

Risoluzione dei problemi di accesso privato con ZTNA CLAP/BAP tramite i connettori di risorse a causa di un errore DNS

Sommario

[Problema](#)

[Ambiente](#)

[Risoluzione](#)

[Passaggio 1: Confronto della configurazione DNS tra ambienti](#)

[Passaggio 2: Verifica configurazione server DNS alternativo](#)

[Passaggio 3: Convalida risoluzione e connettività DNS](#)

[Causa](#)

[Contenuto correlato](#)

- [Problema](#)
 - [Ambiente](#)
 - [Risoluzione](#)
 - [Passaggio 1: Confronto della configurazione DNS tra ambienti](#)
 - [Passaggio 2: Verifica configurazione server DNS alternativo](#)
 - [Passaggio 3: Convalida risoluzione e connettività DNS](#)
 - [Causa](#)
 - [Contenuto correlato](#)
-

Problema

Una risorsa privata configurata per l'accesso ZTNA (Zero Trust Network Access) funziona correttamente quando si utilizza Connettore risorse nell'ambiente di sviluppo. Tuttavia, quando la configurazione delle risorse private viene modificata per utilizzare il connettore di risorse nell'ambiente di produzione, l'accesso alla risorsa privata o alla connessione non riesce con errori correlati al DNS. La connessione raggiunge la regola di blocco predefinita, impedendo la corretta convalida del nuovo connettore delle risorse di produzione prima di instradare le risorse private di produzione attraverso di esso.

I sintomi specifici includono:

- Errori DNS registrati per il connettore delle risorse di produzione
- Errori di connessione dovuti al superamento della regola di blocco predefinita nel report di ricerca attività
- Impossibile convalidare la funzionalità connettore risorse di produzione
- Potenziale impatto sull'accesso alle risorse private tramite il protocollo CLAP ZTNA tramite il connettore di risorse

È stata verificata la connettività di rete, inclusa la corretta risoluzione DNS del nome host del server Web privato direttamente prodotta dal connettore di risorse e la connettività TCP alla porta 8443 sul server Ubuntu. Tutto bene, ma comunque otteniamo l'avviso di errore DNS nel connettore delle risorse di produzione PERCHÉ?

Ambiente

- Tecnologia: Supporto per la soluzione (SSPT - contratto obbligatorio)
- Sottotecnologia: Accesso sicuro - Accesso con attendibilità totale (ZTNA, postura, basato su client, registrazione, risorsa privata)
- Famiglia di prodotti: Accesso sicuro, Zero Trust/ZTNA, Resource Connector
- Server/applicazione privata di destinazione: Server Ubuntu accessibile sulla porta TCP 8443
- Componenti di rete: Connettori di risorse in ambienti DEV e PROD

Risoluzione

L'approccio per la risoluzione dei problemi è incentrato sulle differenze di configurazione DNS tra i connettori delle risorse di sviluppo e di produzione. Si noti che Connettore risorse di sviluppo sta funzionando in base allo scenario. È possibile accedere correttamente alle risorse private. Il connettore della risorsa di produzione non funziona, la prenotazione permanente non è accessibile e viene generato un errore DNS in RC > Connessioni di rete > Connettore risorse > Errore DNS.

Seguire questi passaggi sistematici per identificare e risolvere i problemi di risoluzione DNS.

Passaggio 1: Confronto della configurazione DNS tra ambienti

Eseguire un confronto completo delle impostazioni DNS tra i connettori delle risorse DEV e PROD:

- 1.- Documentare le configurazioni del server DNS nei connettori delle risorse di sviluppo e di produzione.
- 2.- Identificare se il connettore di sviluppo utilizza le impostazioni DNS predefinite o server DNS alternativi.
- 3.- Confrontare la configurazione DNS del connettore di produzione con l'impostazione di sviluppo funzionante.
- 4.- Annotare eventuali differenze nei metodi di risoluzione DNS, nei timeout o nelle configurazioni di fallback.

Passaggio 2: Verifica configurazione server DNS alternativo

Se il connettore delle risorse di produzione utilizza le impostazioni DNS predefinite e il connettore di sviluppo utilizza server DNS alternativi o viceversa:

- Configurare il connettore delle risorse di produzione in modo che utilizzi le stesse impostazioni del server DNS del connettore di sviluppo funzionante
- In alternativa, specificare server DNS alternativi nella configurazione del connettore delle risorse di produzione
- Verificare la connettività delle risorse private dopo ogni modifica della configurazione DNS
- Monitorare i registri dei connettori per verificare l'esito della risoluzione DNS o gli errori continui quando si utilizza la diagnostica, eseguire il dump tcp nell'indirizzo IP di destinazione PR



Nota: Entrambi i connettori di risorsa possono risolvere il nome di dominio completo (FQDN) della prenotazione permanente quando si utilizza il DNS predefinito configurato nella prenotazione permanente, ma non corrisponde al DNS interno configurato nella

configurazione delle risorse private per la prenotazione permanente non funzionante o di produzione.

Passaggio 3: Convalida risoluzione e connettività DNS

Per risolvere il problema, è necessario aggiornare il connettore delle risorse di produzione in modo da utilizzare i server DNS interni in modo che corrispondano alla configurazione della prenotazione permanente. Fare clic sull'ID del connettore di risorse e fare clic su Modifica per selezionare Usa DNS alternativo. È possibile esplorare la pagina Utilizza server DNS alternativi per risolvere le risorse private in base all'impostazione del dominio nella configurazione del connettore. Ciò consente di specificare manualmente il dominio e il server DNS per verificare se la connettività migliora. Dopo questa modifica, sarà possibile accedere alla risorsa privata o al server Ubuntu.

Dopo l'implementazione delle modifiche alla configurazione DNS:

- 1.- Verificare che la risoluzione DNS funzioni correttamente dal connettore delle risorse di produzione
- 2.- Verificare che la risorsa privata non raggiunga più la regola di blocco predefinita
- 3.- Test della connettività end-to-end attraverso il connettore di produzione

Causa

La causa principale del problema è correlata alle differenze di configurazione DNS tra i connettori delle risorse di sviluppo e di produzione. L'ambiente di produzione utilizza server DNS diversi per impostazione predefinita. Questo errore di risoluzione DNS causa il fallback della connessione ai criteri di sicurezza predefiniti, in quanto il traffico viene bloccato dalla regola di blocco predefinita anziché essere instradato correttamente tramite il framework ZTNA. Il connettore delle risorse di sviluppo è configurato per utilizzare i server DNS interni che corrispondono al DNS interno configurato nella configurazione delle risorse private.

Il connettore delle risorse di produzione, tuttavia, è configurato per utilizzare il DNS predefinito, che differisce dai server DNS interni menzionati nella configurazione PR.

Il connettore delle risorse di produzione è stato aggiornato in modo da utilizzare i server DNS interni per la corrispondenza con la configurazione delle pubbliche relazioni per risolvere il problema.

Contenuto correlato

- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).