Network Config Management (NCM)

Network Config Management (NCM)

Introduction

Le serveur NCM (Network Config Management) de Pandora FMS vous permet d'interagir avec n'importe quel périphérique réseau, à l'aide des protocoles Telnet et SSH, pour gérer sa configuration, effectuer des *backups* (sauvegardes), restaurer la configuration des périphériques à partir des sauvegardes effectuées et même pouvoir effectuer des exécutions personnalisées avec eux.

Pour l'exécution de toutes ces tâches, il est basé sur un système de modèles par Fabricant-Modèle qui vous permettra de personnaliser toutes les exécutions que les périphériques réseau effectueront, en ayant le contrôle et la connaissance de toutes les exécutions qui seront effectuées sur chacun de ces périphériques réseau.

Activer le serveur NCM

Pour activer cette fonctionnalité dans Pandora FMS, le service NCM doit être activé sur le serveur `pandorafms`.

Pour ce faire, les paramètres suivants doivent être correctement configurés dans le fichier `pandora_server.conf` :

```
# 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
```

Une fois activées, un nouveau serveur apparaîtra dans la vue serveur et toutes les sections correspondant à cette fonctionnalité seront activées dans la console.

Pour que les menus correspondants à tout ce qui concerne NCM server apparaissent, *chaque utilisateur doit avoir les droits ACL correspondants*. Consultez plus d'informations à ce sujet dans ce même article.

Enterprise Alternative Server packages

Si vous utilisez les paquets Enterprise Alternative Server packages, installez `libnsl` et `openssh-clients` pour que cette fonctionnalité fonctionne correctement.

Définir les vendeurs et les modèles

Avant de commencer à travailler, vous devez vous assurer que le système a le fabricant et le ou les modèles d'appareils à utiliser définis. Pour ce faire, utilisez l'éditeur de Vendeur (*Vendor*) et Modèle (*Model*).

Vous trouverez ces éditeurs dans la section Management → Configuration → Network Config Manager.

Ce n'est qu'une définition descriptive. La logique est appliquée dans les modèles d'ordinateur réseau.

Modèles d'équipement réseau

Les modèles sont appliqués sur un Fabricant et un ou plusieurs modèles. Les modèles définissent la façon dont vous interagissez avec un ordinateur réseau. La connexion entre NCM et l'ordinateur peut se faire via Telnet ou SSH. Dans les deux cas, vous devrez fournir un ou plusieurs jeux d'identifiants (dans le cas du fabriquant Cisco, l'utilisateur/mot de passe d'accès et le *password* du mode `enable`). Sur d'autres appareils, il peut s'agir de deux paires d'identifiants.

Pour les identifiants, utilisez le système interne d'identifiants de Pandora FMS qui vous permet de les réutiliser sans connaître les détails. De cette façon, l'administrateur peut spécifier différents « paires » d'utilisateur/mot de passe avec un identifiant, et un opérateur peut les utiliser sans voir le contenu. Dans NCM, ces utilisateurs et mots de passe sont transmis au dialogue avec l'appareil via des macros.

Macros dans le dialogue avec le périphérique réseau

- `_enablepass_` : Il sera remplacé par la zone `password` de la clé avancée associée à l'agent.
- `_username_` : Il sera remplacé par la zone `username` de la clé d'accès à l'agent.
- `_password_` : Il sera remplacé par la zone `password` de la clé d'accès à l'agent.
- `_advusername_` : Il sera remplacé par la zone `username` de la clé avancée d`'enable`.
- `_advpassword_` : Il sera remplacé par la zone `password` de la clé avancée d`'enable`. C'est un alias de`_enablepass_` et les deux peuvent être utilisés indifféremment dans les modèles car ils équivalent à la même valeur.
- `_applyconfigbackup_` : Développe autant de commandes qu'il y a de lignes de configuration dans la *backup* actuelle, appliquées ligne par ligne, comme c'est le cas pour les appareils Cisco®.

- `_SOURCE_FILE_NAME_` : Il sera remplacé par le chemin d'accès au dernier micrologiciel téléchargé pour un fabricant et un modèle spécifiques dans le serveur Pandora FMS, à télécharger en utilisant l'adresse IP du serveur FTP (champ FTP server IP).
- `_TFTP_SERVER_IP_` : Elle est remplacée par l'adresse IP configurée pour le serveur FTP à partir duquel le microprogramme à utiliser par les dispositifs NCM peut être téléchargé. L'adresse IP peut être spécifiée dans le champ Configuration générale de Pandora FMS.

Création d'un modèle NCM

Cliquez sur le bouton Define a NCM template (menu Management → Configuration → Network Config Manager) et cliquez sur le bouton Create.

Remplissez les zones demandées:

- Vendors (Fabricants) : Séparée par des virgules, une liste de fournisseurs prenant en charge *les scripts*.
- Models (Modèles) : Séparée par des virgules, une liste de modèles prenant en charge *les scripts*.
- Script : Test (Test) : Ce *script* sera utilisé pour tester la disponibilité des appareils.
- Script : Get configuration (Obtenir la configuration) : Ce *script* sera utilisé pour récupérer les paramètres des périphériques.
- Script : set configuration (Définir les paramètres) : Ce *script* sera utilisé pour appliquer les paramètres sauvegardés préalablement aux périphériques.
- Script : get firmware (Obtenir le *firmware*) : Ce *script* sera utilisé pour récupérer la version du *firmware* des périphériques.
- Script : set firmware (Fixer le *firmware*) : Ce *script* sera utilisé pour récupérer la version du *firmware* des périphériques préalablement stockée.
- Script : custom task (Tâche personnalisée) : Ce *script* s'exécutera sur les appareils lors de la sélection de la tâche CUSTOM.

Exemple d'utilisation sur un appareil Cisco 7200

Ces *scripts* ne fonctionnent que si l'utilisateur avec lequel vous allez vous vous connectez (via Telnet ou SSH) fonctionne via *user* et *password* et n'a pas `enable` activé par défaut.

Test

Une connexion de test est effectuée à l'appareil et la connexion est terminée sans effectuer aucune opération.

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

La connexion de test est utilisée pour vérifier qu'il est possible de connecter à l'appareil. Il peut

être modifié (`expect :xxxx`) pour attendre une réponse donnée, telle que `Ready`. Ce n'est qu'un exemple de base.

Récupérer la configuration actuelle

Ce bloc est utilisé pour définir comment obtenir la configuration du périphérique actif. Dans cet exemple (Cisco®), vous obtenez la configuration en cours d'exécution sur l'appareil en exécutant la commande `show running-config` à l'intérieur de l'appareil:

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

`capture:` : Il sert à capturer en tant que paramètre actif ce qu'il renvoie à l'écran.

`sleep:2` : (Version 772 ou ultérieure) Permet d'entrer un “timeout”, en secondes, entre deux commandes dans un modèle.

Récupérer la version du firmware

Comme dans le cas précédent, nous exécutons la commande `show version | i IOS Software` pour obtenir la version du *firmware* de l'appareil, et comme dans le cas précédent, la commande `capture` est utilisée pour capturer la sortie de la commande.

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

Restaurer la sauvegarde de configuration

Dans cette exécution, la macro `_applyconfigbackup_` est utilisée pour appliquer tous les paramètres stockés dans la *sauvegarde* qui ont déjà été stockés dans la console.

```
enable
expect:Password:\s*
_enablepass_
term length 0
```

```
config terminal
_applyconfigbackup_
exit
```

Exemple de script personnalisé

Exemple de script personnalisé dans lequel la valeur maximale des tentatives d'authentification SSH de l'appareil est modifiée. Toute modification ou exécution de commande nécessaire peut être appliquée.

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

Toutes les modifications enregistrées sur l'appareil seront enregistrées lors de la sauvegarde *du firmware* et les modifications effectuées seront contrôlées à la fois par les rapports et par l'écran (Console Web PFMS).

Modèles de données de l'agent

Ces modèles vous permettent d'obtenir des données d'un équipement NCM et de mettre à jour les informations de l'agent pour lequel ils sont exécutés avec ces données. Le fonctionnement et la configuration sont identiques à ceux des modèles d'équipement de réseau, mais dans ce cas, en indiquant le champ de l'agent qui mettra à jour le résultat de chaque script. Les champs qui peuvent être mis à jour dans un agent sont les suivants :

- OS version.

Création d'un modèle de données de l'agent

Cliquez sur le bouton Create (menu Management → Configuration → Network Config Manager → NCM Agents data templates et remplissez les champs demandés:

- Vendors (Fabricants) : Liste de fournisseurs séparée par des virgules et conforme aux scripts..
- Models (Modèles) : Liste séparée par des virgules des modèles pris en charge par les scripts.
- Script OS version : Ce script est utilisé pour mettre à jour le champ de la version du système d'exploitation de l'agent.

Setup dans les agents

Au sein de chacun des agents qui ont besoin de gérer leur configuration à distance, vous devez associer un modèle à celui-ci.

Cette association doit être effectuée dans la section NCM de l'agent, où vous devez sélectionner les paramètres suivants :

- Device manufacturer : Fabricant de l'appareil.
- Device model : Modèle du dispositif.
- Connection method : Type de connexion à réaliser (Telnet ou SSH). Si vous utilisez SSH avec des paires de clés, il est important de les mettre à jour en supprimant ou en ajoutant chaque adresse IP et sa clé respective dans le fichier `/etc/.ssh/known_hosts` .
- Port : Port à utiliser sur la connexion Telnet ou SSH.
- Credentials to access device : Les identifiants stockées dans la section Credential Store de Pandora FMS, qui serviront à établir la connexion initiale par Telnet ou SSH. Il est nécessaire que l'utilisateur au moment de la connexion ait besoin des deux paramètres.
- Credentials to admin device : Identifiants stockés dans la section Credential Store de Pandora FMS, et qui seront identifiés dans le modèle sélectionné dans NCM template to be used, avec les macros `_advusername_` pour l'utilisateur et `_enablepass_` ou `_advpassword_`pour le mot de passe.

Si le modèle choisi a configuré Script : Get configuration peut être sauvegardé périodiquement à l'aide de l'option Backup schedule (if defined). Pour créer un événement en cas de changement entre les sauvegardes de configuration, cochez l'option située juste à droite de la liste de sélection de la période (quotidienne, hebdomadaire, mensuelle ou non programmée).

Pour charger les fichiers de contenu *du firmware* et créer des sauvegardes avec FTP, vous devez le faire de manière cryptée pour avoir la plus grande sécurité possible. Reportez-vous à la section «Paramètres FTP pour recevoir des données dans Pandora FMS » et à l'utilisation de vsFTPd. Vous devez utiliser SFTP avec chroot exclusif sur :

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

Reportez-vous à la section «Architecture de sécurité » de Pandora FMS pour obtenir une vue d'ensemble de cette question.

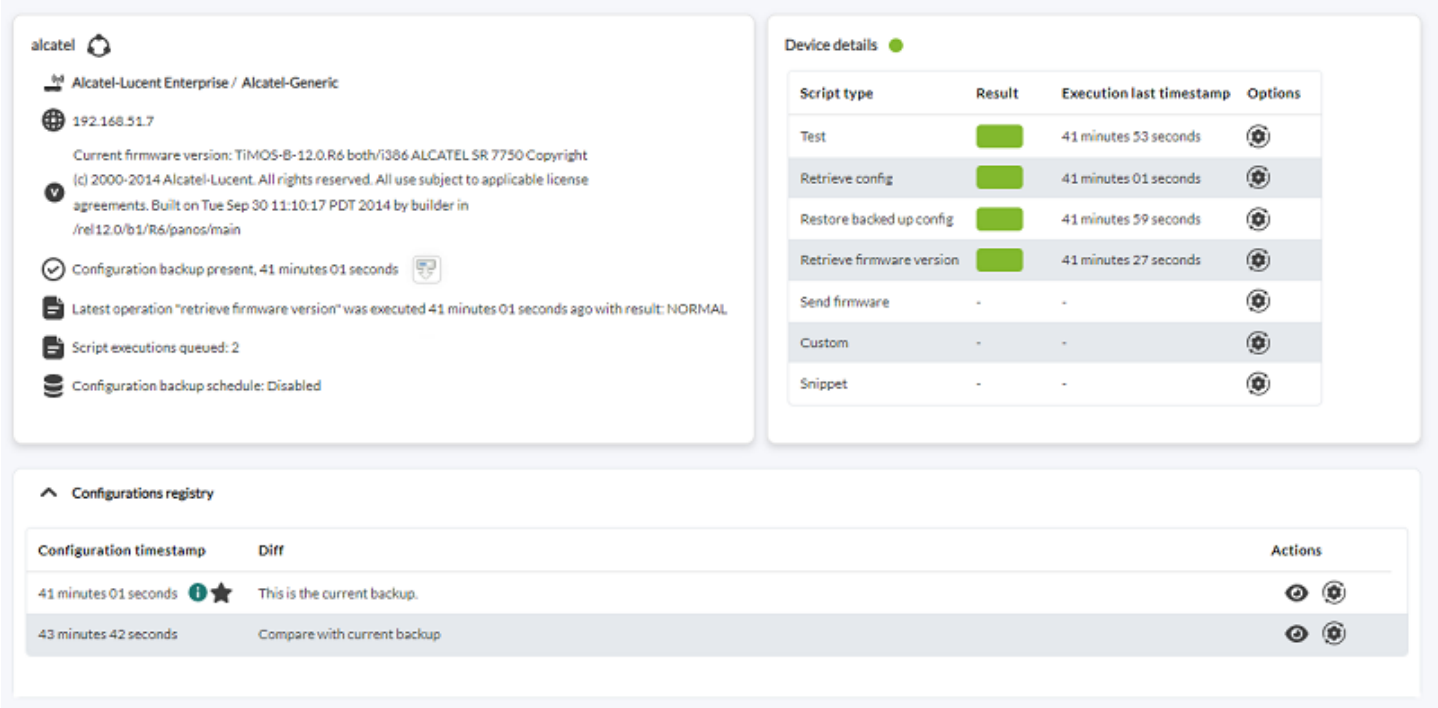
- NCM Agents data templates to be used : S'il existe un modèle qui met à jour les données de l'agent définies, choisissez celui qui est compatible avec le modèle choisi. L'exécution de ce modèle peut être programmée avec l'option Agents data templates schedule (if defined). Pour créer un événement en cas de changement entre les données collectées et les données actuelles, cochez l'option située juste à droite de la liste de sélection de la période (quotidienne, hebdomadaire, mensuelle ou non programmée).

Cette configuration peut être effectuée en bloc pour plusieurs agents répondant aux

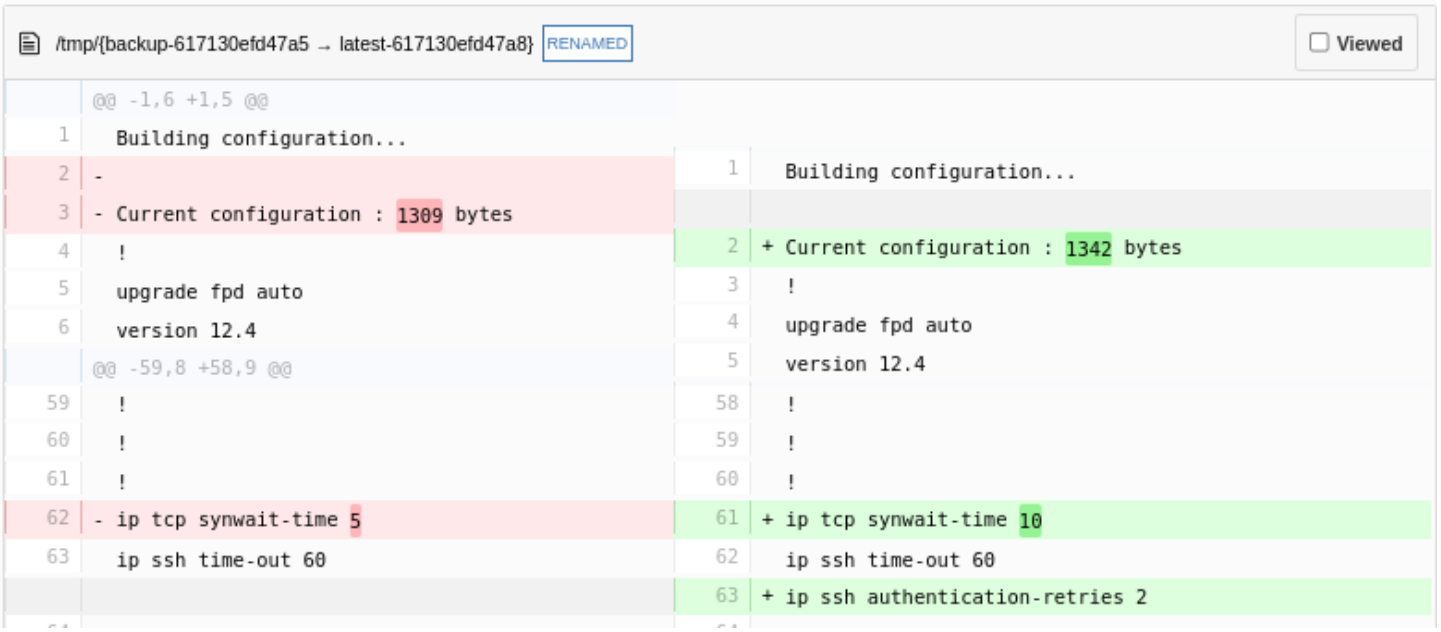
mêmes caractéristiques à partir du menu Management → Configuration → Network Config Manager → Manage NCM devices.

Gestion des configurations sur les appareils

Une fois les appareils NCM configurés, vous pouvez accéder à la vue de l'agent ou à la vue de l'agent. Management → Configuration → Network Config Manager → NCM Devices d'effectuer toutes les gestions possibles dans chacun d'entre eux.

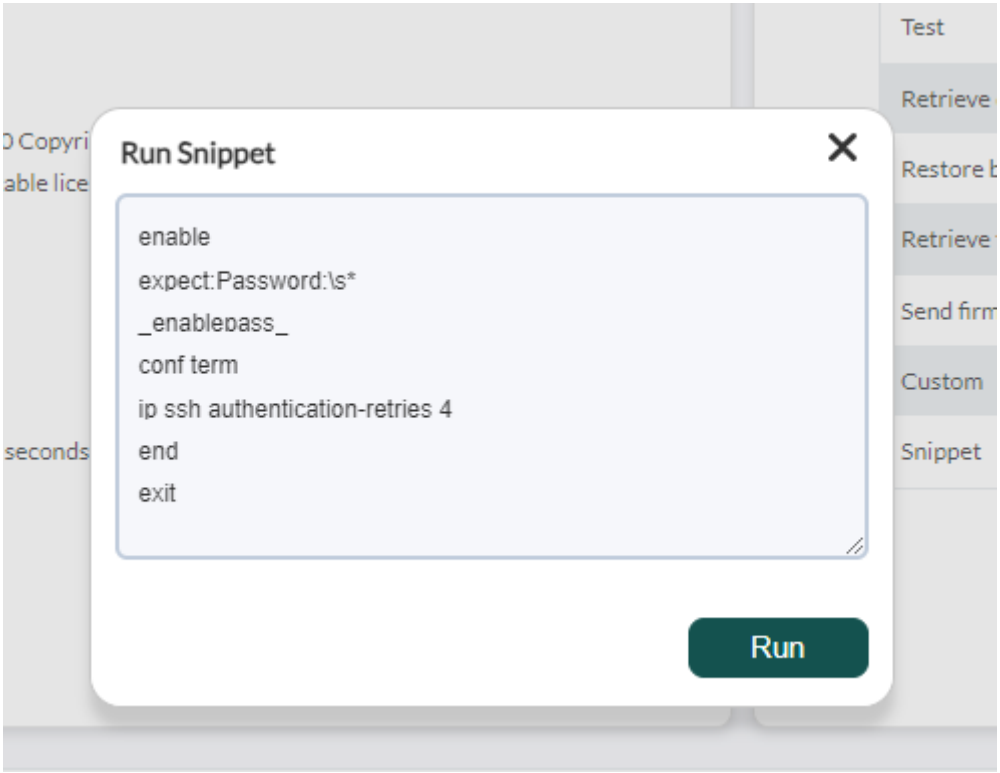


Les deux vues permettent de mettre en file d'attente toutes les tâches définies dans le modèle, de télécharger la configuration actuelle, de visualiser les *backups* générés pour l'appareil et de les comparer avec le dernier *backup* obtenu.



Exécution de snippets

Il doit également être possible d'exécuter des *snippets* sur n'importe quel dispositif NCM, c'est-à-dire des *scripts* qui ne seraient pas définis dans les modèles et qui permettent d'exécuter des blocs de code sur demande. Il s'agit de *scripts* à exécution unique qui ne sont pas stockés.



ACL

Pour la fonctionnalité NCM, il existe trois bits ACL distincts dans lesquels vous pouvez définir les différents utilisateurs à partir des bits définis suivants :

View NCM data → Vous pouvez uniquement visualiser la vue de l'agent et voir les informations qui y sont reflétées sans pouvoir y apporter de modifications.

Operate NCM → Vous pouvez non seulement visualiser la vue, exécuter les exécutions de votre choix sur les agents et dans la vue NCM.

Manage NCM → Cette autorisation permet de générer des modèles, des modèles et de nouveaux fabricants en plus des exécutions déjà effectuées par Operate NCM.

Retour à l'index de documentation Pandora FMS