrade Commands Screen

â€‹

This screen allows administrators to define the commands necessary for upgrading the firmware on specific network devices. The fields available on this screen ensure that every aspect of the firmware upgrade process is carefully managed.

Field

Description

Command

Specify the command to be executed during the firmware upgrade process. This customization allows you to tailor the firmware upgrade sequence to the specific requirements of your network device.

Timeout (ms)

Define the time Motadata AIOps should wait to receive output after command execution. The operation will timeout if no output is received within the specified time.

Prompt

Choose the prompt that Motadata AIOps should identify after executing the command. This ensures precise execution of the subsequent

Prompt Command

.

Prompt Command

Select the specific

Prompt Command

to be executed in the command prompt after the prompt identified in the previous field.

Result Pattern

Define the regex pattern to parse the output of the command and extract specific data required for the upgrade process.

Expected Value

Specify the expected value that the command output should match. This field is used to validate the

output against the expected result, ensuring the command executed successfully before proceeding to the next step. If the output does not match the expected value, the process can be flagged for review or correction.

After specifying the initial firmware upgrade commands, administrators can add commands for additional operations such as getting the current firmware image, verifying the available free space, or backing up the existing firmware image. Below is an example illustrating the configuration of firmware upgrade commands for a Cisco device.

Example: Firmware Upgrade for a Cisco Device

â€‹

Consider a scenario where you need to upgrade the firmware of a Cisco device using a specific sequence of commands.

Step 1: Get Current Firmware Image

â€‹

Enter

terminal length 0

in the

Command

field to prepare the terminal for command execution.

Set a

Timeout (ms)

of

2000

.

Choose

#

as the

Prompt

and select

No Command

from the

Prompt Command

dropdown.

Add

show version

as the

Command

to retrieve the current firmware version.

Define the

Result Pattern

as

System\s+image\s+file\s+is\s+\"\S+\:(\S+)"

to extract the current firmware image file.

Step 2: Get Configuration Register Info

â€‹

Enter

show version

in the

Command

field to fetch the configuration register information.

Set a

Timeout (ms)

of

2000

.

Choose

#

as the

Prompt

and select

No Command

from the

Prompt Command

dropdown.

Define the

Result Pattern

as

Configuration register is 0xF

and set the

Expected Value

as

Configuration register is 0xF

.

Get Free Space

â€‹

Command

:

dir flash:

Timeout (ms)

:

2000

Prompt

:

#

Prompt Command

:

No Command

Result Pattern

:

\d+\s*bytes\s*total\s*\((\d+)\s+bytes\s*free\)

This command checks the available free space on the device to ensure sufficient storage for the new firmware image.

Step 3: Backup Existing Firmware Image

â€‹

Enter

copy flash: tftp:

 in the

Command

 field to initiate the backup process of the existing firmware image.

Set a

Timeout (ms)

 of

2000

.

Choose

]?

 as the

Prompt

 and select

No Command

from the

Prompt Command

dropdown.

Use the macro

&[FirmwareDeviceBackupFileName]

to specify the backup filename.

Continue adding the commands required to complete the backup process, including specifying the TFTP server address and the file name.

Step 4: Transfer Firmware Image to Device

â€‹

Enter

copy tftp: flash:

in the

Command

field to begin transferring the new firmware image to the device.

Set a

Timeout (ms)

of

2000

.

Choose

]?

as the

Prompt

and select

No Command

from the

Prompt Command

dropdown.

Use the macros

&[TransferProtocolServerAddress]

and

&[TransferFileName]

to specify the TFTP server and file name for the new firmware image.

Step 5: Update Boot Variable (Mount)

â€‹

Enter

config terminal

in the

Command

field to access the configuration mode.

Set a

Timeout (ms)

of

2000

.

Choose

#

as the

Prompt

and select

No Command

from the

Prompt Command

dropdown.

Add

no boot system

followed by

boot system flash &[TransferFileName]

to update the boot variable with the new firmware image.

End the command sequence with

end

.

Step 6: Verify Uploaded Firmware Image Integrity

â€‹

Enter

verify flash:&[TransferFileName]

in the

Command

field to verify the integrity of the uploaded firmware image.

Set a

Timeout (ms)

of

600000

.

Choose

#

as the

Prompt

and select

No Command

from the

Prompt Command

dropdown.

By following these steps, you can successfully configure the firmware upgrade commands for a Cisco device. This is just one example; similar steps can be followed for other devices by customizing the commands as per their requirements.

Page Title: ncm-device-inventory

On this page

NCM Device Inventory

In Motadata AIOps, the NCM Device Inventory serves as the central hub for managing and monitoring devices configured for Network Configuration Management (NCM). This inventory provides crucial information about network monitors setup in Motadata AIOps, offering administrators a comprehensive overview and control over their network configurations.

Overview

â€‹

The NCM Device Inventory provides a detailed list of all the network devices, including routers, switches, firewalls, and core infrastructure components, configured as monitors in Motadata AIOps. This helps administrators in monitoring, managing, and ensuring the integrity of configurations across diverse vendor environments.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, select

Network Config Settings

. Select

Device Inventory

. The list of all the network monitors is displayed on the screen.

Device Inventory Screen

â€‹

The following fields are available on the Device Inventory screen:

Field

Description

Device

Displays the name or identifier of the network device configured as a monitor in Motadata AIOps. It helps administrators quickly identify and locate specific devices in the inventory.

IP/Host

Specifies the IP address associated with the network device. This information aids in network identification and ensures accurate communication with the device.

System OID

Represents the System Object Identifier (OID) of the network monitor. The System OID uniquely identifies the device.

Vendor

Indicates the vendor or manufacturer of the network monitor. It helps in categorizing and organizing devices based on their respective manufacturers.

Template

Indicates the NCM device template assigned to the NCM device based on its OID. The template outlines guidelines for backup, restore, and synchronization processes, ensuring standardized configuration management.

Manage NCM Status

This field includes a toggle button that allows administrators to manually enable or disable Network Configuration Management (NCM) functionalities for the specific device. When enabled, the device undergoes NCM discovery and becomes accessible for related functionalities. When disabled, the Backup for the NCM device is stopped.

Credential Status

Provides insights into the credential-related status for enabling NCM for a device. It indicates whether the credentials used for discovery were successful or if failures occurred at a specific stage

of setting up the device as a NCM device. Clicking on the status allows administrators to review and update credentials if needed.

Scheduler

Indicates the scheduler details for the backup of the NCM device.

Type

Specifies the type of the network device, such as router, switch, firewall, or other core infrastructure components.

Actions

Refer the content below to read about the actions available for a NCM device

Actions in NCM Device Inventory

â€‹

The following actions are available for a device listed in NCM device inventory:

Actions

Description

Schedule Backup

This action allows administrators to schedule regular

backups

for the configurations of the NCM device. By defining a backup schedule, users ensure that critical configuration files, including startup and running configs, are periodically saved.

Update Credential

This action provides administrators the ability to modify and update the credential profile associated with the NCM device. If there are changes in authentication details or if the initial credential setup encounters issues, administrators can use this action to ensure communication with the device.

Update Template

This action allows administrators to update the device template assigned to the NCM device. The device template

outlines the configuration management guidelines, including backup and restore processes.

Attach Storage Profile

This action enables administrators to associate a storage profile with the NCM device. This profile defines the storage destination for configuration backups, allowing users to save copies of configuration files externally. By attaching a storage profile, ensure secure storage, especially when backups need to be stored on an external server apart from the local Motadata AIOps server.

Enabling Network Configuration Management from Device Inventory

â€‹

Enable NCM from Device Inventory:

If the device is not enabled for NCM during discovery for monitoring, administrators can switch ON the

Manage NCM Status

button in the NCM Device Inventory. This step activates the NCM discovery for the device, and functionalities become accessible after the initial backup.

Page Title: ncm-device-template

On this page

NCM Device Template

In the Device Template section, administrators can manage the configurations associated with NCM devices. Each NCM device is assigned a unique template based on its Object Identifier (OID). These templates serve as guidelines for executing backup, restore, and synchronisation operations on the startup and running configurations of network devices.

The NCM device template, assigned based on the sysoid of the device, plays a pivotal role in enabling essential functions such as backup, restoration, and synchronisation of configuration files. If, for any reason, a template is not automatically assigned to an NCM device, administrators have the option to manually add the template, either a pre-defined template or a custom created template from the

NCM Device Inventory

.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, select

Network Config Settings

. Select

Device Template

. The list of all the NCM Device Templates is displayed on the screen.

Device Template Screen

â€‹

Field

Description

Template

The name of the template used to identify the template.

Vendor

The vendor for which the template is created.

OS Type

The OS type of the network device for which the template is created.

Devices

The number of monitors to which the template is currently mapped. Select the number in this field to view the monitors to which the Device Template is assigned

Actions

Select

to display permissible actions for the Device Template:

-

Edit

: This button is used to edit a device template.

-

Clone

: This button is used to clone the device template.

-

Download XML/JSON

: This button is used to download the device template in the XML/JSON format.

-

Delete

: This button is used to delete a template from Motadata AIOps.

Create Custom Template

â€‹

Motadata AIOps empowers administrators with the flexibility to create custom templates tailored to specific NCM devices. This customization ensures that you can create a custom template when any of the pre-defined templates are not mapped to a NCM device .

When creating a custom template, administrators can specify details for backup running configuration, backup startup configuration, sync config, and restore config.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, select

Network Config Settings

. Select

Device Template

and then select

Create Template

button to create a custom template.

Create Custom Template Screen

â€‹

This screen empowers administrators to define custom templates for specific NCM devices, ensuring precise control over configurations. Here's a breakdown of the fields on this screen:

Field

Description

Device Template Name

Enter a distinctive name for your template, providing an easily identifiable reference for configuration management.

Description

Add a brief description to your template, offering insights into its purpose or any specific details relevant to the configuration guidelines.

Vendor

Specify the name of the device vendor for which you are creating the template, aiding in categorization.

OS Type

Enter the Operating System name of the targeted device, ensuring that the template aligns with the specific requirements of the device's OS.

Delay Time (ms)

Customize the delay time in milliseconds, dictating the interval Motadata AIOps should wait after executing a command and before reading the output. This feature enhances the execution of commands. The default time is set at 1000 ms, but you can adjust it to suit your needs.

Protocol

Choose the preferred protocol for backup file transfer. Under the selected protocol, define backup commands to ensure file transfer during configuration processes.

Upon selecting your preferred protocol in the custom template creation process, the next step involves specifying operations such as

Backup Running Configuration

,

Backup Startup Configuration

,

Backup Restore Configuration

,

Backup Sync Configuration

, and

Get Hardware Information

. The default display is for

Backup Running Configuration

, and by selecting the

Add Operation

button, you can add operations based on your specific requirements.

Under each operation, you have the flexibility to define commands relevant to the selected operation, serving as guidelines for Backup, Restore, and Sync Operations. Here's an overview of the key fields for specifying commands:

Field

Description

Command

Specify the command to be executed based on the selected operation. This customization allows you to tailor commands to your precise configuration needs. Apart from the commands, you can also use a set of pre-defined

macros

in this field to provide inputs to the template.

Timeout(ms)

Define the time Motadata AIOps should wait to receive output after command execution. The operation will timeout if no output is received within the specified time.

Prompt

Choose the prompt that Motadata AIOps should identify after executing the command. This enables precise execution of the subsequent

Prompt Command

specified in the next field. In case you want to add a prompt that is not already available in the list, you can do so by clicking on

option

Prompt Command

Select the specific

Prompt Command

to be executed in the command prompt after the prompt identified in the previous field. Refer

Prompt Commands

to understand in detail about the prompt commands available in Motadata AIOps while creating a template.

Select

to add subsequent commands under the operation you have selected.

Select the

Add Operation

button to add operations for

Backup Startup Configuration

,

Backup Restore Configuration

, and

Backup Sync Configuration

as per your requirement.

Field

Description

Mapped Devices

Select the network devices to associate with the template. The configured commands within the template will be utilized for backup, restore, and synchronization actions on the chosen network devices. This mapping ensures consistency in configuration management across devices.

Examples of Creating a Custom Template

â€‹

Backup of Running Config file of a Cisco device to a TFTP server

â€‹

Consider a scenario where you need to back up the running configuration file of a Cisco device to a TFTP server.

We will map the process of creating a custom template with how the actual commands are executed in the backend. Let us look into the creation of the custom template step by step:

After you click on the

Create Template

button, enter the details for the

Device Template Name

,

Description

,

Vendor

,

OS Type

,

Delay Time(ms)

as per the device for which you are creating the template. After that select the protocol which in our case would be the

TFTP

protocol.

Under the

Backup Running Configuration

, you need to enter the details for the

Command

,

Timeout(ms)

,

Prompt

, and

Prompt Command

 fields. Let us understand one by one what details need to be entered here.

Enter

copy running-config tftp:

 in the

Command

 field and an appropriate

Timeout

. Select

]?

 from the

Prompt

 dropdown and

No Command

 from the

Prompt Command

 dropdown.

The above step is equivalent to the following configuration in the backend:

This means that AIOps will enter the command

copy running-config tftp:

 on the terminal and press 'Enter' and then look for the prompt

]?

 to execute the

Prompt Command

which is

No Command

in this case.

Now, AIOps will look for the prompt

]?

to enter the next set of commands as per the configuration mentioned in the template. After entering the command mentioned in the step 3 and pressing Enter, the terminal prompts 'Address or name of the host []?'. Thus, we specified

]?

as the

Prompt

in step 3 as this would enable AIOps to identify which prompt to look for before entering the next command.

Click

to enter the next set of backup configuration commands. Now, we need to provide the IP address of the TFTP server as per the prompt received after the command executed in step 3. Enter the macro

&

[TransferProtocolServerAddress]

in the

Command

field to pass the IP address of the TFTP server through the macro

&

[TransferProtocolServerAddress]

and an appropriate

Timeout

. Select

]?

from the

Prompt

dropdown and

No Command

from the

Prompt Command

dropdown.

The above step is equivalent to the following configuration in the backend:

This means that AIOps will enter the command

&

[TransferProtocolServerAddress]

to pass the IP address of the TFTP server to the terminal, press 'Enter', and then look for the prompt

]?

to execute the

Prompt Command

which is

No Command

in this case.

Click

to enter the next set of backup configuration commands. Now, we need to provide the Filename of the running config on TFTP server where the backup will be stored. Enter the macro

&

[TransferFileName]

in the

Command

field to pass the filename of the running config on the TFTP server through the macro

&

[TransferFileName]

and an appropriate

Timeout

. Select

#

from the

Prompt

dropdown and

No Command

from the

Prompt Command

dropdown.

The above step is equivalent to the following configuration in the backend:

This means that AIOps will enter the command

&

[TransferFileName]

to pass the filename of destination running config file on the TFTP server to the terminal, press 'Enter', and then look for the prompt

#

to execute the

Prompt Command

which is

LF

in this case.

In this way, you can create a custom template to take backup of the running config file of a Cisco device to a TFTP server. Note that this is just an example to understand the creation of a custom template as the template for Cisco device is available in Motadata AIOps by default.

Restoring a Running Config file of a Cisco device from a TFTP server

â€‹

Consider a scenario where you need to restore the running configuration file of a Cisco device from a TFTP server.

We will map the process of creating a custom template with how the actual commands are executed in the backend. Let us look into the process of configuring the commands for restoring the backup step by step in the same template as we created in the first example:

We have already provided the details to create the custom template for the backup of running configuration in the 1st example. Now let us add the details to restore the running config from the TFTP server in the same template.

Click on the

Add Operation

button and select the

Backup Restore Configuration

to add commands for the backup of the running config from the TFTP server. Under the

Backup Restore Configuration

, you need to enter the details for the

Command

,

Timeout(ms)

,

Prompt

, and

Prompt Command

fields. Let us understand one by one what details need to be entered here.

Enter

copy tftp: running-config

in the

Command

field and an appropriate

Timeout

. Select

]?

from the

Prompt

dropdown and

No Command

from the

Prompt Command

dropdown.

The above step is equivalent to the following configuration in the backend:

This means that AIOps will enter the command

copy tftp: running-config

on the terminal and press 'Enter' and then look for the prompt

]?

to execute the

Prompt Command

which is

No Command

in this case.

Now, AIOps will look for the prompt

]?

to enter the next set of commands as per the configuration mentioned in the template. After entering the command mentioned in the step 3 and pressing Enter, the terminal prompts 'Address or name of the host []?'. Thus, we specified

]?

as the

Prompt

in step 3 as this would enable AIOps to identify which prompt to look for before entering the next command.

Click

to enter the next set of restore configuration commands. Now, we need to provide the IP address of the TFTP server as per the prompt received after the command executed in step 3. Enter the macro

&

[TransferProtocolServerAddress]

in the

Command

field to pass the IP address of the TFTP server through the macro

&

[TransferProtocolServerAddress]

and an appropriate

Timeout

. Select

]?

from the

Prompt

dropdown and

No Command

from the

Prompt Command

dropdown.

The above step is equivalent to the following configuration in the backend:

This means that AIOps will enter the command

&

[TransferProtocolServerAddress]

to pass the IP address of the TFTP server to the terminal, press 'Enter', and then look for the prompt

]?

to execute the

Prompt Command

which is

No Command

in this case.

Click

to enter the next set of backup configuration commands. Now, we need to provide the Filename of the running config on TFTP server where the backup file is stored. Enter the macro

&

[TransferFileName]

in the

Command

field to pass the filename of the running config on the TFTP server through the macro

&

[TransferFileName]

and an appropriate

Timeout

. Select

]?

 from the

Prompt

 dropdown and

No Command

 from the

Prompt Command

 dropdown.

The above step is equivalent to the following configuration in the backend:

This means that AIOps will enter the command

&

[TransferFileName]

 to pass the filename of backup running config file on the TFTP server to the terminal, press 'Enter', and then look for the prompt

]?

 to execute the

Prompt Command

 which is

No Command

 in this case.

Click

 to enter the next set of backup configuration commands. Now, we need to provide where we need to restore the backup from the TFTP server. Enter

running-config

 in the

Command

field to specify that the backup needs to be restored on the running config file and specify an appropriate

Timeout

. Select

#

from the

Prompt

dropdown and

LF

from the

Prompt Command

dropdown.

The above step is equivalent to the following configuration in the backend:

This means that AIOps will enter the command

running-config

in the

Command

field to specify that the backup needs to be restored on the running config file, press 'Enter', and then look for the prompt

#

to execute the

Prompt Command

which is

LF

in this case.

The NCM Device Template section in Motadata AIOps offers a comprehensive approach to network configuration management, allowing administrators to tailor configurations to specific device

requirements. Whether utilizing default templates or creating custom ones, this functionality ensures the smooth execution of backup, restore, and sync operations in NCM devices.

Page Title: ncm-explorer

On this page

NCM Overview & Explorer

Explore the powerful features of the NCM Explorer, your centre for effective network configuration management. Designed to streamline Network Configuration Management operations and enhance visibility, the NCM Explorer brings your network devices into focus.

In the NCM Explorer, you'll find a comprehensive list of devices discovered as NCM devices, offering a one-stop solution for your network configuration needs. After the initial backup, devices become accessible in NCM Explorer, enabling a range of actions for efficient network configuration management.

NCM Overview

â€‹

Take a deep dive into a detailed visual representation of your Network Configuration Management (NCM) landscape with the

NCM Overview

tab. This dedicated tab within the

NCM

provides a snapshot of essential details for effective network configuration management.

Navigation

â€‹

Go to Menu. Select

NCM

. The

Overview

is selected by default.

NCM Explorer

â€‹

Navigation

â€‹

Go to Menu. Select

NCM

. After that, select the tab

Explorer

.

NCM Explorer Screen

â€‹

The following fields are available on the NCM Explorer screen:

Field

Description

Device

The name of the device.

IP

The IP of the device.

Device Type

The type of the device.

Current Version

The current version of running config of the device.

Config Conflict

This column shows the status of synchronisation between Running Config and Startup Config files of the device. In case there is a conflict between running and startup config files, the status is shown as

Conflict Detected

. Select

Conflict Detected

 to analyse the comparison between the two files.

Last Performed Action

The last performed action for the device.

Last Backup Status

The status of the last backup, whether

Successfull

 or

Failed

.

Last Backup Time

The time of the last successful backup for the device.

Actions

Refer the content below to understand the actions available for the NCM device.

Actions on NCM Explorer

â€‹

Select

 under the

Actions

 column to display the permissible actions for the NCM device in the NCM Explorer. The following actions are available for the device:

Backup Now

â€‹

Select this option to instantly take the backup of the NCM device.

Compare

â€‹

Empower yourself with the 'Compare' functionality, allowing side-by-side comparisons of startup and running configurations across different devices and versions. Easily spot inserted, modified, or deleted lines through color-coded highlighting.

Download Backup

â€‹

Select this option to download the config files of the NCM device on your system locally.

Set as Baseline

â€‹

Select this option to configure a running config of the NCM device as the baseline configuration. This helps you to identify a standard set of configurations for that device that you can restore when needed. Establish a standardized configuration across your network devices by designating a specific backup version as the baseline. The running config setup as baseline won't be deleted even if it qualifies to be deleted based on the

data retention settings

SSH Terminal

â€‹

Select this option to open an SSH terminal for the selected NCM device. This feature allows you to establish a secure SSH connection to the device directly from the NCM Explorer, enabling real-time command-line interactions.

View

â€‹

Select this option to take a deep dive into detailed insights about each NCM device.

Sync

â€‹

Select this option to sync the running config and startup config files of the NCM device.

Restore

â€‹

Select this option to restore the running config file from the backups available for that NCM device.

NCM Device Details

â€‹

By clicking on a device name in the NCM Explorer, you can access a comprehensive overview of the device, neatly divided into two important tabs:

Device Details

and

Action History

. This structured layout makes it easy to view and manage all relevant information about your network devices.

Accessing Device Details

â€‹

To access the device details, navigate to the NCM Explorer screen and click on the device name. This action will take you to a detailed view of the device, which includes the following tabs:

Device Details

Hardware Details

Action History

Device Details

â€‹

On the

Device Details

tab, you can view basic information about the device, such as OS Type, Series, Model Number, OID, Template, and more.

Additionally, this tab provides details about all versions of the running configuration and startup configuration files, along with their contents. You have the option to:

Download a specific config file.

Set a running config file as the baseline.

This tab is essential for understanding the current state and history of your device configurations.

Hardware Details

â€‹

The

Hardware Details

tab provides specific information related to the hardware of the NCM device. Here, you can find details such as the

CPU

,

Flash Size

,

CPU Revision

,

Configuration Register

,

MAC Address

,

DRAM Size

and more.

To fetch these hardware details, click on the

Get Hardware Details

option under the

Actions

column for the desired device in the NCM Explorer. This functionality helps in obtaining and reviewing critical hardware specifications directly within the platform.

Ensure the

Get Harware Details

commands are available in the

NCM Device Template

associated with the NCM device for which you are trying to retrieve the hardware details. In case the commands are not available in the template, you can add the commands for the same to the template.

Working with NCM Device Templates

If the device is associated with a pre-defined (inbuilt) device template, you cannot directly edit the template to add the hardware detail commands.

In this case, you need to

Clone

the existing template, add the

Get Hardware Details

commands, and then associate the cloned template with the device.

The required commands for retrieving the hardware details may already be available in the built-in device template attached to the device. If so, the

Get Hardware Details

will be enabled without further action.

Custom Device Templates

If the device is associated with a custom-created template, you can directly add the necessary commands if not already added beforehand.

After adding the commands, save the template to enable the

Get Hardware Details

option for the NCM device.

Action History

â€‹

The

Action History

tab offers a log of all actions performed on the NCM device. This includes actions such as the Last performed backup, Last executed runbook, Restoration of a particular backup file to the running configuration and more.

This tab is invaluable for tracking and auditing changes made to your network devices, ensuring that all actions are documented and easily retrievable for future reference.

By leveraging these tabs in the NCM Explorer, administrators can gain a holistic view of each network device, manage configurations effectively, and ensure the stability and security of their network infrastructure.

Filter Network Devices

â€‹

Effortlessly navigate through your network devices using the filtering options available on the panel present on the left side of the screen. Tailor your view and focus on the devices that matter most to you with the help of important filters such as the

Backup Status

,

Device Type

,

Vendor

,

OS Type

,

Tags

, and more.

Versioning

â€‹

Track configuration changes over time through versioning. Each backup creates a new version,

providing insights into the evolution of configurations. Manage versions based on your data retention settings.

The NCM Explorer in Motadata AIOps provides a user-friendly and powerful interface for network administrators to navigate, analyze, and optimize network configurations. Whether you're ensuring adherence to standards, troubleshooting issues, or maintaining historical records, the NCM Explorer is your go-to tool for efficient network configuration management.

Page Title: ncm-macros-and-prompts

On this page

Macros and Prompt Commands for Custom Template

Introduction to Macros in NCM Device Template

â€‹

Macros in Motadata AIOps serve as dynamic placeholders that facilitate customization and automation within the platform. These placeholders are substituted with specific values during execution, allowing users to create versatile and adaptable configurations. Each macro represents a predefined parameter or value that plays a crucial role in various operations, such as configuration management, and file transfers.

Understanding and leveraging these macros is essential for tailoring Motadata AIOps to specific network environments and requirements. Below is an overview of the key macros available in Motadata AIOps and their functions.

Key Macros and their Functions

â€‹

Macros

Description

&

[Enter]

This macro represents the Enter key or newline character ("\n"). It is essential for simulating the press of the Enter key, which is often required for navigating command-line interfaces and executing commands.

&

[TransferFilePath]

This macro represents the file path used during file transfer operations. It is particularly useful when specifying the location of files being transferred within the platform.

&

[TransferProtocolServerAddress]

This macro denotes the server address or host used during transfer protocol operations. It specifies the destination address for file transfers, allowing users to dynamically configure the server address.

&

[TransferProtocolServerUser]

This macro denotes the user account used during transfer protocol operations. This macro is used to specify the user credentials required to authenticate and perform file transfers to or from the server.

&

[TransferProtocolServerPassword]

This macro denotes the user password employed during transfer protocol operations. This macro is utilized to provide the necessary password for authentication when transferring files to or from the server.

&

[TransferFileName]

This macro denotes the unique filename assigned during file upload operations. When interacting with external systems or transferring files, this macro represents the specific name assigned to the file being uploaded.

&

[ConfigModePassword]

This macro represents the password required to access configuration mode. It is particularly useful when configuring devices with specific password protection, ensuring secure access to configuration settings.

&

[VRFName]

This macro represents the name of the Virtual Routing and Forwarding (VRF) instance. It is used in

configurations where devices support VRF, allowing users to dynamically specify the VRF name during template creation or configuration management.

These macros provide users with dynamic placeholders to enhance customization and automation within Motadata AIOps, enabling efficient configuration management and file transfers.

Prompt Commands in NCM Device Template

â€‹

Prompt commands are integral elements in the interaction between users and the Motadata AIOps system, especially during the execution of commands and configuration tasks. These commands dictate the system's response to specific queries or prompts, enabling a streamlined and automated workflow. Understanding the significance of each prompt command is crucial for effectively configuring templates and ensuring accurate command execution.

In Motadata AIOps, prompt commands guide the system's behavior when faced with various prompts during command execution. Whether confirming an action, providing responses, or navigating through command line interfaces, prompt commands play a pivotal role in automating tasks and maintaining a cohesive configuration management process.

The following Command Prompts are available in Motadata AIOps while creating a NCM device template:

Command Prompt

Description

LF

LF stands for Line Feed. It represents a control character that moves the cursor to the next line without advancing to the next page. It is commonly used to denote the end of a line in text files.

yes followed by LF

This indicates entering "yes" and then pressing Enter (LF). It is used when a positive response is required, followed by confirming the action by pressing Enter.

y

"y" is a shorthand notation for "yes." It is commonly used in command-line interfaces to

acknowledge or confirm an action.

y followed by LF

This represents entering "y" and then pressing Enter (LF) to confirm or acknowledge an action.

y followed by CR and LF

This represents entering "y" and then pressing Carriage Return (CR) followed by Enter (LF). It might be used as an alternative way to confirm an action.

n followed by LF

Indicates entering "n" (no) and then pressing Enter (LF). It is used to provide a negative response or decline an action.

yes followed by CR and LF

This represents entering "yes" and then pressing Carriage Return (CR) followed by Enter (LF) to confirm an action.

CR and LF

Represents pressing Carriage Return (CR) followed by Enter (LF). It is used to confirm or submit a command or action.

CR and Space

Involves pressing Carriage Return (CR) followed by a space. It might be used in specific scenarios where this combination is required.

Space

Represents pressing the spacebar. It might be used as an input or to navigate through options.

No Command

This indicates no specific command associated with the prompt. It is used when no additional command is required after reaching a specific prompt.

LF followed by LF

Represents pressing Enter (LF) twice consecutively. It might be used in scenarios where a double Enter is required.

yes

Represents entering "yes" without pressing Enter. It might be used in scenarios where a confirmation is needed without a newline character.

no

Represents entering "no" without pressing Enter. it is used when a negative response is required without a newline character.

Page Title: ncm-runbooks

On this page

NCM Runbooks

NCM Runbooks in Motadata AIOps can be created by executing SSH Runbooks, enabling you to automate various tasks and streamline network configuration management. Runbooks allow you to achieve numerous use cases, such as changing the description of all interfaces, modifying VLANs on specific interfaces, enabling SNMP across all devices, and activating SNMP traps on all devices simultaneously.

Once a runbook is created, you can execute it for an NCM device either manually through the NCM Explorer or by scheduling it to run at a specific time. Before scheduling, you need to assign the runbook to the NCM device.

Use Cases for Runbooks

â€‹

Here are some of the scenarios for which a Runbook can be employed:

Change the Description of All Interfaces at Once

: Update the description field for all network interfaces on a device. This is particularly useful for standardizing interface descriptions across multiple devices, making it easier to manage and identify them.

Modify VLAN Settings on a Specific Interface

: Adjust VLAN settings on a targeted interface. This can include adding, modifying, or removing VLANs, ensuring that your network segments are correctly configured according to your requirements.

Enable SNMP Across All Devices at Once

: Activate SNMP (Simple Network Management Protocol) on all network devices. This is crucial for network monitoring and management, allowing you to collect valuable performance data and manage devices remotely.

Activate SNMP Traps Across All Devices at Once

: Enable SNMP traps on all network devices to receive alerts and notifications about specific events. This helps in proactive network management and quick troubleshooting.

NCM Runbook Execution

â€‹

Executing a Runbook Manually

â€‹

To execute a runbook manually for an NCM device:

Create a Runbook

: Ensure that you have created a

SSH runbook

 for the NCM device. Also, ensure that the

Apply To NCM

 option is enabled while creating the SSH Runbook.

Navigate to NCM Explorer

: Go to the NCM Explorer and locate the NCM device for which you need to execute the runbook.

Select Execute Runbook

: In the

Actions

 column against the device, select the

Execute Runbook

 option.

Choose the Runbook

: A list of all runbooks created for the same vendor type as the NCM device will be displayed. Select the runbook to execute.

.

Upload CSV (Optional)

: You can also upload a CSV file to use with the runbook script to execute your custom use cases.

Scheduling a Runbook

â€‹

To schedule a runbook for execution at a specific time:

Assign Runbook to Monitor

: Ensure the Runbook is assigned to the monitor.

Schedule the Runbook

: Refer to the

Scheduling a Runbook

 for detailed steps on how to schedule the runbook.

By leveraging runbooks in Motadata AIOps, you can automate repetitive tasks, ensure consistency across network configurations, and enhance the efficiency of your network management operations. Whether you choose to execute runbooks manually or schedule them for future execution, the flexibility and power of runbooks will help you achieve various network configuration management goals with ease.

Page Title: overview

On this page

Overview

In the complex world of modern network administration, overseeing the configuration of a diverse range of devices such as routers, switches, firewalls, and other core network infrastructure components poses a significant challenge. Managing these elements in a multi-vendor environment requires a holistic approach to network configuration management.

Motadata AIOps introduces a robust solution in the form of Network Configuration Management (NCM). Tailored to address the complexities of managing diverse devices, NCM emerges as a specialized module designed to handle configuration changes efficiently. This module empowers network administrators, providing a centralized hub for effective device management in the face of constant challenges.

The Challenge

â€‹

In large organizations, managing constant configuration changes is a real struggle. Administators need to maintain proper version control, making sure configurations meet the set standards set in a organisation. Even small deviations can lead to big problems, and handling configurations manually takes a lot of time and is prone to human errors.

For a network infrastructure with multiple vendor setup , sticking to the organization's established standards becomes not only important but extremely difficult. This is where NCM comes in as a crucial tool, making sure configurations smoothly matches the established configuration baseline. This is vital for keeping everything consistent, lowering risks, and building a strong and dependable network infrastructure.

The Solution: Motadata AIOps NCM

â€‹

Motadata AIOps introduces the Network Configuration Manager, a powerful solution crafted to tackle

these challenges head-on. With NCM, administrators unlock efficient ways to handle configuration changes by automating backup and restoration processes while implementing robust version control mechanisms.

Configuration Management

â€‹

NCM streamlines the handling of configuration changes, offering a centralized platform to manage devices efficiently. Administrators can easily add, remove, and handle configuration changes across the network. Whether dealing with routers, switches, or core infrastructure components, NCM provides a centralized platform for effective device management.

Navigating Multi-Vendor Complexity

â€‹

In a world of diverse vendors, NCM serves as a unifying platform, simplifying the management of configurations across different devices. It streamlines the complexities associated with multi-vendor environments, ensuring a consistent approach to configuration management.

Efficient Backup and Restore

â€‹

Scheduled backups, both locally and externally, offer a safety net for configuration files. NCM enables administrators to effortlessly back up the running config and startup config files of network devices. In case of discrepancies, administrators can swiftly restore configurations to a desired state, ensuring data integrity and network resilience.

Precise Comparison and Synchronization of Network Device Configuration

â€‹

NCM facilitates detailed comparison of startup and running configurations, highlighting differences. Administrators can easily identify any discrepancies and synchronize configurations to maintain harmony across devices. This precise approach minimizes the risk of inconsistencies in network configurations.

Version Control

â€‹

Ensure accountability and mitigate risks by implementing version control for configurations. NCM allows administrators to roll back to previous versions if needed, providing a safety net for configuration changes.

Adherence to Standards

â€‹

NCM ensures strict adherence to organizational configuration standards, promoting consistency and reducing the likelihood of configuration-related issues. By providing a standardized approach, NCM enhances network security and stability.

Automation

â€‹

Automate repetitive tasks associated with configuration management, reducing the likelihood of human errors and enhancing operational efficiency. NCM simplifies complex tasks, improving overall network management.

Motadata AIOps NCM emerges as a pivotal module, empowering network administrators to navigate the complexities of configuration management effectively. From preventing adverse effects of configuration changes to enabling quick recovery, NCM establishes a proactive and robust approach to network configuration. This comprehensive solution ensures efficient network configuration management and enhances overall network security.