

Dépannage des échecs APP_UNREACHABLE pour les applications privées dans l'accès sécurisé

Table des matières

Problème

Lors d'une tentative d'accès aux applications ZTNA (Zero Trust Network Access) via Cisco Secure Access, les utilisateurs rencontrent un message d'erreur « Application Unreachable » (Application inaccessible).

- Le connecteur affiche sain/actif dans le tableau de bord et l'exécution de l'application est confirmée par son propriétaire.
- La panne peut affecter tous les utilisateurs d'une application alors que les autres applications desservies par le même connecteur fonctionnent normalement.
- Dans les déploiements de pools de connecteurs, les échecs peuvent apparaître intermittents : les sessions réussissent ou échouent selon le connecteur sélectionné dans le pool.

Environnement

- Déploiement de Cisco Secure Private Access avec ZTNA
- Ressources privées configurées pour l'accès ZTNA
- Déploiement du connecteur de ressources pour l'accès aux ressources privées

Résolution

Étape 1. Test de l'accessibilité directe à partir du segment de réseau Connecteurs

- Le connecteur de ressource est un appareil verrouillé et ne fournit pas d'accès shell pour exécuter des commandes telles que curl ou nc directement. Au lieu de cela, effectuez le test d'accessibilité à partir d'un hôte de test (ou d'une machine virtuelle temporaire) placé dans le même sous-réseau/VLAN que le connecteur, afin qu'il obéisse aux mêmes règles de chemin réseau, de routage et de pare-feu que l'application :

```
curl -v http://APP_IP:PORT/health  
nc -zv APP_IP PORT
```

- En cas d'échec, le problème est confirmé dans le chemin réseau ou sur le serveur d'applications. Corrigez d'abord ce problème avant d'examiner toute configuration d'accès sécurisé.



Remarque : Un test à partir d'un sous-réseau différent n'est pas concluant : les règles de pare-feu et le routage sont évalués par source, car la source de test doit refléter le plus fidèlement possible l'emplacement IP du connecteur.

Étape 2 : vérification de la configuration des ressources privées

- Dans le tableau de bord d'accès sécurisé, accédez à Ressources > Ressources privées, ouvrez la ressource privée affectée et comparez l'adresse IP configurée, le nom de domaine complet et le port caractère pour caractère à l'adresse de liaison et au port réels de l'application en cours d'exécution.
- Toute incohérence (IP obsolète après une migration de serveur, port incorrect, HTTP ou HTTPS) produit APP_UNREACHABLE même avec un chemin réseau parfaitement sain.

Étape 3. Validation de la résolution DNS pour le connecteur

- Si la ressource privée est définie par le nom de domaine complet, vérifiez que les serveurs DNS affectés au connecteur peuvent la résoudre. À partir de l'interface de ligne de commande du connecteur de ressources (les déploiements de VM fournissent une interface

de ligne de commande de diagnostic avec des commandes de dépannage Linux standard prises en charge), exécutez :

```
nslookup app.internal.company.com <internal_DNS_server_IP>
```

- Vérifiez que l'adresse IP privée correcte est renvoyée. Assurez-vous que les points de configuration réseau du connecteur sur les serveurs DNS internes peuvent résoudre les noms de domaine complets des applications privées ; un connecteur configuré avec des résolveurs publics ne peut pas résoudre les zones internes.

Étape 4. Vérification du chemin du pare-feu

- Vérifiez que les règles de pare-feu (pare-feu réseau et pare-feu hôte sur le serveur d'applications) autorisent le trafic de l'adresse IP du connecteur vers l'adresse IP du serveur d'applications sur le port requis.

Étape 5. Capture du trafic avec tcpdump sur le connecteur de ressources

- Exécutez une capture de paquets sur le connecteur de ressources pour observer les tentatives de connexion du dernier kilomètre vers l'application. L'utilitaire tcpdump est disponible sur le connecteur de ressources. Reportez-vous au guide [Exécuter tcpdump sur les connecteurs de ressources](#).



Conseil : Pour rendre la capture déterministe dans un déploiement de groupe de connecteurs, ne laissez temporairement qu'un seul connecteur de ressource activé dans le groupe afin que toutes les sessions de la ressource la traversent, puis exécutez la capture filtrée sur le serveur d'applications et le port.

-
- Exemple :

```
tcpdump 'host x.x.x.x and tcp port 443'
```

(où x.x.x.x est l'adresse IP du serveur d'applications et 443 est le port de l'application)

- Interpréter les résultats : les SYN sortants sans SYN-ACK indiquent une perte de pare-feu ou une absence d'écoute de l'application ; un RST immédiat indique que l'hôte est accessible mais que rien n'est lié au port ; aucun paquet vers l'application n'indique que la session n'atteint pas ce connecteur ou que le DNS est résolu en une adresse inattendue.
- Réactivez les connecteurs restants dans le groupe une fois la capture terminée.

Motif

- Pare-feu bloquant le trafic du connecteur à l'application : Un pare-feu réseau ou basé sur hôte bloque le port requis entre l'adresse IP hôte du connecteur et l'adresse IP du serveur d'applications.
- Non-concordance de la configuration des ressources privées dans Secure Access : L'adresse IP, le nom de domaine complet ou le port configuré dans la définition de ressource privée (Ressources > Ressources privées) ne correspond pas à ce que l'application écoute réellement (par exemple, l'application a été déplacée vers une nouvelle adresse IP ou écoute le 8443 alors que le 443 est configuré).
- Échec de la résolution DNS pour le connecteur : La ressource privée est définie par le nom de domaine complet, mais les serveurs DNS du connecteur ne résolvent pas les noms de domaine complets des applications privées.
- Serveur d'applications arrêté ou non à l'écoute : Le serveur semble sain par d'autres mesures, mais n'est pas lié au port attendu, ou le service a planté pendant que l'hôte est resté actif.
- Accessibilité partielle dans un pool de connecteurs : Un ou plusieurs connecteurs du pool se trouvent dans un segment de réseau qui ne peut pas atteindre l'application. Par conséquent, seules les sessions attribuées à ces connecteurs échouent.

Autres informations utiles

- [Dépannage et collecte des informations de base pour Cisco Secure Access](#)
- [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.