Configuration de l'authentification NTP sur Secure Network Analytics

Table des matières

Introduction

Ce document décrit comment configurer votre Secure Network Analytics (SNA) appliance pour authentifier la connexion au serveur NTP configuré.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration de l'appliance Cisco Secure Network Analytics
- Protocole NTP (Network Time Protocol)

Composants utilisés

L'appliance Cisco Secure Network Analytics Manager utilisée pour ce document est la version 7.4.2.

Ce processus s'applique à tous les types d'appareils Cisco Secure Network Analytics.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configurer

Configuration requise pour NTP

Les valeurs utilisées pour authentifier la communication NTP doivent répondre aux exigences suivantes :

- La valeur de l'ID de clé doit être inférieure ou égale à 65535
- La validation de la clé est SHA1
- La valeur de clé ne doit pas comporter plus de 32 caractères alphanumériques imprimables (ASCII) : 0-9, A-Z, a-z et symboles (sauf #)

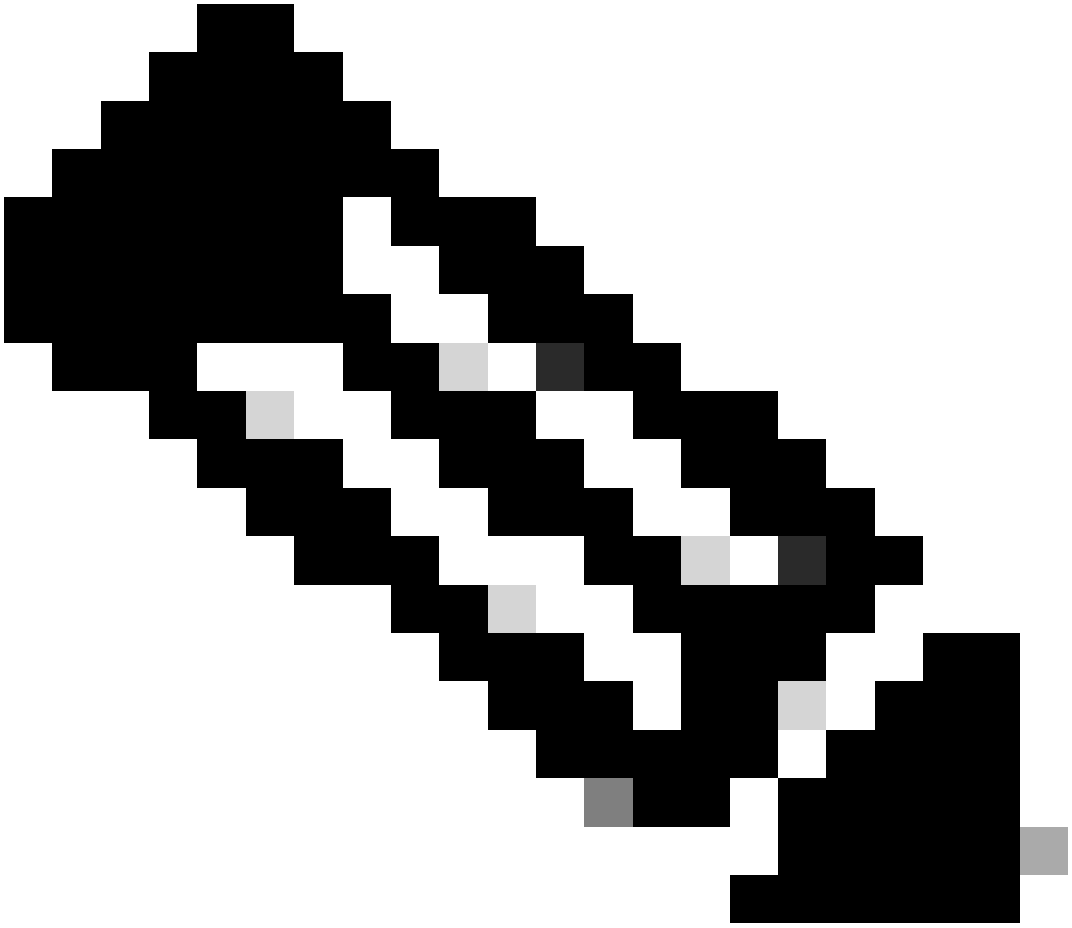
Détails de la valeur clé

NTP suppose que les valeurs de clé supérieures à 20 octets sont supposées être HEX.

La longueur maximale de la valeur de clé est de 64 octets, de sorte qu'une clé déhexée ne peut pas dépasser 32 octets.

Reportez-vous au tableau pour voir des exemples de valeurs clés pour le serveur NTP et l'appliance Secure Network Analytics.

Octet de clé	Configuration de la valeur de clé du serveur NTP	Configuration de la valeur clé Secure Network Analytics
Moins de 20 octets	Lan1cope !	Lan1cope !
Entre 20 et 32 octets	4C616E31636F7065214C616E31636F7065214C616E31636F7065214C616E3163	Lan1cope ! Lan1scope ! Lan1scope ! Lan1c



Remarque : les valeurs utilisées dans le tableau ne sont que des exemples et ne sont pas recommandées dans votre environnement

---

Configuration Authentification NTP SNA Manager

Ouvrir les paramètres du serveur NTP

Connectez-vous au **SNA Manager** et ouvrez les **NTP Server** paramètres.

- Dans le menu principal, sélectionnez Configure > GLOBAL Central Management.
- Dans l'onglet Inventaire, cliquez sur l'icône ... (Ellipsis) de l'appliance.

- Sélectionnez Edit Appliance Configuration.
- Sélectionnez l'Network Services onglet.

Ajouter un serveur NTP

Suivez ces instructions pour ajouter un serveur NTP à la configuration de l'appliance sélectionnée si nécessaire.

- Dans la section NTP Server, cliquez sur Add New.
- Dans le champ,NTP Servers cliquez sur la flèche de la liste déroulante. Sélectionnez un serveur NTP dans la liste.
- Saisissez le nom ou l'adresse IP du serveur.
- Cliquez sur Add.
- Cliquez sur Apply Settings.
- Acceptez les invites affichées à l'écran. L'appliance redémarre automatiquement.

Ajouter une authentification

Utilisez ces instructions pour authentifier la connexion au serveur NTP sélectionné.

Préparation : assurez-vous que vous avez l'ID de clé du serveur NTP et la valeur de clé.

- Dans la section Serveur NTP, cliquez sur l'icône ... (Ellipsis) du serveur NTP.
- Sélectionnez Authenticate Connection.
- Saisissez l'ID et la valeur de la clé.
- Cliquez sur Apply Authentication.
- Cliquez sur Apply Settings.
- Acceptez les invites affichées à l'écran. L'appliance redémarre automatiquement.

Vérifier

Confirmer l'authentification

Si vous ajoutez l'authentification à un serveur, l'icône de clé indique que l'authentification est configurée. Vérifiez le journal d'audit pour confirmer que l'authentification a réussi.

- Dans le menu principal, sélectionnez Configure > GLOBAL Central Management.
- Dans l'onglet Inventaire, cliquez sur l'icône ... (Ellipsis) de l'appliance.
- Sélectionnez Support.
- Sélectionnez l'Audit Logs onglet.
- Dans le champ,Category sélectionnez Management.
- Cliquez sur Search.
- Confirmez que l'état de la communication NTP et les modifications de l'heure système sont indiqués comme réussis. (Cochez la colonne Success pour confirmer que l'événement est affiché comme Yes).

Dépannage

Confirmer le nombre d'octets

Vous pouvez utiliser un shell sur un périphérique Linux pour tester le nombre d'octets des valeurs de clé.

Les valeurs de clé des exemples proviennent du tableau de la section Longueur de la valeur de clé de ce document.

Exécutez la commande echo -n '{key_value}' | wc -c pour voir le nombre d'octets remplacer {key_value} par la valeur de clé que vous souhaitez utiliser.

```
742smc:~# echo -n 'Lan1cope!' | wc -c 9 742smc:~# echo -n 'Lan1cope!Lan1cope!Lan1cope!Lan1c' | wc -c 32
```

Les résultats des lignes 2, 4 et 6 montrent que les nombres d'octets de la valeur clé sont respectivement de 9, 32 et 64.

Confirmer l'utilisation des caractères

Si le nombre d'octets est inférieur à 20, vérifiez que vous utilisez des caractères ASCII imprimables, comme indiqué dans les exigences de configuration NTP.

Vous pouvez exécuter la echo '{key_value}' | xxd -r -p && echo commande pour convertir les valeurs HEX en ASCII en remplaçant {key_value} par la valeur de clé que vous souhaitez utiliser.

```
742smc:~# echo '4C616E31636F7065214C616E31636F7065214C616E31636F7065214C616E3163' | xxd -r -p && echo L
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.