NTP-verificatiefout configureren op ISE 3.4 vanwege HEX Prefix-verwerking

Inhoud

uitgifte

Cisco Identity Services Engine (ISE) 3.4.0.608 Patch 1 synchroniseert niet met NTP-servers bij gebruik van geverifieerde NTP met SHA1-sleutels met een lengte van 40 tekens. De opdrachten voor de NTP-verificatiesleutel worden zonder fouten op de CLI geaccepteerd, maar NTP-synchronisatie vindt niet plaats wanneer de verificatie is ingeschakeld. Zonder verificatie werkt NTP-synchronisatie correct. Andere netwerkapparaten, waaronder Cisco-switches, kunnen met succes worden geverifieerd met dezelfde NTP-server met dezelfde sleutel-ID en sleutelwaarden.

Tijdens het oplossen van problemen bleek uit de analyse van het vastleggen van pakketten dat ISE geverifieerde NTP-verzoeken verzendt met de juiste velden Key ID en MAC / authenticator, maar de serverantwoorden bevatten een Key ID van alle nullen en geen MAC / authenticator, waardoor ISE de verificatie weigert. Foutopsporingsuitvoer op Cisco-switches die optreden als NTP-servers, wordt "SHA1-Match: 0" weergegeven, wat wijst op een verificatiefout.

milieu

- Cisco Identity Services Engine (ISE) versie 3.4.0.608 met Patch 1
- NTP-verificatie met behulp van SHA1-algoritme
- NTP-verificatiesleutels met een lengte van 40 tekens
- Cisco Catalyst 9500 Switches (C9500-24Y4C) met versie 17.12.04
- NTP-serverapparaten met geverifieerde NTP-configuratie

resolutie

Dit probleem wordt veroorzaakt door Cisco bug ID: CSCwq79772, wat van invloed is op hoe ISE omgaat met lange NTP-verificatiesleutels wanneer het HEX-prefix vereist is. Deze bug werd opgelost in ISE 3.4 Patch 8 en ISE 3.5 Patch 3.

Begrijpen van de oorzaak

Bij het configureren van NTP-verificatiesleutels op Cisco-apparaten worden sleutels van 20 tekens of langer automatisch behandeld als hexadecimale tekenreeksen in plaats van platte tekst. Hiervoor moet ISE het voorvoegsel "HEX:" gebruiken bij het configureren van de sleutel. Vanwege de bug accepteert ISE echter slechts 36 tekens van een sleutel van 40 tekens vanwege de extra "HEX:" prefix-verwerking, wat resulteert in een authenticatiefout.

Opties voor onmiddellijke tijdelijke oplossing

Gebruik een van de volgende oplossingen totdat ISE-software kan worden geüpgraded naar een versie met de oplossing:

Optie 1: Gebruik een SHA1-sleutel van 36 tekens

Configureer zowel de NTP-server als ISE met een SHA1-sleutel van 36 tekens in plaats van de sleutel van 40 tekens.

Over ISE:

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

Op de NTP-server (voorbeeld van Cisco switch):

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

Optie 2: MD5-verificatie gebruiken

Switch van SHA1 naar MD5-verificatie, waarvoor niet dezelfde lengtebeperking geldt.

Over ISE:

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

Op de NTP-server:

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

Verificatiestappen

Controleer na het implementeren van een van beide oplossingen de NTP-synchronisatie:

Over ISE:

```
show ntp
show clock
```

Op de switch (als u switch als NTP-server gebruikt):

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

Zoek naar succesvolle synchronisatie-indicatoren en controleer of de verificatie werkt door te bevestigen dat NTP-synchronisatie mislukt wanneer de verificatie aan de ene kant is uitgeschakeld maar aan de andere kant is ingeschakeld.

permanente resolutie

Upgrade ISE naar een van deze versies die de oplossing bevat voor Cisco bug ID: CSCwq79772:

- ISE 3.4 Patch 8 (indien beschikbaar)
- ISE 3.5 Patch 3 of hoger

Na het upgraden werkt de oorspronkelijke 40-tekens SHA1-sleutelconfiguratie correct met het HEX-prefix.

Oorzaak

Dit probleem wordt veroorzaakt door Cisco bug ID: CSCwq79772, in ISE-versies voorafgaand aan 3.4 Patch 8 en 3.5 Patch 3. Wanneer NTP-verificatiesleutels 20 tekens of langer zijn, behandelen Cisco-apparaten deze als hexadecimale tekenreeksen, waarvoor het "HEX:"-prefix in de configuratie vereist is. Vanwege deze bug verwerkt ISE de berekening van de sleutellengte onjuist wanneer het HEX-prefix wordt gebruikt, waarbij slechts 36 tekens van een sleutel van 40 tekens worden geaccepteerd. Dit resulteert in een belangrijke mismatch tussen ISE en de NTP-server, waardoor de verificatie mislukt tijdens NTP-synchronisatiepogingen.

Gerelateerde inhoud

- Cisco-bug CSCwq79772
- Cisco Wireless Controller opdrachtreferentie - NTP-verificatie
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.