Beveiligde toegang VPN-beheerder Verbreking van verbindingen opnieuw instellen vanwege beperking van de lengte van VPN-profielnamen

Inhoud

uitgeven

Externe toegang VPN-gebruikers ondervonden intermitterende verbroken verbindingen op Cisco Secure Access tijdens actieve sessies .De Cisco Secure Access (CSA)-logs registreerden deze verbroken verbindingen als Administrator Reset ondanks dat er op dat moment geen geplande onderhoudsactiviteit plaatsvond. De verbroken verbindingen beïnvloedden gebruikers met externe toegang tijdens normale bedrijfsactiviteiten en veroorzaakten onverwachte sessiebeëindigingen terwijl gebruikers actief waren verbonden met de VPN-service.

De ontkoppelingsgebeurtenissen werden in de logboeken voor externe toegang weergegeven als items voor het opnieuw instellen van beheerders, die meestal wijzen op administratieve interventie of het beëindigen van door het systeem geïnitieerde sessies. Er werden echter geen administratieve handelingen met betrekking tot het systeem verricht gedurende het gerapporteerde tijdsbestek.

milieu

- Cisco Secure Access (CSA) - VPN-service voor externe toegang
- VPN-profielconfiguraties met namen van meer dan 46 tekens

resolutie

De oplossing omvat het implementeren van een tijdelijke oplossing om de beperking van de lengte

van de VPN-profielnaam aan te pakken die de beheerdersinstellingen veroorzaakt:

Onmiddellijke tijdelijke oplossing

Stap 1: VPN-profielen identificeren met namen van meer dan 46 tekens

Bekijk alle bestaande VPN-profielconfiguraties in het Cisco Secure Access-dashboard en identificeer profielen met namen die langer zijn dan 46 tekens.

Stap 2: VPN-profielen hernoemen om te voldoen aan de tekenlimiet

Wijzig de naam van alle VPN-profielen die meer dan 46 tekens bevatten om er zeker van te zijn dat ze 46 tekens of minder lang zijn. Dit kan worden gedaan via de beheerinterface van Cisco Secure Access.

Stap 3: Monitor voor ontkoppelingsgebeurtenissen

Nadat u de naamswijzigingen van het VPN-profiel hebt geïmplementeerd, controleert u de logboeken voor Externe toegang om te controleren of er tijdens normale bewerkingen geen beheerdersinstellingen meer voorkomen.

Oplossing op lange termijn

Er wordt een permanente oplossing ontwikkeld om de GUI-beperking aan te pakken waarmee VPN-profielnamen de back-endverwerkingslimiet kunnen overschrijden. Deze oplossing handhaaft de limiet van 46 tekens op het niveau van de gebruikersinterface, waardoor het maken van VPN-profielen met namen die problemen met de back-endverwerking veroorzaken, wordt voorkomen.

Het ontwikkelingsteam werkt aan de implementatie van de juiste validatie in de GUI om de lengte van de VPN-profielnaam te beperken tijdens het maken en wijzigen, waardoor dit probleem in toekomstige configuraties wordt voorkomen.

Aanvullende overwegingen

In sommige gevallen kunnen instellingen voor energiebeheer van de Wi-Fi-adapter op clientapparaten bijdragen aan verbindingsproblemen. Als de verbindingen verbroken blijven nadat de correctie voor de lengte van de VPN-profielnaam is geïmplementeerd, moet u controleren of de energiebesparende functies van de Wi-Fi-adapter zijn uitgeschakeld op de betreffende clientapparaten, omdat deze instellingen kunnen leiden tot herverbindingsgebeurtenissen die in de logboeken worden weergegeven als items voor het opnieuw instellen van de beheerder.

Oorzaak

De hoofdoorzaak van de beheerdersreset-gebeurtenissen is een back-endverwerkingsbeperking in Cisco Secure Access, waarbij VPN-profielnamen van meer dan 46 tekens systeemfouten veroorzaken tijdens sessiebeheer. Wanneer het backend-systeem VPN-profielen tegenkomt met namen die langer zijn dan deze limiet, wordt een Administrator Reset geactiveerd om de getroffen sessies te beëindigen als een beschermende maatregel.

Dit probleem treedt op omdat de GUI-interface gebruikers toestaat om VPN-profielnamen langer dan 46 tekens te maken, maar het backend-verwerkingssysteem heeft een strikte limiet van 46 tekens. Wanneer grote tekenreekslengtes door de backend worden verwerkt, wordt een gebeurtenis voor het opnieuw instellen van de beheerder geregistreerd en wordt de verbinding met de bijbehorende VPN-sessies verbroken.

Verwante inhoud

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.