Konfigurieren eines NTP-Authentifizierungsfehlers auf ISE 3.4 aufgrund der HEX-Präfixbehandlung

Inhalt

Problem

Cisco Identity Services Engine (ISE) 3.4.0.608 Patch 1 kann bei Verwendung von authentifizierten NTPs mit SHA1-Schlüsseln mit 40 Zeichen Länge nicht mit NTP-Servern synchronisiert werden. Die NTP-Authentifizierungsschlüsselbefehle werden von CLI ohne Fehler akzeptiert, aber die NTP-Synchronisierung findet nicht statt, wenn die Authentifizierung aktiviert ist. Ohne Authentifizierung funktioniert die NTP-Synchronisierung ordnungsgemäß. Andere Netzwerkgeräte, darunter Cisco Switches, authentifizieren sich erfolgreich mit demselben NTP-Server und verwenden dabei identische Schlüssel-IDs und Schlüsselwerte.

Bei der Fehlerbehebung zeigte die Paketerfassungsanalyse auf, dass die ISE authentifizierte NTP-Anforderungen mit den richtigen Feldern für Schlüssel-ID und MAC/Authentifizierer sendet. Die Serverantworten enthalten jedoch eine Schlüssel-ID mit allen Nullen und keine MAC/Authentifizierer, sodass die ISE die Authentifizierung ablehnt. Die Debug-Ausgabe auf Cisco Switches, die als NTP-Server fungieren, zeigte "SHA1-Match: 0" für fehlgeschlagene Authentifizierung.

Umwelt

- Cisco Identity Services Engine (ISE) Version 3.4.0.608 mit Patch 1
- NTP-Authentifizierung mit SHA1-Algorithmus
- NTP-Authentifizierungsschlüssel mit 40 Zeichen Länge
- Cisco Catalyst Switches der Serie 9500 (C9500-24Y4C) mit Version 17.12.04
- NTP-Server-Appliances mit authentifizierter NTP-Konfiguration

Auflösung

Dieses Problem wird durch die Bug-ID von Cisco verursacht: CSCwq79772: Diese Eigenschaft beeinflusst, wie ISE lange NTP-Authentifizierungsschlüssel behandelt, wenn das HEX-Präfix erforderlich ist. Dieser Fehler wurde in ISE 3.4 Patch 8 und ISE 3.5 Patch 3 behoben.

Die Ursache verstehen

Bei der Konfiguration von NTP-Authentifizierungsschlüsseln auf Cisco Geräten werden Schlüssel mit mindestens 20 Zeichen automatisch als Hexadezimalzeichenfolgen und nicht als Nur-Text-Schlüssel behandelt. Dazu muss die ISE beim Konfigurieren des Schlüssels das Präfix "HEX:" verwenden. Aufgrund des Fehlers akzeptiert die ISE aufgrund der zusätzlichen "HEX:"-Präfixbehandlung jedoch nur 36 Zeichen eines 40-Zeichen-Schlüssels, was zu einem Authentifizierungsfehler führt.

Sofortige Problemumgehungsoptionen

Verwenden Sie eine der folgenden Problemumgehungen, bis ein Upgrade der ISE-Software auf eine Version mit dem Fix möglich ist:

Option 1: Verwenden einer 36-Zeichen-SHA1-Taste

Konfigurieren Sie den NTP-Server und die ISE mit einem 36-stelligen SHA1-Schlüssel anstelle des 40-stelligen Schlüssels.

Auf der ISE:

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

Auf dem NTP-Server (Beispiel für einen Cisco Switch):

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

```
ntp trusted-key 1
```

Option 2: MD5-Authentifizierung verwenden

Wechseln Sie von der SHA1- zur MD5-Authentifizierung, die nicht dieselbe Längenbeschränkung aufweist.

Auf der ISE:

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

Auf dem NTP-Server

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

Verifizierungsschritte

Nach der Implementierung der Problemumgehung überprüfen Sie die NTP-Synchronisierung:

Auf der ISE:

```
show ntp
show clock
```

Auf dem Switch (wenn Switch als NTP-Server verwendet wird):

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

Prüfen Sie, ob die Synchronisierungsindikatoren erfolgreich sind, und vergewissern Sie sich, dass

die Authentifizierung funktioniert, indem Sie bestätigen, dass die NTP-Synchronisierung fehlschlägt, wenn die Authentifizierung auf einer Seite deaktiviert, auf der anderen jedoch aktiviert ist.

Ständige Entschließung

Aktualisieren Sie ISE auf eine der folgenden Versionen, die die Korrektur für die Cisco Bug-ID enthält: CSCwq79772:

- ISE 3.4 Patch 8 (sofern verfügbar)
- ISE 3.5 Patch 3 oder spätere Version

Nach der Aktualisierung funktioniert die ursprüngliche 40-stellige SHA1-Schlüsselkonfiguration korrekt mit dem HEX-Präfix.

Ursache

Dieses Problem wird durch die Bug-ID von Cisco verursacht: CSCwq79772 in ISE-Versionen vor 3.4 Patch 8 und 3.5 Patch 3. Wenn NTP-Authentifizierungsschlüssel 20 Zeichen oder mehr enthalten, behandeln Cisco Geräte diese als hexadezimale Zeichenfolgen, die das Präfix "HEX:" in der Konfiguration erfordern. Aufgrund dieses Fehlers verarbeitet die ISE die Berechnung der Schlüssellänge falsch, wenn das HEX-Präfix verwendet wird. Dabei werden nur 36 Zeichen eines Schlüssels mit 40 Zeichen akzeptiert. Dies führt zu einer Schlüsselungleichheit zwischen der ISE und dem NTP-Server, was zu einem Authentifizierungsfehler während der NTP-Synchronisierungsversuche führt.

Verwandte Inhalte

- Cisco Bug CSCwq79772
- Cisco Wireless Controller Command Reference - NTP-Authentifizierung
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.