Configuration de l'échec d'authentification NTP sur ISE 3.4 en raison de la gestion du préfixe HEX

Table des matières

Problème

Cisco Identity Services Engine (ISE) 3.4.0.608 Patch 1 ne parvient pas à se synchroniser avec les serveurs NTP lors de l'utilisation de NTP authentifié avec des clés SHA1 de 40 caractères. Les commandes de clé d'authentification NTP sont acceptées sans erreur sur l'interface de ligne de commande, mais la synchronisation NTP ne se produit pas lorsque l'authentification est activée. Sans authentification, la synchronisation NTP fonctionne correctement. D'autres périphériques réseau, y compris les commutateurs Cisco, s'authentifient avec succès auprès du même serveur NTP en utilisant des ID et des valeurs de clé identiques.

Au cours du dépannage, l'analyse de capture de paquets a révélé que l'ISE envoie des requêtes NTP authentifiées avec l'ID de clé et les champs MAC/authentificateur appropriés. Cependant, les réponses du serveur contiennent un ID de clé de zéro et aucun MAC/authentificateur, ce qui entraîne le rejet de l'authentification par l'ISE. La sortie de débogage sur les commutateurs Cisco agissant comme serveurs NTP affiche « SHA1-Match: 0" indique un échec d'authentification.

Environnement

- Cisco Identity Services Engine (ISE) version 3.4.0.608 avec patch 1
- Authentification NTP utilisant l'algorithme SHA1
- Clés d'authentification NTP de 40 caractères
- Commutateurs Cisco Catalyst 9500 (C9500-24Y4C) exécutant la version 17.12.04
- Appliances serveur NTP avec configuration NTP authentifiée

Résolution

Ce problème est causé par l'ID de bogue Cisco : CSCwq79772, qui affecte la façon dont ISE gère les longues clés d'authentification NTP lorsque le préfixe HEX est requis. Ce bogue a été corrigé dans ISE 3.4 Patch 8 et ISE 3.5 Patch 3.

Comprendre la cause première

Lors de la configuration de clés d'authentification NTP sur des périphériques Cisco, les clés de 20 caractères ou plus sont automatiquement traitées comme des chaînes hexadécimales plutôt que comme du texte brut. Pour cela, ISE doit utiliser le préfixe « HEX: » lors de la configuration de la clé. Cependant, en raison du bogue, ISE n'accepte que 36 caractères d'une clé de 40 caractères en raison du traitement supplémentaire du préfixe « HEX: », ce qui entraîne un échec de l'authentification.

Options de contournement immédiat

Jusqu'à ce que le logiciel ISE puisse être mis à niveau vers une version contenant le correctif, utilisez l'une des solutions suivantes :

Option 1: Utiliser une clé SHA1 de 36 caractères

Configurez le serveur NTP et ISE avec une clé SHA1 de 36 caractères au lieu de la clé de 40 caractères.

Sur ISE :

```
ntp authentication-key 1 sha1 plain HEX:1d3f35b762ab7c21e5f1265dc9762fe421fa
```

Sur le serveur NTP (exemple de commutateur Cisco) :

```
ntp authentication-key 1 sha1 1d3f35b762ab7c21e5f1265dc9762fe421fa
ntp authenticate
```

```
ntp trusted-key 1
```

Option 2: Utiliser l'authentification MD5

Passez de l'authentification SHA1 à l'authentification MD5, qui ne présente pas la même limitation de longueur.

Sur ISE :

```
ntp authentication-key 1 md5 plain [MD5-key-value]
ntp server [NTP-server-IP] key 1
```

Sur le serveur NTP :

```
ntp authentication-key 1 md5 [MD5-key-value]
ntp authenticate
ntp trusted-key 1
```

Étapes de vérification

Après avoir implémenté l'une des solutions, vérifiez la synchronisation NTP :

Sur ISE :

```
show ntp
show clock
```

Sur le commutateur (si vous utilisez le commutateur comme serveur NTP) :

```
show ntp associations
show ntp status
```

Recherchez les indicateurs de synchronisation réussie et vérifiez que l'authentification fonctionne

en confirmant l'échec de la synchronisation NTP lorsque l'authentification est désactivée d'un côté, mais activée de l'autre.

Résolution Permanente

Mettez à niveau ISE vers l'une des versions suivantes qui contient le correctif pour l'ID de bogue Cisco : CSCwq79772 :

- ISE 3.4 Patch 8 (si disponible)
- ISE 3.5 Patch 3 ou ultérieur

Après la mise à niveau, la configuration initiale de la clé SHA1 de 40 caractères fonctionne correctement avec le préfixe HEX.

Motif

Ce problème est causé par l'ID de bogue Cisco : CSCwq7972, dans les versions ISE antérieures à 3.4 Patch 8 et 3.5 Patch 3. Lorsque les clés d'authentification NTP comportent 20 caractères ou plus, les périphériques Cisco les traitent comme des chaînes hexadécimales, ce qui nécessite le préfixe « HEX: » dans la configuration. En raison de ce bogue, ISE gère incorrectement le calcul de la longueur de clé lorsque le préfixe HEX est utilisé, acceptant seulement 36 caractères d'une clé de 40 caractères. Il en résulte une non-concordance de clé entre ISE et le serveur NTP, ce qui entraîne un échec d'authentification lors des tentatives de synchronisation NTP.

Autres informations utiles

- Bogue Cisco CSCwq79772
- Référence des commandes du contrôleur sans fil Cisco - Authentification NTP
- Assistance technique de Cisco et téléchargements

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.