

Secure Client AnyConnect VPN-toegang geweigerd vanwege problemen met de naleving van de beveiligingspositie van het eindpunt

Inhoud

uitgifte

Meerdere gebruikers kunnen geen verbinding maken met AnyConnect VPN en Zero Trust Access (ZTA) en ontvangen de foutmelding "Login geweigerd. Uw omgeving voldoet niet aan de toegangscriteria die door uw beheerder zijn gedefinieerd."

Het probleem houdt verband met de naleving van de eindpunthouding, waarbij de vereiste voor de Endpoint Security Agent wordt gerapporteerd als niet-overeenkomend. Gebruikers ervaren VPN- en ZTA-toegangswegering wanneer ze proberen verbinding te maken via Cisco Secure Client.

De postuur evaluatie laat zien dat de Trellix Endpoint Security houding faalt op de getroffen eindpunten, waardoor succesvolle authenticatie naar de VPN-service wordt voorkomen.

milieu

- Cisco Secure Client (AnyConnect en Zero Trust Access)
- Trellix Endpoint Security Agent versie 5.8.4.505
- Profiel VPN-houding: KFIN_SECURE_VPN met handhaving van endpoint-beveiligingsagent
- Houdingseis: Endpoint-beveiligingsagent die de laatste 14 dagen wordt bijgewerkt
- Windows-eindpunten met Trellix Agent Service
- Umbrella Agent-processen gedetecteerd op eindpunten

resolutie

Het probleem werd opgelost door de problemen met de naleving van de houding van de Trellix Endpoint Security-agent aan te pakken. De stappen voor probleemoplossing en -oplossing die in de volgende secties worden beschreven, zijn geïmplementeerd.

Stap 1: De configuratie van het postuur-profiel valideren

Controleer het profiel van de VPN-houding om de vereisten van de endpoint-beveiligingsagent te bevestigen. Het KFIN_SECURE_VPN-profiel bepaalt dat een endpoint-beveiligingsagent binnen de laatste 14 dagen moet worden uitgevoerd en bijgewerkt.

Stap 2: De beveiligingsstatus van Trellix Endpoint verifiëren

Controleer de huidige status van de Trellix Endpoint Security-agent op de betreffende eindpunten:

```
Trellix Agent Service: masvc.exe  
Version: 5.8.4.505  
Install Location: C:\Program Files\McAfee\Agent\  
Display Name: Trellix Agent  
Publisher: Trellix
```

Stap 3: Trellix Endpoint Security opnieuw installeren

Voer een volledige herinstallatie van Trellix Endpoint Security uit op de betreffende eindpunten:

1. De bestaande Trellix Endpoint Security-agent volledig verwijderen.
2. Start het systeem opnieuw op.
3. Installeer de nieuwste goedgekeurde versie van de Trellix-agent volgens de organisatorische normen.

4. Controleer of de agent na de installatie goed werkt.

5. Bevestig dat handtekening-/inhoudsupdates met succes zijn voltooid.

Stap 4: TRACE-registratie inschakelen voor Cisco Secure Client (ZTA)

Schakel gedetailleerde logboekregistratie in om de details van de postuur-evaluatie vast te leggen.

Maak het bestand logconfig.json met deze inhoud:

```
{ "global": "DBG_TRACE" }
```

Plaats het bestand in de juiste directory:

- Windows: C:\ProgramData\Cisco\Cisco Secure Client\ZTA
- macOS: /opt/cisco/secureClient/zta

Start de Cisco Secure Client/ZTA-service opnieuw nadat u het bestand hebt gemaakt.

Stap 5: Verzamel bijgewerkte DART-bundel

Nadat u de wijzigingen hebt geïmplementeerd, verzamelt u een nieuwe DART-bundel om de resolutie te valideren en de juiste detectie van de naleving van de houding te bevestigen.

Oorzaak

De hoofdoorzaak werd geïdentificeerd als Trellix Endpoint Security agent houding compliance problemen. Het profiel van de VPN-houding vereiste dat een endpoint-beveiligingsagent de afgelopen 14 dagen met updates werd uitgevoerd, maar de Trellix Endpoint Security-agent voldeed niet aan deze nalevingscriteria. De evaluatiemodule voor de houding kon de status van de veiligheidsagent voor het eindpunt niet goed detecteren of valideren, wat resulteerde in

toegangsweigering voor VPN- en ZTA-verbindingen. Het probleem hield specifiek verband met de configuratie van de Trellix-agent en vereiste interventie van het Trellix-ondersteuningsteam om de onderliggende problemen met de naleving van de agent op te lossen.

Gerelateerde inhoud

- [Gedetailleerde ZTNA-logboeken verzamelen voor probleemoplossing](#)
- [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.