

Ressources de liaison privée inaccessibles via l'appliance virtuelle d'accès sécurisé dans Azure en raison de la configuration DNS interne

Table des matières

Problème

Les ressources de liaison privée Azure ne sont pas accessibles à partir des espaces de travail et des charges de travail Azure lorsque le trafic est acheminé via une appliance virtuelle d'accès sécurisé Cisco (VA) déployée dans Azure. Ce problème persiste malgré la configuration d'exceptions de pilotage du trafic pour contourner l'accès sécurisé pour les domaines privés Azure, l'activation de la désactivation DNS et la configuration du DNS privé sur la VA.

Les tentatives d'accès aux points de terminaison de liaison privée Azure à partir des charges de travail Azure derrière la VA d'accès sécurisé entraînent une résolution et une connectivité défaillantes.

Environnement

- Appliance virtuelle d'accès sécurisé Cisco (VA) déployée dans Azure
- Espaces de travail Azure et charges de travail hébergées Azure
- Lien privé Azure activé pour la connectivité de ressources Azure privées
- Exceptions de pilotage du trafic configurées pour contourner l'accès sécurisé pour les domaines privés Azure
- Désactivation DNS activée dans Secure Access VA
- Zones DNS privées configurées dans Secure Access VA
- Version du logiciel: ALL (le problème est indépendant de la version)

Résolution

La résolution impliquait la mise à jour de la configuration DNS au sein de l'appliance virtuelle d'accès sécurisé Cisco afin d'inclure des entrées de serveur DNS interne qui sont capables de résoudre les domaines de liaison privée Azure. Ces étapes détaillent les actions de dépannage et les mesures correctives prises :

Diagnostiquer la configuration DNS locale sur l'appliance virtuelle d'accès sécurisé

1. Pour examiner la configuration DNS existante et vérifier si les serveurs DNS internes sont définis, utilisez cette commande sur l'appliance virtuelle d'accès sécurisé :

```
config localdns show
```

1. Exemple de résultat (avec le nom du périphérique remplacé) :

```
device# config localdns show
No internal DNS servers configured.
Conditional forwarders present for Azure private domains.
```

Ajout d'entrées de serveur DNS interne à Secure Access VA

1. Pour activer la résolution appropriée des domaines de liaison privée Azure, ajoutez les adresses IP de serveur DNS interne appropriées à l'aide de cette commande :

```
config localdns add <internal-DNS-server-IP>
```

1. Remplacez <internal-DNS-server-IP> par l'adresse IP réelle de votre serveur DNS interne qui peut résoudre les domaines de liaison privée Azure.

Vérifier la résolution DNS pour les domaines de liaison privée Azure

1. Après la mise à jour de la configuration DNS, vérifiez que les domaines de liaison privée Azure peuvent être résolus via l'appliance virtuelle d'accès sécurisé. Utilisez cette commande pour confirmer la configuration du serveur DNS :

```
config localdns show
```

1. Exemple de résultat (nom du périphérique remplacé) :

```
device# config localdns show
Internal DNS servers configured:
- x.x.x.x
Conditional forwarders present for Azure private domains.
```

1. Aucune commande CLI trouvée qui montre le changement de `config localdns show` sans serveurs DNS à un état de fonctionnement avec la résolution confirmée.

Valider la connectivité aux ressources de liaison privée Azure

Une fois la résolution DNS correcte, testez la connectivité des charges de travail Azure derrière l'appliance virtuelle d'accès sécurisé vers les points de terminaison de liaison privée Azure prévus pour garantir un accès approprié.

Motif

La cause principale du problème était l'absence de configurations de serveur DNS interne dans l'appliance virtuelle d'accès sécurisé Cisco. L'appliance virtuelle a été configurée avec des redirections conditionnels pour les domaines privés Azure, mais il manquait des serveurs DNS internes nécessaires à la résolution DNS appropriée des domaines de liaison privée Azure. L'ajout des entrées du serveur DNS interne a résolu 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.