Configurazione dell'errore di autenticazione NTP su ISE 3.4 a causa della gestione del prefisso HEX

Sommario

Problema

Cisco Identity Services Engine (ISE) 3.4.0.608 La patch 1 non riesce a eseguire la sincronizzazione con i server NTP quando si utilizza un protocollo NTP autenticato con chiavi SHA1 lunghe 40 caratteri. I comandi della chiave di autenticazione NTP sono accettati sulla CLI senza errori, ma la sincronizzazione NTP non viene eseguita quando l'autenticazione è abilitata. Senza autenticazione, la sincronizzazione NTP funziona correttamente. Altri dispositivi di rete, inclusi gli switch Cisco, vengono autenticati correttamente con lo stesso server NTP utilizzando valori di chiave e ID di chiave identici.

Durante la risoluzione dei problemi, l'analisi di acquisizione dei pacchetti ha rivelato che ISE invia richieste NTP autenticate con i campi ID chiave e MAC/Authenticator corretti. Tuttavia, le risposte del server contengono un ID chiave di tutti gli zeri e nessun MAC/Authenticator, causando il rifiuto dell'autenticazione da parte di ISE. L'output del debug sugli switch Cisco che agiscono come server NTP è visualizzato "SHA1-Match: 0" che indica un errore di autenticazione.

Ambiente

- Cisco Identity Services Engine (ISE) versione 3.4.0.608 con patch 1
- Autenticazione NTP tramite algoritmo SHA1
- Chiavi di autenticazione NTP di 40 caratteri
- Switch Cisco Catalyst 9500 (C9500-24Y4C) con versione 17.12.04
- Appliance server NTP con configurazione NTP autenticata

Risoluzione

Questo problema è causato dall'ID bug Cisco: CSCwq79772, che influenza il modo in cui ISE gestisce le chiavi di autenticazione NTP lunghe quando è richiesto il prefisso HEX. Questo bug è stato risolto in ISE 3.4 Patch 8 e ISE 3.5 Patch 3.

Comprensione della root cause

Quando si configurano le chiavi di autenticazione NTP sui dispositivi Cisco, le chiavi di almeno 20 caratteri vengono automaticamente considerate come stringhe esadecimali anziché come testo normale. Ciò richiede che ISE utilizzi il prefisso "HEX:" quando si configura la chiave. Tuttavia, a causa del bug, ISE accetta solo 36 caratteri di una chiave di 40 caratteri a causa della gestione del prefisso "HEX:" aggiuntivo, che risulta in un errore di autenticazione.

Opzioni di soluzione immediata

Fino a quando il software ISE non può essere aggiornato a una versione contenente la correzione, utilizzare una delle seguenti soluzioni:

Opzione 1: Usa un tasto SHA1 di 36 caratteri

Configurare sia il server NTP che ISE con un tasto SHA1 di 36 caratteri anziché con il tasto di 40 caratteri.

ISE:

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

Sul server NTP (esempio di switch Cisco):

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

Opzione 2: Usa autenticazione MD5

Passare dall'autenticazione SHA1 all'autenticazione MD5, che non presenta la stessa limitazione di lunghezza.

ISE:

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

Sul server NTP:

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

Fasi di verifica

Dopo aver implementato una soluzione alternativa, verificare la sincronizzazione NTP:

ISE:

```
show ntp
show clock
```

Sullo switch (se si utilizza lo switch come server NTP):

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

Cercare gli indicatori di sincronizzazione riusciti e verificare che l'autenticazione funzioni confermando che la sincronizzazione NTP non riesce quando l'autenticazione è disabilitata su un lato ma abilitata sull'altro.

Risoluzione permanente

Aggiornare ISE a una delle seguenti versioni contenente la correzione per l'ID bug Cisco: CSCwq79772:

- Patch 8 per ISE 3.4 (quando disponibile)
- ISE 3.5 Patch 3 o versioni successive

Dopo l'aggiornamento, la configurazione originale della chiave SHA1 di 40 caratteri funziona correttamente con il prefisso HEX.

Causa

Questo problema è causato dall'ID bug Cisco: CSCwq79772, nelle versioni ISE precedenti alle patch 3.4, 8 e 3.5. Quando le chiavi di autenticazione NTP hanno una lunghezza di 20 caratteri o superiore, i dispositivi Cisco le considerano stringhe esadecimali, che richiedono il prefisso "HEX:" nella configurazione. A causa di questo bug, ISE gestisce in modo errato il calcolo della lunghezza della chiave quando si usa il prefisso HEX, accettando solo 36 caratteri di una chiave di 40 caratteri. Ne consegue una mancata corrispondenza delle chiavi tra ISE e il server NTP, che causa un errore di autenticazione durante i tentativi di sincronizzazione NTP.

Contenuto correlato

- Cisco Bug CSCwq7972
- Guida di riferimento ai comandi di Cisco Wireless Controller - Autenticazione NTP
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).