Veilige toegang RAVPN-verificatie mislukt met Duo SAML-integratie

Inhoud

uitgifte

Wanneer gebruikers proberen verbinding te maken met Cisco Secure Access Remote Access VPN (RAVPN) met behulp van Duo als de Identity Provider (IDP) met Active Directory-integratie op de achtergrond, ervaren gebruikers verificatiefouten ondanks succesvolle verificatie op het niveau van de Duo-portal.

De specifieke symptomen zijn onder meer:

- Duo Portal geeft een succesbericht voor verificatie weer.
- Cisco SecureClient geeft een foutmelding "Verificatie mislukt" weer direct na het succes van de Duo.
- Duo-logs tonen de status "Toegankelijkheid verleend".
- In de logboeken van het Cisco Secure Access-portaal wordt de status "AAA-fout" weergegeven.

Hierdoor wordt de verbinding verbroken wanneer de externe identiteitsprovider een succesvolle verificatie bevestigt, maar de VPN-client de verbinding niet tot stand kan brengen vanwege fouten in de verificatie-validatie binnen de Secure Access-infrastructuur.

milieu

- Implementatie van Cisco Secure Access RAVPN
- Duo Security als SAML Identity Provider
- Active Directory-integratie met Duo

- Cisco SecureClient voor VPN-connectiviteit
- SAML-gebaseerde verificatiestroom

resolutie

De verificatiefout is verholpen door de toewijzing van gebruikerskenmerken tussen Duo en Cisco Secure Access te corrigeren. De stappen die in de volgende secties worden beschreven, zijn genomen om het probleem te identificeren en op te lossen.

Stap 1: Zoeken naar activiteiten controleren

1.- Log in op het Cisco Secure Access Dashboard. Klik op Monitor> Logboeken voor externe toegang.

2.- Controleer op het veld Gebruikersnaam onder de foutmeldingen voor autorisatiecontrole.

3.- Vergelijk het met de UPN-waarde onder Verbinden > Gebruikers en groepen.

Cisco Secure Access kijkt naar de waarde van de gebruikersnaam voor de autorisatiecontrole.

De gebruikersnaam die door Duo werd doorgegeven, kwam niet overeen met de waarde van de gebruikersnaam die voor die gebruiker is opgegeven onder Gebruiker en Groepen.

Uit het onderzoek bleek:

- E-mailadres van de gebruiker: user@gmail.com
- Gebruikersnaam (UPN-gebruikersnaam)

Stap 2: Duo Configuration Adjustment

De resolutie hield in dat de configuratie van de Duo SAML werd gewijzigd om een juiste toewijzing

van gebruikerskenmerken te garanderen:

- Ga naar het Duo Admin Panel.
- Ga naar de SAML-toepassingsconfiguratie voor Cisco Secure Access.
- Wijzig de toewijzing van het gebruikerskenmerk om het e-mailadres te verzenden dat moet overeenkomen met de waarde van de gebruikersnaam en de hoofdnaam voor die gebruiker onder Gebruiker en Groepen.
- De configuratiewijzigingen opslaan.

Stap 4: Verificatie

Nadat de Duo-configuratie was aangepast, werd de verificatiestroom getest en met succes geverifieerd. De gebruiker kon verbinding maken met behulp van Remote Access VPN zonder verificatiefouten.

Oorzaak

De hoofdoorzaak van de verificatiefout was een mismatch tussen de beweringen van Duo SAML en de verwachtingen van Cisco Secure Access. Duo is geconfigureerd om de gebruikersnaam onder User Principal Name (UPN) te verzenden in SAML-beweringen, terwijl Cisco Secure Access is geconfigureerd om het e-mailadres van de gebruiker te verwachten. Deze mismatch zorgde ervoor dat de verificatie mislukte op het niveau van Secure Access ondanks succesvolle verificatie op het niveau van Duo IDP, wat resulteerde in de "AAA-fout" die werd aangemeld bij Secure Access, terwijl Duo-logs "toegang verleend" toonden.

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.