Cisco Secure Client VPN-verbindingsfout met SAML-verificatie en Bencode Dictionary-fouten

Inhoud

uitgeven

VPN-verbindingen die gebruikmaken van Cisco Secure Client kunnen niet worden vastgesteld bij het gebruik van SAML-verificatie met Google IdP. Hoewel SAML-verificatie succesvol is aan de IdP-kant, mislukt de client tijdens de verwerking na verificatie en overgaat naar een niet-verbonden status, waardoor de VPN-tunnel niet kan worden gemaakt.

milieu

- Cisco Secure Client versie 5.1.13.177
- SAML-verificatie geconfigureerd met Google IdP
- Veilige toegang - Veilige externe toegang voor clients (VPN, houding, privébron)
- Google IdP-verificatielogboeken tonen succesvolle SAML-verificatie

resolutie

Het probleem is opgelost door de Cisco Secure Client opnieuw te installeren. De volgende aanpak voor probleemoplossing werd gedocumenteerd:

Eerste diagnostische stappen

Stap 1: verzamel DART-logs van het getroffen eindpunt - https://www.cisco.com/c/en/us/support/docs/security/secure-client/221919-collect-dart-bundle-for-secure-client.html

Extract Dart Bundle > Cisco Secure client > Anyconnect VPN > Logs > Under VPN Folder > AnyConnectVPN.txt - laat de volgende fouten zien tijdens het lezen van interne instellingen, waarbij de volgende fouten continu verschijnen:

- Bencode-woordenboek internaliseren mislukt
- Bencode-woordenboek is niet gemaakt
- PHONEHOMEVPN_ERROR_UNEXPECTED
- GLOBAL_ERROR_UNEXPECTED

Stap 2: Verifieer de SAML-verificatiestatus aan de IdP-zijde

Bevestig dat Google IdP-logs succesvolle SAML-verificatie tonen om het probleem te isoleren voor de verwerking van de verificatie aan de clientzijde.

Implementatie van afwikkeling

Stap 1: Cisco Secure Client opnieuw installeren

De installatie van de bestaande Cisco Secure Client ongedaan maken en de clientsoftware opnieuw installeren.

Stap 2: VPN-connectiviteitsherstel verifiëren

Nadat u de VPN-verbinding opnieuw hebt geïnstalleerd, test u deze met SAML-verificatie om te bevestigen dat de verbinding met succes tot stand is gebracht en dat de tunnel correct is gemaakt.

De herinstallatie van Cisco Secure Client herstelde VPN-functionaliteit, waardoor een succesvolle SAML-verificatie en tunnelinstelling mogelijk werd.

Oorzaak

De hoofdoorzaak lijkt verband te houden met beschadigde interne configuratiegegevens binnen de installatie van de Cisco Secure Client, met name van invloed op de mogelijkheid van de component CPhoneHomeVPN/PhoneHomeAgent om Bencode-woordenboekgegevens te verwerken tijdens verwerking na verificatie. De herhaalde fouten "Bencode dictionary internalize failed" en "Failed to create Bencode dictionary" geven aan dat de client niet in staat was om de interne configuratiegegevens die nodig zijn voor het tot stand brengen van de VPN-tunnel na succesvolle SAML-verificatie goed te ontleden of te verwerken.

Het probleem werd opgelost door de client opnieuw te installeren, wat suggereert dat het probleem verband hield met beschadigde gegevens aan de clientzijde in plaats van server-side configuratie- of IdP-integratieproblemen.

Verwante 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.