

Dépannage d'un problème d'accès privé avec ZTNA CLAP/BAP via des connecteurs de ressources en raison d'une défaillance DNS

Table des matières

[Problème](#)

[Environnement](#)

[Résolution](#)

[Étape 1: Comparer la configuration DNS entre les environnements](#)

[Étape 2: Tester la configuration du serveur DNS secondaire](#)

[Étape 3: Valider la résolution et la connectivité DNS](#)

[Motif](#)

[Autres informations utiles](#)

- [Problème](#)
 - [Environnement](#)
 - [Résolution](#)
 - [Étape 1: Comparer la configuration DNS entre les environnements](#)
 - [Étape 2: Tester la configuration du serveur DNS secondaire](#)
 - [Étape 3: Valider la résolution et la connectivité DNS](#)
 - [Motif](#)
 - [Autres informations utiles](#)
-

Problème

Une ressource privée configurée pour ZTNA (Zero Trust Network Access) fonctionne correctement lors de l'utilisation d'un connecteur de ressource dans l'environnement de développement. Cependant, lorsque la configuration de la ressource privée est modifiée pour utiliser le connecteur de ressource dans l'environnement de production, l'accès à la ressource privée ou à la connexion échoue avec des erreurs liées au DNS. La connexion atteint la règle de blocage par défaut, ce qui empêche la validation du nouveau connecteur de ressources de production avant le routage des ressources privées de production via celui-ci.

Les symptômes spécifiques sont les suivants :

- Erreurs de défaillance DNS enregistrées pour le connecteur de ressources de production
- Échecs de connexion dus à l'application de la règle de blocage par défaut dans le rapport de recherche d'activité
- Impossible de valider la fonctionnalité du connecteur de ressources de production
- Impact potentiel sur l'accès aux ressources privées via ZTNA CLAP à l'aide de Resource Connector

La connectivité réseau a été vérifiée, y compris la résolution DNS réussie du nom d'hôte du serveur Web privé directement la production à partir du connecteur de ressources et la connectivité TCP au port 8443 sur le serveur Ubuntu. Tout va bien, mais nous recevons toujours une alerte d'échec DNS dans le connecteur de ressources de production POURQUOI ?

Environnement

- Technologie : Assistance pour les solutions (SSPT - contrat requis)
- Sous-technologie : Accès sécurisé - Accès sans confiance (ZTNA, posture, basé sur le client, inscription, ressource privée)
- Gamme de produits : Accès sécurisé, ZTNA/Zero Trust, connecteur de ressources
- Serveur/application privée cible : Serveur Ubuntu accessible sur le port TCP 8443
- Composants réseau : Connecteurs de ressources dans les environnements DEV et PROD

Résolution

L'approche de dépannage se concentre sur les différences de configuration DNS entre les connecteurs de ressources de développement et de production. Notez que le connecteur de ressources de développement fonctionne : accès à la ressource privée réussi.

Le connecteur de ressources de production ne fonctionne pas, le RP n'est pas accessible et une erreur de défaillance DNS est générée dans RC > Connexions réseau > Connecteur de ressources > Défaillance DNS.

Suivez ces étapes systématiques pour identifier et résoudre les problèmes de résolution DNS.

Étape 1: Comparer la configuration DNS entre les environnements

Effectuez une comparaison complète des paramètres DNS entre les connecteurs de ressources DEV et PROD :

- 1.- Documentez les configurations du serveur DNS dans les connecteurs de ressources de développement et de production.
- 2.- Indiquez si le connecteur de développement utilise les paramètres DNS par défaut ou d'autres serveurs DNS.
- 3.- Comparez la configuration DNS du connecteur de production à la configuration de développement en cours.
- 4.- Notez toute différence dans les méthodes de résolution DNS, les délais d'attente ou les configurations de secours.

Étape 2: Tester la configuration du serveur DNS secondaire

Si le connecteur de ressources de production utilise les paramètres DNS par défaut et que le connecteur de développement utilise d'autres serveurs DNS, ou vice versa :

- Configurez le connecteur de ressources de production pour utiliser les mêmes paramètres de serveur DNS que le connecteur de développement en cours
- Vous pouvez également spécifier d'autres serveurs DNS dans la configuration du connecteur de ressources de production
- Tester la connectivité des ressources privées après chaque modification de la configuration DNS
- Surveillez les journaux du connecteur pour la résolution DNS réussie ou les erreurs continues lorsque vous utilisez des diagnostics, tcpdump vers l'IP de destination PR



Remarque : Les deux connecteurs de ressources peuvent résoudre le nom de domaine complet (FQDN) du RP lorsque vous utilisez le DNS par défaut configuré sur le RC, mais il ne correspond pas au DNS interne configuré sur la configuration de ressource privée pour

le RC non fonctionnel ou de production.

Étape 3: Valider la résolution et la connectivité DNS

Vous devez mettre à jour le connecteur de ressources de production afin d'utiliser les serveurs DNS internes pour correspondre à la configuration PR afin de résoudre le problème. Cliquez sur l'ID du connecteur de ressource et cliquez sur Edit afin de sélectionner Use Alternate DNS. Vous pouvez explorer la section Utiliser d'autres serveurs DNS pour résoudre les ressources privées en fonction des paramètres de domaine dans la configuration du connecteur. Cela vous permet de spécifier manuellement le domaine et le serveur DNS afin de tester si la connectivité s'améliore. Après cette modification, vous pouvez accéder à la ressource privée ou au serveur Ubuntu.

Après avoir implémenté les modifications de configuration DNS :

- 1.- Vérifiez que la résolution DNS fonctionne correctement à partir du connecteur de ressources de production
- 2.- Confirmez que la ressource privée n'atteint plus la règle de blocage par défaut
- 3.- Tester la connectivité de bout en bout via le connecteur de production

Motif

La cause première du problème est liée aux différences de configuration DNS entre les connecteurs de ressources de développement et de production. Par défaut, l'environnement de production utilisait différents serveurs DNS. Cet échec de résolution DNS entraîne le retour de la connexion aux stratégies de sécurité par défaut, ce qui entraîne le blocage du trafic par la règle de blocage par défaut plutôt que son routage correct via l'infrastructure ZTNA. Le connecteur de ressources de développement est configuré pour utiliser les serveurs DNS internes qui correspondent au DNS interne configuré dans la configuration de ressources privées.

Cependant, le connecteur de ressources de production est configuré pour utiliser le DNS par défaut, qui diffère des serveurs DNS internes mentionnés dans la configuration PR.

Le connecteur de ressources de production a été mis à jour pour utiliser les serveurs DNS internes pour correspondre à la configuration PR afin de résoudre le problème.

Autres informations utiles

- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.