

Probleem met privétoegang oplossen met ZTNA CLAP/BAP via Resource Connectors als gevolg van DNS-storing

Inhoud

[uitgifte](#)

[milieu](#)

[resolutie](#)

[Stap 1: Vergelijk DNS-configuratie tussen omgevingen](#)

[Stap 2: Alternatieve DNS-serverconfiguratie testen](#)

[Stap 3: DNS-resolutie en -connectiviteit valideren](#)

[Oorzaak](#)

[Gerelateerde inhoud](#)

- [uitgifte](#)
 - [milieu](#)
 - [resolutie](#)
 - [Stap 1: Vergelijk DNS-configuratie tussen omgevingen](#)
 - [Stap 2: Alternatieve DNS-serverconfiguratie testen](#)
 - [Stap 3: DNS-resolutie en -connectiviteit valideren](#)
 - [Oorzaak](#)
 - [Gerelateerde inhoud](#)
-

uitgifte

Een private resource die is geconfigureerd voor Zero Trust Network Access (ZTNA) functioneert correct wanneer de resourceconnector in de ontwikkelingsomgeving wordt gebruikt. Wanneer de configuratie van de privébron echter wordt gewijzigd om de bronconnector in de productieomgeving te gebruiken, mislukt de toegang tot de privébron of verbinding met DNS-gerelateerde fouten. De verbinding raakt de standaard blokregel, waardoor een succesvolle validatie van de nieuwe productiemiddelenconnector wordt voorkomen voordat particuliere productiemiddelen erdoorheen worden geleid.

De specifieke symptomen zijn onder meer:

- DNS-foutfouten geregistreerd voor de productieresourceconnector
- Verbindingsfouten als gevolg van het raken van de standaard blokregel in het activiteitenzoekrapport
- Onmogelijkheid om de functionaliteit van de productiemiddelenconnector te valideren
- Mogelijke gevolgen voor toegang tot privébronnen via ZTNA CLAP met Resource Connector

Netwerkconnectiviteit is geverifieerd, inclusief succesvolle DNS-resolutie van de private webserver hostname direct productie van resource connector en TCP-connectiviteit naar poort 8443 op de Ubuntu-server. Alles goed, maar toch krijgen we DNS-foutmelding in de productiemiddelenconnector WAAROM?

milieu

- Technologie: ondersteuning voor oplossingen (SSPT - contract vereist)
- Subtechnologie: beveiligde toegang - Zero Trust Access (ZTNA, houding, clientgebaseerd, inschrijving, privébron)
- Productfamilie: veilige toegang, zero trust/ZTNA, bronconnector
- Target Private Application/Server: Ubuntu-server toegankelijk op TCP-poort 8443
- Netwerkkomponenten: Resourceconnectors in zowel DEV- als PROD-omgevingen

resolutie

De aanpak voor probleemoplossing is gericht op DNS-configuratieverschillen tussen de connectors voor ontwikkeling en productiemiddelen. Houd er rekening mee dat de ontwikkelingsresourceconnector werkt scenario - Toegang tot privébronnen met succes. De connector voor productiemiddelen werkt niet, de PR is niet toegankelijk en er wordt een DNS-fout weergegeven in RC > Netwerkverbindingen > Resourceconnector > DNS-fout.

Volg deze systematische stappen om de DNS-oplossingsproblemen te identificeren en op te lossen.

Stap 1: Vergelijk DNS-configuratie tussen omgevingen

Voer een uitgebreide vergelijking uit van de DNS-instellingen tussen de DEV- en PROD-bronconnectors:

- 1.- Documenteer de DNS-serverconfiguraties in zowel de ontwikkelings- als de productieresourceconnectors.
- 2.- Bepaal of de ontwikkelingsconnector standaard DNS-instellingen of alternatieve DNS-servers gebruikt.
- 3.- Vergelijk de DNS-configuratie van de productieconnector met de installatie van de werkontwikkeling.
- 4.- Let op eventuele verschillen in DNS-resolutiemethoden, time-outs of fallback-configuraties.

Stap 2: Alternatieve DNS-serverconfiguratie testen

Als de productieresourceconnector standaard DNS-instellingen gebruikt en de ontwikkelingsconnector alternatieve DNS-servers gebruikt, of omgekeerd:

- Configureer de connector voor productiebronnen om dezelfde DNS-serverinstellingen te gebruiken als de connector voor werkontwikkeling
- U kunt ook alternatieve DNS-servers opgeven in de configuratie van de productiebronnen
- De verbinding met de privébron testen na elke DNS-configuratiwijziging
- Controleer de verbindingslogboeken op succes bij DNS-oplossing of aanhoudende fouten wanneer u diagnostiek gebruikt, tcpdump naar het IP-adres van de PR-bestemming



Opmerking: beide bronconnectoren kunnen de Fully Qualified Domain Name (FQDN) van de PR oplossen wanneer u de standaard DNS gebruikt die op de RC is geconfigureerd, maar deze komt niet overeen met de interne DNS die is geconfigureerd op de configuratie van de privébron voor de niet-werkende of productie-RC.

Stap 3: DNS-resolutie en -connectiviteit valideren

U moet de Production Resource Connector bijwerken om de interne DNS-servers te gebruiken die overeenkomen met de PR-configuratie om het probleem op te lossen. Klik op de bronconnector-ID en klik op Bewerken om Alternatieve DNS gebruiken te selecteren. U kunt de alternatieve DNS-servers gebruiken om privébronnen op te lossen op basis van de domeininstelling binnen de connectorconfiguratie. Hiermee kunt u het domein en de DNS-server handmatig opgeven om te testen of de connectiviteit verbetert. Na deze wijziging kunt u met succes toegang krijgen tot de privébron of Ubuntu-server.

Na het implementeren van DNS-configuratiwijzigingen:

- 1.- Controleer of de DNS-resolutie correct werkt vanaf de connector voor de productieresource
- 2.- Bevestig dat de privéresource niet langer de standaardblokregel bereikt
- 3.- Test end-to-end connectiviteit via de productieconnector

Oorzaak

De hoofdoorzaak van het probleem had betrekking op DNS-configuratieverschillen tussen de connectors voor ontwikkeling en productiemiddelen. De productieomgeving gebruikte standaard verschillende DNS-servers. Deze fout in de DNS-resolutie zorgt ervoor dat de verbinding terugvalt naar het standaardbeveiligingsbeleid, waardoor het verkeer wordt geblokkeerd door de standaardblokregel in plaats van op de juiste manier via het ZTNA-framework te worden gerouteerd. De Development Resource Connector is geconfigureerd om de interne DNS-servers te gebruiken die overeenkomen met de interne DNS die is geconfigureerd in de configuratie van de privébron.

De Production Resource Connector is echter geconfigureerd om de standaard DNS te gebruiken, die verschilt van de interne DNS-servers die in de PR-configuratie worden genoemd.

De Production Resource Connector is bijgewerkt om de interne DNS-servers te gebruiken om het probleem op te lossen in overeenstemming met de PR-configuratie.

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.