Configuration de l'authentification NTP dans ISE

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Configurer
  - Diagramme du réseau
  - Configurations
    - Avant de commencer
    - Étapes de GUI
    - Étapes CLI
    - Configuration sur le routeur
- Vérifier
- Dépannage
- Défauts De Référence
- Informations connexes

Introduction

Ce document décrit comment configurer l'authentification NTP sur Cisco Identity Services Engine (ISE) et dépanner les problèmes d'authentification NTP.

Conditions préalables

Exigences

Il est recommandé que vous ayez des connaissances sur les sujets suivants :

- Configuration CLI Cisco ISE
- Connaissance de base du protocole NTP (Network Time Protocol)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Noeud autonome ISE 2.7
- CISCO2911/K9 version 15.2(1)T2

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

Diagramme du réseau



Configurations

Avant de commencer

Vous devez disposer du rôle d'administrateur super-administrateur ou administrateur système affecté à l'accès ISE.

Assurez-vous que le port NTP n'est pas bloqué dans le chemin de transit entre ISE et le ou les serveurs NTP.

Nous supposons que vos serveurs NTP sont configurés sur ISE. Si vous voulez modifier votre serveur NTP, naviguez à Administration > System > Settings > System Time. Pour une courte vidéo, vous pouvez voir Configuration NTP ISE

Remarque : Dans le cas d'un déploiement distribué, choisissez le même serveur NTP (Network Time Protocol) pour tous les noeuds. Pour éviter les problèmes de fuseau horaire entre les noeuds, vous devez fournir le même nom de serveur NTP avec l'installation de chaque noeud. Cela garantit que les rapports et les journaux des différents noeuds de votre déploiement sont toujours synchronisés avec les horodatages.

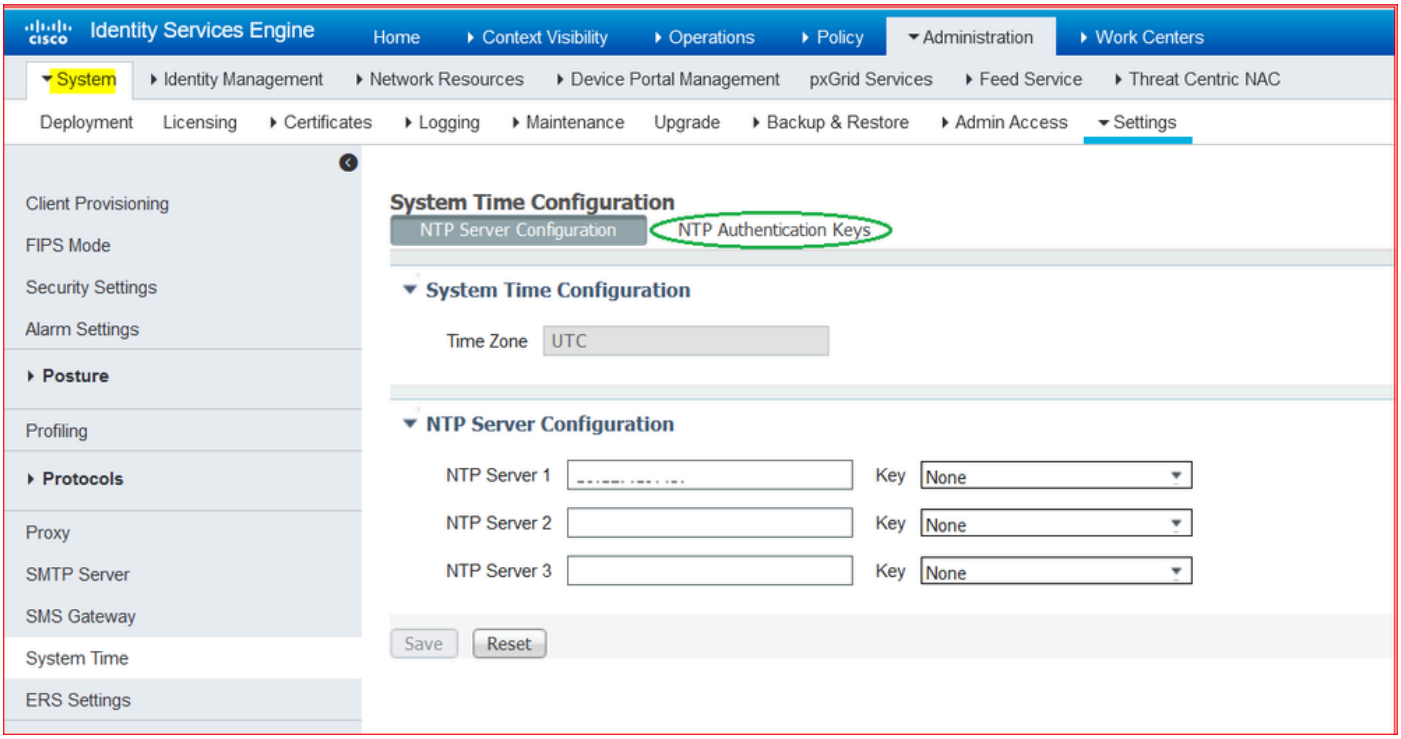
Remarque : Vous ne pouvez pas modifier le fuseau horaire depuis l'interface utilisateur graphique. Vous pouvez le faire via l'interface de ligne de commande qui nécessite le redémarrage du service ISE pour ce noeud particulier. Il est recommandé d'utiliser le fuseau horaire préféré (UTC par défaut) au moment de l'installation lorsque l'assistant de configuration initiale vous demande d'indiquer les fuseaux horaires. Veuillez consulter l'ID de bogue Cisco CSCvo49755 associé à l'activation de la commande CLI clock timezone.

Si votre déploiement comporte à la fois des noeuds Cisco ISE principaux et secondaires, vous devez vous connecter à l'interface utilisateur de chaque noeud et configurer l'heure système et les paramètres du serveur NTP (Network Time Protocol).

Vous pouvez configurer l'authentification NTP dans ISE à partir de l'interface utilisateur graphique ou de l'interface de ligne de commande.

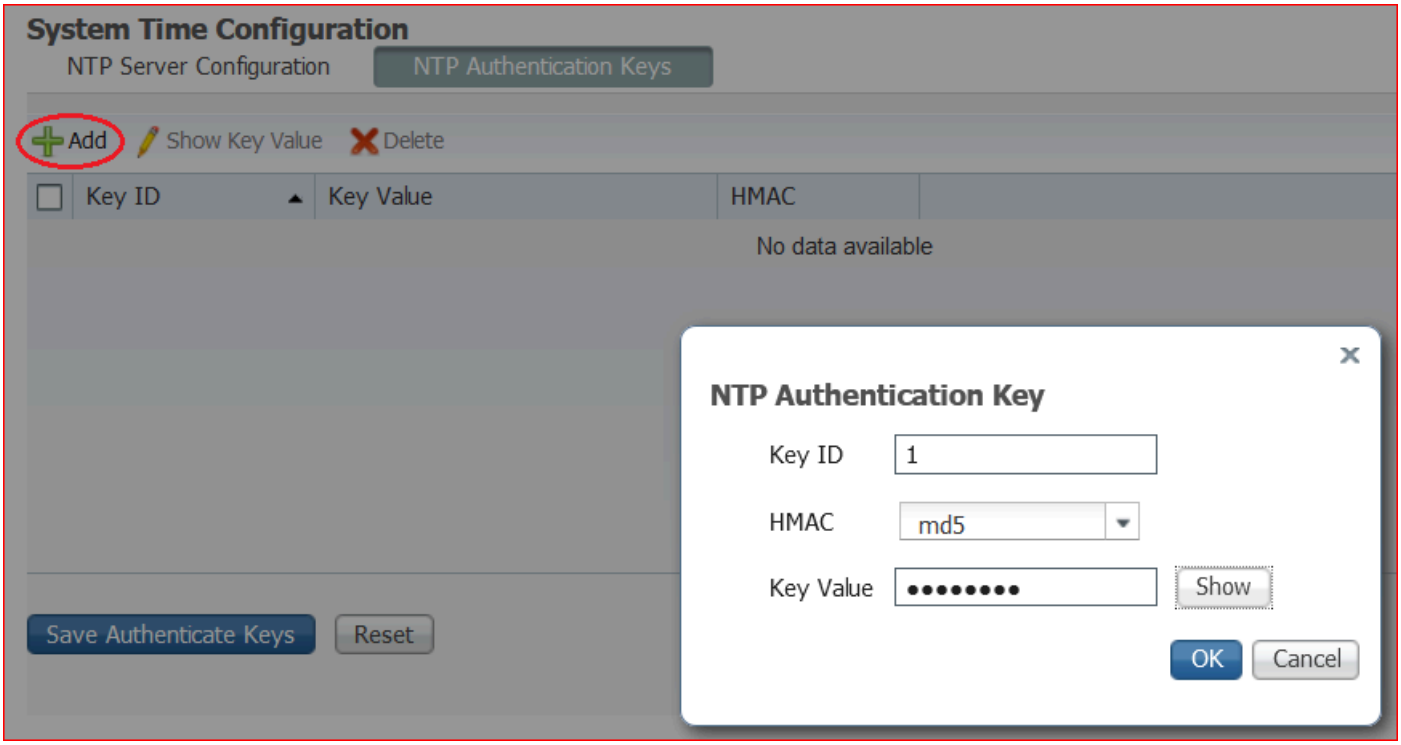
Étapes de GUI

Étape 1. Accédez à Administration > System > Settings > System Time et cliquez sur NTP Authentication Keys, comme indiqué dans cette image.



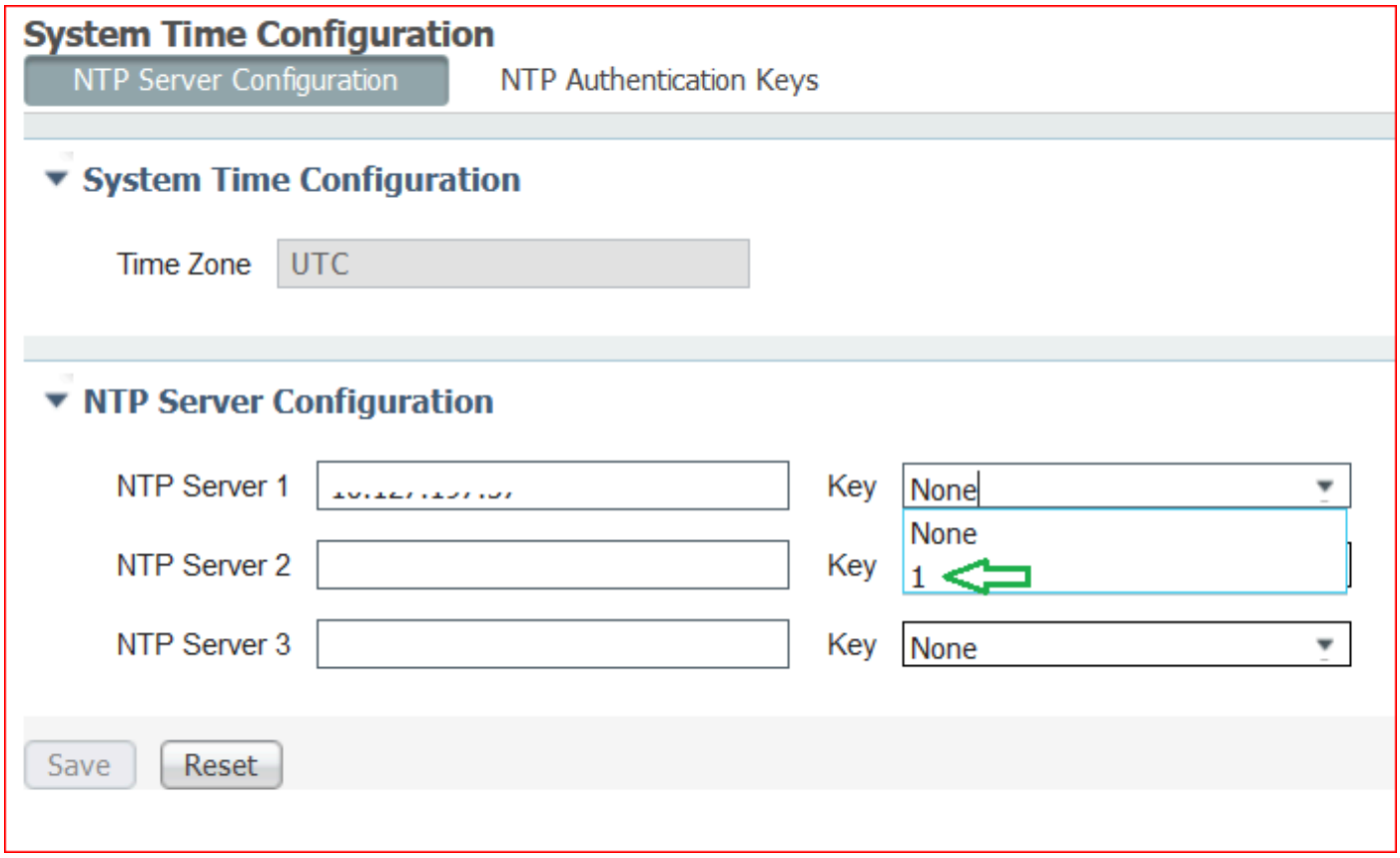
Étape 2. Vous pouvez ajouter ici une ou plusieurs clés d'authentification. Cliquez sur Add, puis vous obtenez une fenêtre contextuelle. Ici, le champ ID de clé prend en charge les valeurs numériques comprises entre 1 et 65535 et le champ Valeur de clé prend en charge jusqu'à 15

caractères alphanumériques. La valeur de clé est la clé NTP réelle qui est utilisée pour authentifier ISE comme client sur le serveur NTP. En outre, l'ID de clé doit correspondre à celui configuré sur le serveur NTP. Sélectionnez la valeur HMAC (Hashed Message Authentication Code) requise dans la liste déroulante HMAC.



Étape 3. Cliquez sur OK, puis sur Save Authentication Keys. Vous revenez à l'onglet Configuration du serveur NTP.

Étape 4. Maintenant, dans la liste déroulante des clés, vous voyez l'ID de clé que vous avez configuré à l'étape 3. Cliquez sur l'ID de clé respectif si vous avez configuré plusieurs ID de clé. Cliquez ensuite sur Enregistrer.



Étapes CLI

Étape 1 : configuration de la clé d'authentification NTP.

```
admin(config)# ntp authentication-key ?
<1-65535> Key number >>> This is the Key ID
admin(config)# ntp authentication-key 1 ? >>> Here you can choose the HMAC value
md5 MD5 authentication
sha1 SHA1 authentication
sha256 SHA256 authentication
sha512 SHA512 authentication
admin(config)# ntp authentication-key 1 md5 ? >>> You can choose either to paste the hash of the actual
hash Specifies an ENCRYPTED (hashed) key follows
plain Specifies an UNENCRYPTED plain text key follows

admin(config)# ntp authentication-key 1 md5 plain Ntp123 >>> Ensure there are no spaces given at the en
```

Étape 2 : définition du serveur NTP et association de l'ID de clé configuré à l'étape 1

```
admin(config)# ntp server IP/HOSTNAME ?
key Peer key number
<cr> Carriage return.
```

```
admin(config)# ntp serve IP/HOSTNAME key ?
<1-65535>

admin(config)# ntp serve IP/HOSTNAME key 1 ?
<cr> Carriage return.

admin(config)# ntp serve IP/HOSTNAME key 1
```

Configuration sur le routeur

Le routeur agit en tant que serveur NTP. Configurez ces commandes pour activer le routeur en tant que serveur NTP avec l'authentification NTP.

```
ntp authentication-key 1 md5 Ntp123 >>> The same key that you configured on ISE
ntp authenticate
ntp master STRATUM
```

Vérifier

Sur ISE :

Utilisez la commande show ntp. Si l'authentification NTP réussit, vous devez voir l'ISE à synchroniser avec le serveur NTP.

```
admin# sh ntp
Configured NTP Servers:
NTP_SERVER_IP

Reference ID : 0A6A23B1 (NTP_SERVER_IP)
Stratum : 3
Ref time (UTC) : Fri Mar 26 09:14:31 2021
System time : 0.000008235 seconds fast of NTP time
Last offset : +0.000003193 seconds
RMS offset : 0.000020295 seconds
Frequency : 10.472 ppm slow
Residual freq : +0.000 ppm
Skew : 0.018 ppm
Root delay : 0.000571255 seconds
Root dispersion : 0.000375993 seconds
Update interval : 519.3 seconds
Leap status : Normal >>> If there is any issue in NTP synchronization, it shows "Not synchronised".

210 Number of sources = 1
MS Name/IP address Stratum Poll Reach LastRx Last sample
```

```
===============================================================================
^* NTP_SERVER_IP 2 9 377 100 +3853ns[+7046ns] +/- 684us

M indicates the mode of the source.
^ server, = peer, # local reference clock.

S indicates the state of the sources.
* Current time source, + Candidate, x False ticker, ? Connectivity lost, ~ Too much variability

Warning: Output results can conflict at the time of changing synchronization.

admin#
```

Dépannage

Cette section fournit les informations que vous pouvez utiliser afin de dépanner votre configuration.

1. Si l'authentification NTP ne fonctionne pas, la première étape à assurer est l'accessibilité entre ISE et le serveur NTP.

2. Assurez-vous que la configuration de l'ID de clé correspond sur ISE et sur le serveur NTP.

3. Assurez-vous que l'ID de clé est configuré en tant que clé approuvée sur le serveur NTP.

4. Les versions plus anciennes d'ISE comme 2.4 et 2.6 prennent en charge la commande ntp trusted-key. Assurez-vous donc que vous avez configuré la clé NTP comme trusted-key sur ces versions d'ISE.

5. ISE 2.7 introduit un changement de comportement pour la synchronisation NTP. Alors que les versions précédentes utilisent ntpd, les versions 2.7 et ultérieures utilisent chrony. La chronie a des exigences différentes de celles de la dpntc. L'un des plus remarquables est que, tandis que ntpd se synchronise avec les serveurs qui ont une dispersion de racine allant jusqu'à 10 secondes, chrony se synchronise uniquement lorsque la dispersion de racine est inférieure à 3 secondes. Cela entraîne la désynchronisation des serveurs NTP qui ont pu synchroniser la pré-mise à niveau sur la version 2.7 sans raison évidente.

   En raison de ce changement, les problèmes de synchronisation NTP seraient fréquemment vus si vous utilisez le serveur NTP Windows car ils signalent une très grande dispersion de la racine (3 secondes ou plus) et cela entraîne la chronie d'ignorer le serveur NTP comme trop imprécis.

Défauts De Référence

ID de bogue Cisco CSCvw78019

ID de bogue Cisco CSCvw03693

Informations connexes

- Guide de dépannage et de débogage relatif aux problèmes de protocole NTP (Network Time Protocol)

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.