

Risorse di collegamento privato inaccessibili tramite l'appliance virtuale di accesso sicuro in Azure a causa della configurazione DNS interna

Sommario

Problema

Le risorse di collegamento privato di Azure non sono accessibili dalle aree di lavoro e dai carichi di lavoro di Azure quando il traffico viene instradato tramite un'appliance virtuale Cisco Secure Access (VA) distribuita in Azure. Questo problema persiste nonostante la configurazione delle eccezioni di indirizzamento del traffico per ignorare l'accesso sicuro per i domini privati di Azure, l'abilitazione del backoff DNS e la configurazione del DNS privato nell'appliance VA.

I tentativi di accedere agli endpoint di collegamento privato di Azure dai carichi di lavoro di Azure dietro l'accesso sicuro VA hanno causato errori di risoluzione e connettività.

Ambiente

- Appliance virtuale Cisco Secure Access (VA) distribuita in Azure
- Aree di lavoro di Azure e carichi di lavoro ospitati da Azure
- Azure Private Link abilitato per la connettività delle risorse di Azure private
- Eccezioni di gestione del traffico configurate per ignorare l'accesso sicuro per i domini privati di Azure
- Backoff DNS abilitato in Secure Access VA
- Zone DNS private configurate in Secure Access VA
- Versione del software: ALL (problema indipendente dalla versione)

Risoluzione

La risoluzione ha comportato l'aggiornamento della configurazione DNS in Cisco Secure Access VA per includere le voci del server DNS interno in grado di risolvere i domini di Azure Private Link. Nei passaggi seguenti vengono descritte in dettaglio le azioni di risoluzione dei problemi e di correzione intraprese:

Esegui diagnosi della configurazione DNS locale su Secure Access VA

1. Per esaminare la configurazione DNS esistente e verificare se i server DNS interni sono impostati, utilizzare questo comando sulla scheda Secure Access VA:

```
config localdns show
```

1. Output di esempio (con nome dispositivo sostituito):

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

Aggiungi voci interne del server DNS a Secure Access VA

1. Per consentire la corretta risoluzione dei domini di collegamento privato di Azure, aggiungere gli indirizzi IP interni appropriati del server DNS utilizzando questo comando:

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

1. Sostituire <internal-DNS-server-IP> con l'indirizzo IP effettivo del server DNS interno in grado di risolvere i domini di collegamento privato di Azure.

Verifica risoluzione DNS per i domini di collegamento privato di Azure

1. Dopo aver aggiornato la configurazione DNS, verificare che i domini di collegamento privato di Azure possano essere risolti tramite l'accesso sicuro VA. Usare questo comando per confermare la configurazione del server DNS:

```
config localdns show
```

1. Output di esempio (nome dispositivo sostituito):

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

1. Non è stato trovato alcun comando CLI che indica la modifica da `config localdns show` senza server DNS a uno stato funzionante con risoluzione confermata.

Convalida connettività alle risorse di collegamento privato di Azure

Una volta risolta correttamente la risoluzione DNS, verificare la connettività dagli endpoint di Azure Private Link dietro l'VA di accesso sicuro agli endpoint di Azure Private Link desiderati per garantire un accesso corretto.

Causa

La causa principale del problema è stata l'assenza di configurazioni di server DNS interni all'interno di Cisco Secure Access VA. L'istanza di Azure è stata configurata con i server d'inoltro condizionali per i domini privati di Azure, ma non disponeva dei server DNS interni necessari per la risoluzione DNS corretta dei domini di collegamento privato di Azure. L'aggiunta delle voci del server DNS interno ha risolto 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).