

ZTNA-clientfout " Active Directory-integratie niet gedetecteerd voor dit gebruikersapparaat" op apparaten die zijn aangesloten op een netwerk

Inhoud

uitgifte

Gebruikers die de ZTNA-functionaliteit testen, ervaren intermitterende fouten waarbij de ZTNA-client "Active Directory Integration not detected for this user device" weergeeft op apparaten met Entra-join. Deze fout is van voorbijgaande aard en inconsistent tussen gebruikers, en verschijnt onvoorspelbaar tijdens ZTNA-toegangscontroles. Sommige gebruikers met Entra-aangesloten apparaten komen deze fout nooit tegen, terwijl anderen deze meerdere keren ervaren. De fout verdwijnt meestal na een periode zonder tussenkomst van de gebruiker.

Het probleem lijkt verband te houden met postuur-evaluatieprocessen waarbij afzonderlijke toegangsregels worden geconfigureerd voor Entra-gekoppelde en on-premises AD-gekoppelde apparaten. Tijdens deze houdingscontroles kunnen getroffen gebruikers worden gemarkeerd of geblokkeerd om toegang te krijgen tot ZTNA-bronnen, wat van invloed is op hun vermogen om verbinding te maken met interne systemen via het Zero Trust Network Access-framework.

milieu

- Ondersteuning voor oplossing (SSPT - contract vereist)
- Beveiligde toegang - Zero Trust Access (ZTNA, houding, client-based, inschrijving, privébron)
- Gemengde omgeving met zowel Entra-domeingekoppelde als on-premise Active Directory-domeingekoppelde apparaten
- Aparte profielen voor de houding die zijn geconfigureerd voor Entra-apparaten en AD-apparaten op locatie
- Beleidsregels voor dubbele toegang: "Alle interne bronnen - Entra-apparaten" en "Alle

interne bronnen - Mac en On-Prem DS"

- Meerdere gebruikers in testgroep in de hele organisatie

resolutie

Volg de stappen voor probleemoplossing en verificatie die in de volgende sectie worden beschreven om dit probleem met de intermitterende Active Directory-integratie op te lossen.

Stap 1: ZTNA-clientversie bijwerken

Upgrade naar de nieuwste ZTNA-clientversie 5.1.16 en test of het probleem zich blijft voordoen met de bijgewerkte clientsoftware.

Stap 2: Verzamel gedetailleerde voorvalinformatie

Wanneer de fout optreedt, documenteert u deze informatie:

- Exacte tijdstempels van wanneer de fout verschijnt
- Getroffen gebruikersnamen en apparaat-id's
- Besturingssysteemversies van getroffen apparaten
- Gebruikerslocaties en netwerkcontext tijdens het optreden van een fout
- Duur van de persistentie van de fout vóór de automatische oplossing

Stap 3: Controleer de status van de apparaatregistratie

Voer tijdens het optreden van een fout deze opdracht op het betreffende apparaat uit om de registratiestatus van het domein te controleren:

dsregcmd /status

Leg de volledige uitvoer van deze opdracht vast om de registratiestatus van de Entra ID van het apparaat te controleren en eventuele inconsistenties in de registratie te identificeren.

Stap 4: Instellingen apparaataccount documenteren

Navigeer naar Instellingen > Accounts > Toegang tot werk of school en maak een schermafbeelding van de accountconfiguratie tijdens een foutmelding om de verbindingstatus van het apparaatdomein te verifiëren vanuit het perspectief van de gebruikersinterface.

Stap 5: DART-logboeken en foutscreenshots bekijken

Verzamel en analyseer de DART-uitvoer (Data Analysis and Reporting Tool) van getroffen apparaten, samen met foutscreenshots om patronen in het posturevaluatieproces te identificeren die de intermitterende detectiefouten kunnen veroorzaken.

Stap 6: Een workaround toepassen

Het gedrag wordt weergegeven in overeenstemming met een probleem met de timing tijdens het opstarten van het systeem, waarbij de ZTNA-client de eerste posturecontrole kan uitvoeren voordat Windows de initialisatie van Entra (Azure AD) na een herstart volledig heeft voltooid. Dit kan tijdelijk resulteren in het bericht "Active Directory Integration not detected for this user device", ook al is het apparaat correct aangesloten op Entra.

Als eerste en eenvoudige oplossing wordt aanbevolen om de ZTNA-agent zo te configureren dat deze met een korte vertraging wordt opgestart.

Stappen

1.- Open Services (services.msc).

2.- Zoek Cisco Secure Client – Zero Trust Access Agent.

3.- Klik met de rechtermuisknop op Eigenschappen.

4.- Stel het opstarttype in op Automatisch (vertraagd opstarten).

5.- Klik op Toepassen en OK.

6.- Start de machine opnieuw op en test de ZTNA-toegang.

Deze vertraagde opstart (doorgaans ~60–120 seconden) geeft Entra de tijd om de status van join, Azure AD PRT en Windows Identity Services (WAM) volledig te initialiseren voordat de ZTNA-postuur-evaluatie wordt uitgevoerd.

Oorzaak

De intermitterende "Active Directory Integration not detected"-fout lijkt verband te houden met inconsistenties in het postuur-evaluatieproces voor apparaten met Entra-join. Het probleem is waarschijnlijk het gevolg van timing- of synchronisatieproblemen tijdens de verificatie van het apparaatdomein binnen het ZTNA-evaluatiekader voor de houding van de client. Aangezien er voor apparaten met Entra-join en AD-joined on-premises aparte profielen nodig zijn vanwege beperkingen van domeinherkenning, kan het evaluatieproces soms niet goed het Entra-domeinlidmaatschap identificeren, wat resulteert in de tijdelijke foutstatus.

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.