

Behebung von Problemen mit privatem Zugriff mit ZTNA CLAP/BAP über Ressourcenkonnektoren aufgrund eines DNS-Fehlers

Inhalt

[Problem](#)

[Umwelt](#)

[Auflösung](#)

[Schritt 1: Vergleich der DNS-Konfiguration zwischen Umgebungen](#)

[Phase 2: Alternative DNS-Serverkonfiguration testen](#)

[Schritt 3: Validierung der DNS-Auflösung und -Verbindung](#)

[Ursache](#)

[Verwandte Inhalte](#)

- [Problem](#)
 - [Umwelt](#)
 - [Auflösung](#)
 - [Schritt 1: Vergleich der DNS-Konfiguration zwischen Umgebungen](#)
 - [Phase 2: Alternative DNS-Serverkonfiguration testen](#)
 - [Schritt 3: Validierung der DNS-Auflösung und -Verbindung](#)
 - [Ursache](#)
 - [Verwandte Inhalte](#)
-

Problem

Eine private Ressource, die für den Zero Trust Network Access (ZTNA) konfiguriert wurde, funktioniert ordnungsgemäß, wenn in der Entwicklungsumgebung ein Ressourcenkonnektor verwendet wird. Wenn jedoch die Konfiguration der privaten Ressource so geändert wird, dass der Ressourcenkonnektor in der Produktionsumgebung verwendet wird, schlägt der Zugriff auf die private Ressource oder Verbindung mit DNS-bezogenen Fehlern fehl. Die Verbindung trifft auf die Standard-Blockregel und verhindert eine erfolgreiche Validierung des neuen Produktionsressourcenkonnektors, bevor private Produktionsressourcen durch diesen geleitet werden.

Zu den spezifischen Symptomen gehören:

- Für den Produktionsressourcen-Connector aufgezeichnete DNS-Fehlermeldungen
- Verbindungsfehler aufgrund der Standardblockregel im Aktivitätssuchbericht
- Die Funktionalität des Produktionsressourcen-Connectors kann nicht überprüft werden.
- Potenzielle Auswirkungen auf den Zugriff auf private Ressourcen über ZTNA CLAP mithilfe von Resource Connector

Die Netzwerkkonnektivität wurde überprüft, einschließlich der erfolgreichen DNS-Auflösung des privaten Webserver-Hostnamens direkt aus dem Ressourcenkonnektor und der TCP-Verbindung mit Port 8443 auf dem Ubuntu-Server. Alles in Ordnung, aber immer noch erhalten wir DNS-Fehler Warnung in Production Resource Connector WARUM?

Umwelt

- Technologie: Solution Support (SSPT - Vertrag erforderlich)
- Untertechnologie: Sicherer Zugriff ohne Trust (ZTNA, Status, Client-basiert, Registrierung, private Ressource)
- Produktfamilie: Sicherer Zugriff, kein Vertrauen/ZTNA, Ressourcen-Connector
- Private Zielanwendung/Server: Zugriff auf Ubuntu-Server über TCP-Port 8443
- Netzwerkkomponenten: Ressourcenstecker in DEV- und PROD-Umgebungen

Auflösung

Der Ansatz zur Fehlerbehebung konzentriert sich auf Unterschiede bei der DNS-Konfiguration zwischen den Konnektoren für Entwicklungs- und Produktionsressourcen. Beachten Sie, dass der Entwicklungsressourcen-Connector im Arbeitsszenario ausgeführt wird und erfolgreich auf private Ressourcen zugreifen kann.

Der Produktionsressourcen-Connector funktioniert nicht. Der Zugriff auf PR ist nicht möglich, und es wird ein DNS-Fehler in RC > Netzwerkverbindungen > Ressourcenconnector > DNS-Fehler ausgegeben.

Befolgen Sie diese systematischen Schritte, um die DNS-Probleme zu identifizieren und zu beheben.

Schritt 1: Vergleich der DNS-Konfiguration zwischen Umgebungen

Führen Sie einen umfassenden Vergleich der DNS-Einstellungen zwischen dem DEV- und dem PROD-Ressourcenverbinder durch:

- 1.- Dokumentieren der DNS-Serverkonfigurationen in den Konnektoren für Entwicklungs- und Produktionsressourcen
- 2.- Ermitteln Sie, ob der Entwicklungs-Connector Standard-DNS-Einstellungen oder alternative DNS-Server verwendet.
- 3.- Vergleichen Sie die DNS-Konfiguration des Produktions-Connectors mit der funktionierenden Entwicklungskonfiguration.
- 4.- Beachten Sie alle Unterschiede bei DNS-Auflösungsmethoden, Timeouts oder Fallback-Konfigurationen.

Phase 2: Alternative DNS-Serverkonfiguration testen

Wenn der Produktionsressourcen-Connector die DNS-StandardEinstellungen verwendet und der Entwicklungsconnector alternative DNS-Server verwendet oder umgekehrt:

- Konfigurieren Sie den Produktionsressourcen-Connector so, dass er die gleichen DNS-Servereinstellungen wie der funktionierende Entwicklungsconnector verwendet.
- Alternativ können Sie alternative DNS-Server in der Konfiguration des Produktionsressourcen-Connectors angeben.
- Testen der privaten Ressourcenverbindung nach jeder Änderung der DNS-Konfiguration
- Überwachen Sie die Connector-Protokolle auf erfolgreiche DNS-Auflösung oder fortgesetzte Fehler, wenn Sie die Diagnose verwenden, tcpdump zur PR-Ziel-IP



Anmerkung: Beide Ressourcenkonnektoren können den vollqualifizierten Domännennamen (Fully Qualified Domain Name, FQDN) des PR auflösen, wenn Sie den auf dem RC konfigurierten Standard-DNS verwenden, der jedoch nicht mit dem internen DNS übereinstimmt, der auf der privaten Ressourcenkonfiguration für den nicht funktionierenden oder produktiven RC konfiguriert ist.

Schritt 3: Validierung der DNS-Auflösung und -Verbindung

Sie müssen den Production Resource Connector aktualisieren, damit die internen DNS-Server zur Lösung des Problems mit der PR-Konfiguration übereinstimmen. Klicken Sie auf die Ressourcenkonnektor-ID, und klicken Sie auf Bearbeiten, um Alternativer DNS zu verwenden auszuwählen. Sie können den Befehl Alternative DNS-Server verwenden verwenden erkunden, um private Ressourcen basierend auf den Domäneneinstellungen in der Connector-Konfiguration aufzulösen. Dadurch können Sie die Domäne und den DNS-Server manuell angeben, um zu testen, ob sich die Konnektivität verbessert. Nach dieser Änderung können Sie erfolgreich auf die private Ressource oder den Ubuntu-Server zugreifen.

Nach der Implementierung der DNS-Konfigurationsänderungen:

- 1.- Überprüfen der ordnungsgemäßen Funktion der DNS-Auflösung über den Produktionsressourcen-Connector
- 2.- Bestätigen Sie, dass die private Ressource nicht mehr auf die Standard-Blockregel trifft
- 3.- Testen der End-to-End-Konnektivität über den Produktions-Connector

Ursache

Die Ursache des Problems liegt in den Unterschieden zwischen der DNS-Konfiguration der Entwicklungs- und Produktionsressourcenkonnektoren. In der Produktionsumgebung wurden standardmäßig unterschiedliche DNS-Server verwendet. Diese DNS-Auflösung führt dazu, dass die Verbindung auf die Standard-Sicherheitsrichtlinien zurückgreift, was dazu führt, dass der Datenverkehr durch die Standard-Blockregel blockiert wird, anstatt ordnungsgemäß durch das ZTNA-Framework geroutet zu werden. Der Development Resource Connector ist für die Verwendung der internen DNS-Server konfiguriert, die mit dem internen DNS übereinstimmen, der in der privaten Ressourcenkonfiguration konfiguriert wurde.

Der Production Resource Connector ist jedoch für die Verwendung des Standard-DNS konfiguriert, der sich von den in der PR-Konfiguration genannten internen DNS-Servern unterscheidet.

Der Produktionsressourcen-Connector wurde aktualisiert, damit zur Lösung des Problems die internen DNS-Server für die PR-Konfiguration verwendet werden können.

Verwandte Inhalte

- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.