Network Config Management (NCM)

Network Config Management (NCM)

Introduction

Pandora FMS NCM Server (Network Config Management) allows interacting with any network device, through Telnet and SSH protocols, to manage its configuration, perform backups, restore the configuration of the devices from the backups made and even perform custom executions with them.

To carry out all of these tasks, it is based on a system of templates by Manufacturer-Model that will allow to customize all the executions the network devices will carry out, having the control and knowledge of all the executions that will be carried out in each and every one of the above mentioned network devices.

Enable NCM server

To enable this feature in Pandora FMS, it is necessary for the NCM service to be enabled in `pandorafms` server.

The following parameters must be correctly configured in `pandora_server.conf` file:

```
# Network manager configuration server.
ncmserver 1

# Threads for NCM server.
ncmserver_threads 1

# NCM utility to execute SSH and Telnet connections.
ncm_ssh_utility /usr/share/pandora_server/util/ncm_ssh_extension
```

Once enabled and restarted the PFMS server, a new server will appear in the server view and all the sections corresponding to this feature will be enabled in the console.

To display the menus for everything related to NCM server each user must have the corresponding ACL rights. See more information about that in this article.

Enterprise Alternative Server packages

If you use the Enterprise Alternative Server packages, must install `libnsl` and `openssh-clients` for the feature to work properly.

Defining vendors and models

Before starting work, you must make sure that the system has the manufacturer and model(s) of the devices to be used defined. To that end use the *Vendor* and *Model* editors.

You will find these editors in the Configuration → Network Config Manager section.

This is only a descriptive definition. The logic is applied in the network equipment Templates.

Network equipment templates

Templates are applied on a Manufacturer and on one or more models. Templates define how to interact with a network computer. The NCM and the equipment can be connected through Telnet or SSH. In both cases it will be necessary to provide one or more sets of credentials (in the case of the Cisco manufacturer the access username/password and the `enable` mode password). In other devices there may be two pairs of credentials.

For the credentials, use Pandora FMS internal credentials system that allows to reuse them without knowing the details. That way the administrator may specify different user/password “pairs” with an identifier, and an operator may use them without seeing the content. In NCM, these users and passwords are passed to the dialog with the device through macros.

Macros in the dialog with the network device

- `_enablepass_` : It will be replaced by the `password` field of the advanced key associated to the agent.
- `_username_` : It will be replaced by the `username` field of the agent's access key.
- `_password_` : It will be replaced by the `password` field of the agent's access key.
- `_advusername_` : It will be replaced by the `username` field of the `enable` advanced key.
- `_advpassword_` : It will be replaced by the `password` field of the `enable` advanced key. It is an alias of `_enablepass_` and both can be used in the templates since they are equivalent to the same value.
- `_applyconfigbackup_` : Expands by as many commands as there are configuration lines in the current backup, applied line by line, as they are applied in Cisco® devices.
- `_SOURCE_FILE_NAME_`: It will be replaced by the path to the last firmware uploaded for a specific manufacturer and model in Pandora FMS server, to be downloaded using the IP address of the FTP server (FTP server IP field).

- _TFTP_SERVER_IP_: It will be replaced by the IP address configured for the FTP server from which the *firmware* to be used by NCM devices can be downloaded. The IP address can be specified in Pandora FMS general configuration.

Creating a NCM template

Click the Define a NCM template button (menu Management → Configuration → Network Config Manager) and click Create.

Fill the fields:

- Name: NCM template name.
- Vendors: Comma separated, a vendors list compatible with scripts defined within template.
- Models: Comma separated, a model list compatible with scripts defined within template.
- Script: Test: This script will be used to test devices availability.
- Script: Get configuration: This script will be used to retrieve configuration from devices
- Script: set configuration: This script will be used to apply configuration, previously backed up, to devices.
- Script: get firmware: This script will be used to retrieve firmware version from devices.
- Script: set firmware: This script will be used to upgrade firmware version of the devices.
- Script: custom task:This script will be executed on the devices when selecting CUSTOM task.

Example of use on a Cisco 7200 device

These scripts only work if the user you log in with (via Telnet or SSH) works with user and password and does not have `enable` field enabled by default.

Test

A test connection is made to the device and ended without performing any operation.

```
enable
expect:Password:\s*
_enablepass_
exit
```

The test connection is used to verify that you can actually connect to the device. It can be modified (`expect:xxxx`) to expect a certain response, such as `Ready`. This is only a basic example.

Retrieve current configuration

This block is used to define the way to obtain the configuration of the active device. In this

example (Cisco®), the running configuration of the device is obtained by executing the `show running-config` command inside the device:

```
enable
expect:Password:\s*
_enablepass_ term length 0
capture:show running-config exit
```

`capture:<comando>` : It is used to capture as active configuration what is returned by the screen.

`sleep:2`: (Version 772 or later) Allows you to enter a “timeout”, in seconds, between two commands in a model.

Retrieve firmware version

Similar to the previous case, run the `show version | i IOS Software` command to retrieve the firmware version of the device, and as in the previous case, the `capture` command is used to capture the output of the command.

```
enable
expect:Password:\s*
_enablepass_
term length 0
capture:show version | i IOS Software
exit
```

Restore configuration backup

In this execution, the macro `_applyconfigbackup_` is used to apply all the configuration stored in the Backup previously stored in the Console.

```
enable
expect:Password:\s*
_enablepass_
term length 0
config terminal
_applyconfigbackup_
exit
```

Example custom script

Example of a custom script in which the values of some SHH parameters of the device are

changed. Any necessary modification or command execution can be applied.

```
enable
expect:Password:\s*
_enablepass_
conf term
ip ssh authentication-retries 4
ip tcp synwait-time 10
end
exit
```

All changes recorded in the device will be recorded when performing a firmware backup and you will have control of the changes made, both by reports and by screen (Web Console PFMS).

Agent data templates

These templates allow obtaining data from an NCM device and updating the information of the agent for which they are executed with such data. The operation and configuration is identical to that of the network equipment templates, but in this case indicating the agent field that will update the result of each script. The fields that can be updated in an agent are:

- OS version.

Creating an agent data template

Click Create (menu Management → Configuration → Network Config Manager → NCM Agents data templates and fill in the requested fields:

- Vendors: Comma-separated, script-compatible list of vendors.
- Models: A comma-separated list of models supported by scripts.
- Script OS version: This script will be used to update the agent version OS field.

Setup in Agents

Within each of the agents that need to manage their remote configuration, associate a model to it.

This association will have to be done in the NCM section of the agent, where the following parameters must be selected:

- Device manufacturer.
- Device model.
- Connection method: Type of connection to be made (Telnet or SSH). If you use SSH with key pairs, it is important that you keep it updated by deleting or adding each IP address and its respective key in the file `/etc/.ssh/known_hosts` .

- Port: Port to use in the Telnet or SSH connection.
- Credentials to access device: Credentials stored in Credential Store of Pandora FMS, which will be used to make the initial Telnet or SSH connection. It is necessary for the user to need both parameters when connecting.
- Credentials to admin device: Credentials stored in Credential Store of Pandora FMS, which will be identified within the template selected in NCM template to be used, with the macros `_advusername_` for the user and `_enablepass_` or `_advpassword_` for the password.
- NCM template to be used: If there is a template defined, choose one that is compatible with the chosen model.

If the chosen template has Script: Get configuration can be backed up periodically using the Backup schedule (if defined) option. To create an event if there are changes between configuration backups, check the option just to the right of the period selection list (daily, weekly, monthly or unscheduled).

To upload the firmware files and create backups of them with FTP, you must do it in an encrypted way to have the highest possible security. See section "FTP configuration to receive data in Pandora FMS" and the use of vsFTPd. You must use SFTP with exclusive chroot in:

```
/var/spool/pandora/firmware/
```

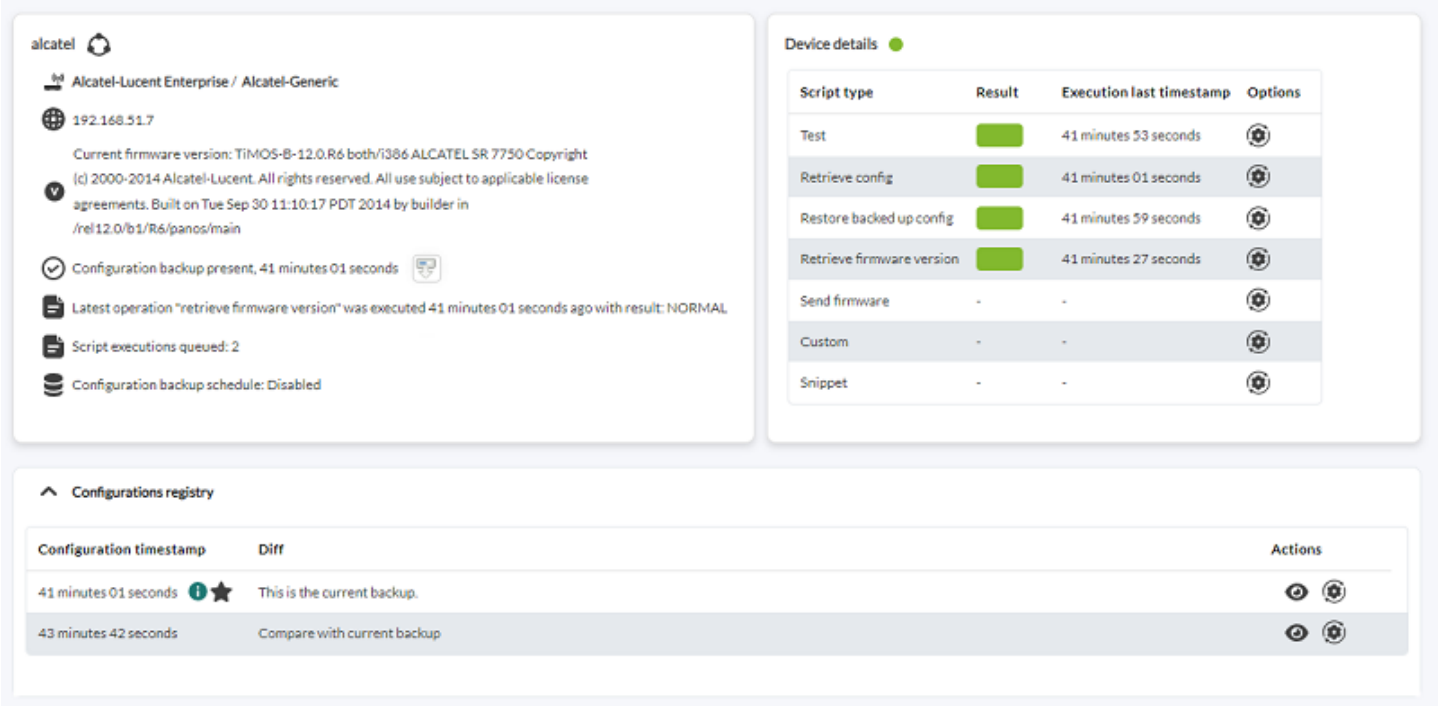
See Pandora FMS "Security Architecture" for a comprehensive overview of this issue.

- NCM Agents data templates to be used: If there is any template that updates agent data defined, choose one that is compatible with the chosen model. It will be possible to schedule the execution of such template with the Agents data templates schedule (if defined) option. To create an event if there are changes between the data obtained and the current data, check the option just to the right of the period selection list (daily, weekly, monthly or unscheduled).

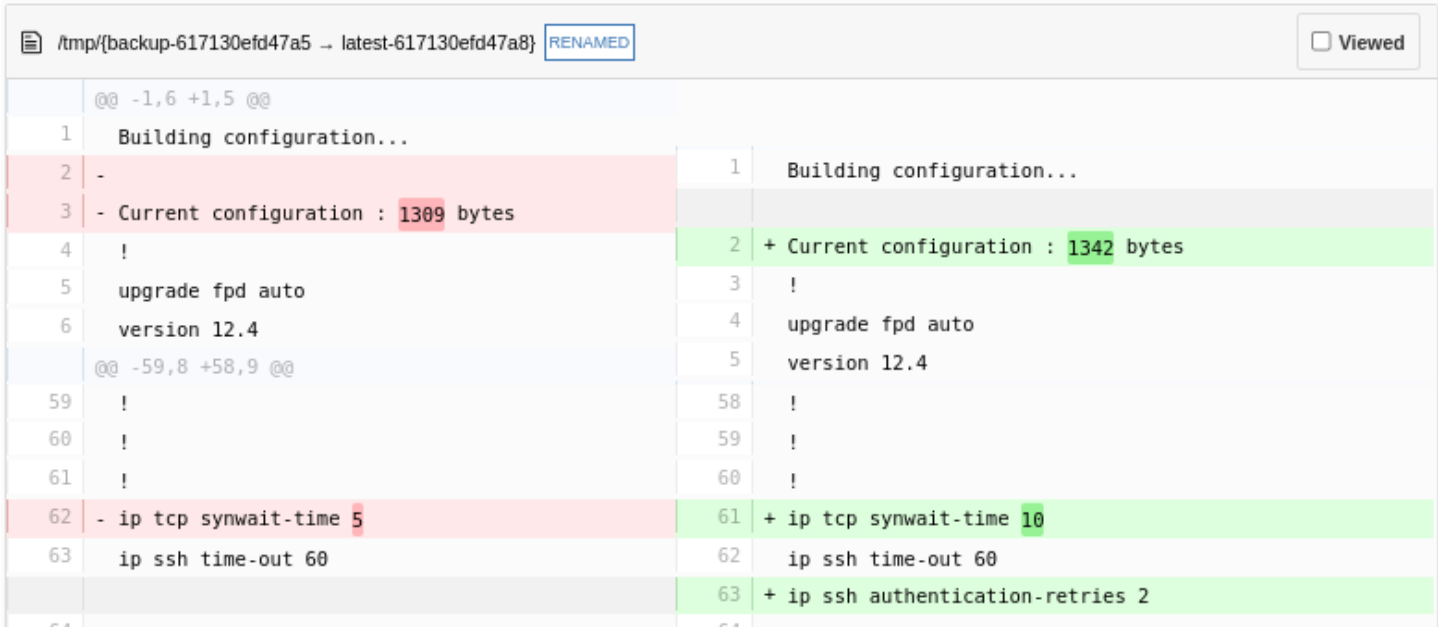
This configuration can be performed in bulk for several agents meeting the same characteristics from the menu Management → Configuration → Network Config Manager → Manage NCM devices.

Configuration management on the devices

After the NCM devices have been configured, you may access the agent view or go to Management → Configuration → Network Config Manager → NCM Devices to perform all possible management on each device.

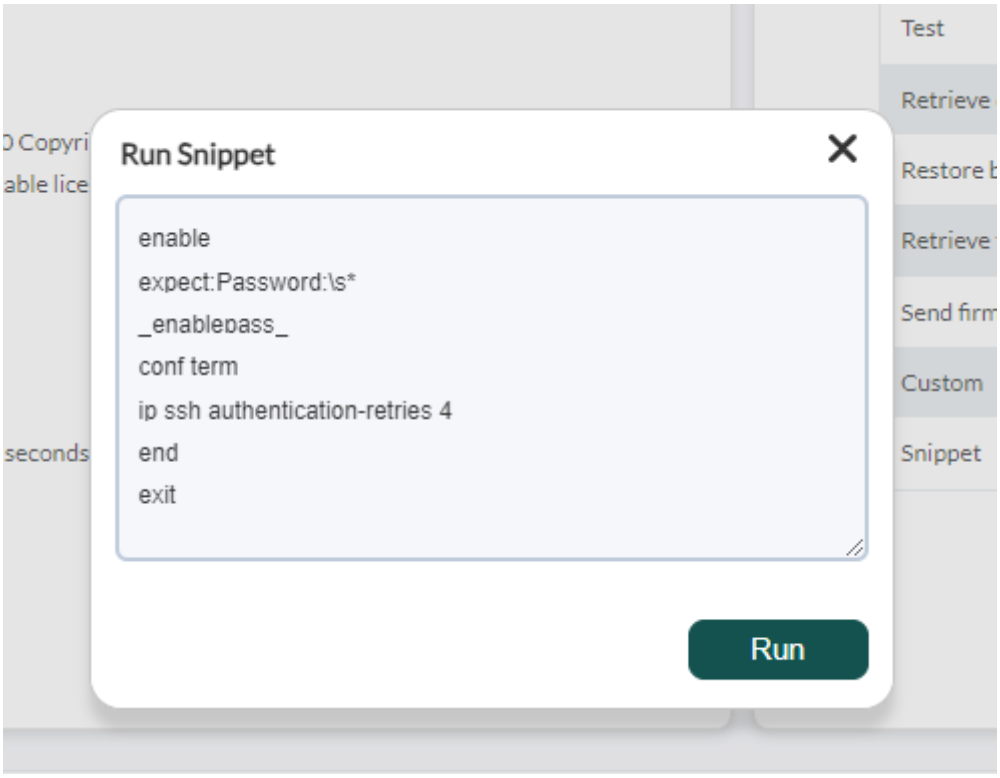


From both views you may queue all the tasks defined in the template, download the current configuration, see the backups generated for the device and compare them with the last backup obtained.



Snippet execution

It will also be possible to execute snippets on any NCM device, i.e. scripts that would not be defined in the templates and that allow code blocks to be executed on demand. These are one-time scripts that are not stored.



ACL

For the NCM feature there are three different ACL bits in which you may define the different users from the following defined bits:

View NCM data → You will only be able to see the agent view and see the information reflected on it without being able to apply any changes on it.

Operate NCM → You will be able to not only see the view, but also to perform the executions you wish on the agents and on the NCM view.

Manage NCM → With this permission you will be able to generate templates, models and new manufacturers in addition to the executions already performed by Operate NCM.

Go back to Pandora FMS documentation index