

ISE SFTP RSA Key Authentication Timeout-fout

Inhoud

uitgifte

Een SFTP-repository die is geconfigureerd met RSA-sleutelverificatie werkt met succes op één ISE-node (ise1), maar faalt op een andere ISE-node (ise2) waarop ISE 3.4 wordt uitgevoerd. Op de defecte node zijn de SSH-handdruk en servervalidatie succesvol voltooid, maar de verificatie met openbare sleutel is niet voltooid en de SFTP-sessie wordt afgesloten met een foutbericht "sftp_select Error: timeout!".

Wanneer u probeert de inhoud van de SFTP-repository aan te bieden met de opdracht `show repository SFTP` op de betreffende ISE-node, treedt deze foutreeks op:

```
device/admin# show repository SFTP
6 [4005534]:[info] transfer: cars_xfer.c[333] [system]: sftp dir of repository SFTP requested
6 [4005534]:[info] transfer: cars_xfer_util.c[2654] [system]: Server validation successful 10.50.60.200
7 [4005534]:[debug] transfer: sftp_handler.c[1295] [system]: Running sftp command: 10.50.60.200 will.ki
6 [4005534]:[info] transfer: sftp_handler.c[695] [system]: DEBUG: local user: admin UID: 0 sftp_run_par
7 [4005534]:[debug] transfer: sftp_handler.c[705] [system]: fd is:7
7 [4005535]:[debug] transfer: sftp_handler.c[327] [system]: Executing SFTP command: 0 admin /usr/bin/sf
3 [4005534]:[error] transfer: sftp_handler.c[417] [system]: sftp_select Error: timeout!
7 [4005534]:[debug] transfer: sftp_handler.c[1136] [system]: sftp parent status -999
% Failure occurred during request
```

Dit voorkomt het gebruik van de SFTP-repository van de betreffende ISE-node voor kritieke ISE-functies zoals back-upbewerkingen.

milieu

- Cisco Identity Services Engine (ISE) versie 3.4.0
- Implementatie van ISE met meerdere nodes met ten minste twee nodes (ise1 en ise2)
- SFTP-repository geconfigureerd met RSA-sleutelverificatie

- SSH-sleutelgebaseerde verificatie met RSA-privésleutel (/home/admin/.ssh/id_rsa)
- SFTP-server toegankelijk
- Wachtwoordverificatie uitgeschakeld (-oPasswordAuthentication=no)

resolutie

Deze zaak wordt momenteel onderzocht door het engineeringteam. Het probleem is geescaleerd voor root log analyse om de onderliggende oorzaak van de SFTP time-out op de getroffen ISE node te bepalen.

Voer op basis van de debug-uitvoer de stappen voor probleemoplossing uit die in de volgende secties worden beschreven om aanvullende informatie te verzamelen.

Stap 1: Controleer de consistentie van de SFTP-repository tussen nodes

Vergelijk de configuratie van de SFTP-repository op beide ISE-nodes om er zeker van te zijn dat ze identiek zijn.

Stap 2: Controleer SSH Key File Permissions and Ownership

Controleer of het SSH-bestand met de privésleutel (/home/admin/.ssh/id_rsa) de juiste machtigingen en eigenaarschap heeft voor de betreffende node.

Stap 3: Netwerkconnectiviteit testen

Bevestig dat de betreffende ISE-node de SFTP-server op poort 22 kan bereiken en dat er geen problemen zijn met blokkering op netwerkniveau.

Stap 4: Extra foutopsporing inschakelen

Schakel meer uitgebreide SSH/SFTP-foutopsporing in om gedetailleerde informatie over de verificatiefout vast te leggen.

Van de aangetaste knoop CLI:

1.- Schakel deze foutopsporingen in met opdrachten:

- Foutopsporingskopie 7
- Foutopsporingsoverdracht 7

2.- Gebruik de opdracht `show repository xxxxx` nadat u foutmeldingen hebt ingeschakeld om meer informatie vast te leggen.

Stap 5: Vergelijk SSH Key Fingerprints

Controleer of de openbare SSH-sleutel op de SFTP-server overeenkomt met de privésleutel die door de betreffende ISE-node wordt gebruikt.

Het probleem is opgelost door de juiste wachtwoordzin te identificeren die wordt gebruikt om de RSA-sleutel op de SPAN-node te genereren en de repository-instellingen opnieuw te configureren om uit te lijnen met de geldige referenties.

Tussentijdse workaround

U wordt geadviseerd om de wachtwoordzin handmatig te verifiëren met behulp van `ssh-keygen -y -f /home/admin/.ssh/id_rsa` op de CLI om te bevestigen welk wachtwoord de privésleutel succesvol heeft ontgrendeld voordat u de configuratie van de repository opnieuw toepast in de GUI.

Stappen om de RSA-sleutel te regenereren:

1.- Open de betreffende knooppunt CLI.

2.- Verwijder de oude RSA Key met de `crypto key delete rsa` commando.

3.- Genereer een nieuwe RSA-sleutel met de gewenste wachtwoordzin met de crypto-sleutel genereer rsa-wachtwoordzin XXXXXXXXXXXXXXX opdracht.



Opmerking: wachtwoordgroep moet uit 13 of meer tekens bestaan.

4.- Haal de nieuwe RSA public key om te importeren naar het andere systeem met de show crypto key commando.

Oorzaak

Gebruikersfout / configuratiefout. Uit het onderzoek is gebleken dat de storing in de authenticatie van de repository op de secundaire node is veroorzaakt door een mismatch tussen de verwachte wachtwoordzin en de wachtwoordzin die wordt gebruikt om de opgeslagen RSA-privésleutel te beveiligen. Hierdoor kon het cryptografische subsysteem de sleutel voor het ondertekenen van de SSH-verificatie-uitdaging niet decoderen.

Gerelateerde inhoud

- [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.