

Risolvere i problemi relativi agli errori APP_UNREACHABLE per le applicazioni private in Accesso sicuro

Sommario

Problema

Quando si cerca di accedere ad applicazioni ZTNA (Zero Trust Network Access) tramite Cisco Secure Access, gli utenti ricevono un messaggio di errore "Application Unreachable" (Applicazione non raggiungibile).

- Il Connettore viene visualizzato integro/attivo nel dashboard e l'esecuzione dell'applicazione viene confermata dal relativo proprietario.
- L'errore può interessare tutti gli utenti di un'applicazione, mentre le altre applicazioni servite dallo stesso connettore funzionano normalmente.
- Nelle distribuzioni pool di connettori, gli errori possono apparire intermittenti, ovvero le sessioni hanno esito positivo o negativo a seconda del connettore selezionato nel pool.

Ambiente

- Implementazione di Cisco Secure Private Access con ZTNA
- Risorse private configurate per l'accesso ZTNA
- Distribuzione del connettore di risorse per l'accesso alle risorse private

Risoluzione

Passaggio 1. Verifica della raggiungibilità diretta dal segmento di rete dei connettori

- Il Connettore di risorse è un accessorio bloccato e non consente l'accesso alla shell per l'esecuzione diretta di comandi quali curl o nc. Eseguire invece il test di raggiungibilità da un host di test (o da una VM temporanea) situato nella stessa subnet/VLAN del connettore, in modo che rispetti le stesse regole di percorso di rete, routing e firewall per l'applicazione:

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

- Se l'operazione non riesce, il problema viene confermato nel percorso di rete o nel server applicazioni. Risolvere il problema prima di esaminare qualsiasi configurazione di Accesso sicuro.



Nota: Un test da una subnet diversa non è conclusivo: le regole del firewall e il routing vengono valutati per origine, in quanto l'origine del test deve rispecchiare il posizionamento IP del connettore il più possibile.

Passaggio 2. Verificare la configurazione della risorsa privata

- Nel dashboard Accesso sicuro passare a Risorse > Risorse private, aprire la risorsa privata interessata e confrontare l'IP, il nome di dominio completo (FQDN) e la porta configurati carattere per carattere con l'indirizzo di binding e la porta effettivi dell'applicazione in esecuzione.
- Qualsiasi mancata corrispondenza (IP non aggiornato dopo una migrazione del server, porta errata, HTTP vs HTTPS) genera APP_UNREACHABLE anche con un percorso di rete perfettamente integro.

Passaggio 3. Convalida della risoluzione DNS per il connettore

- Se la risorsa privata è definita da FQDN, verificare che i server DNS assegnati al connettore siano in grado di risolverla. Dalla CLI di Resource Connector (le implementazioni di VM forniscono una CLI di diagnostica con comandi di risoluzione dei problemi Linux standard

supportati), eseguire:

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

- Verificare che venga restituito l'indirizzo IP privato corretto. Verificare i punti di configurazione della rete del connettore nei server DNS interni in grado di risolvere i nomi FQDN delle applicazioni private. Un connettore configurato con resolver pubblici non è in grado di risolvere le zone interne.

Passaggio 4. Esaminare il percorso del firewall

- Confermare le regole del firewall (firewall di rete e firewall host sul server applicazioni) per consentire il traffico dall'indirizzo IP del connettore all'IP del server applicazioni sulla porta richiesta.

Passaggio 5. Acquisire il traffico con tcpdump sul connettore risorse

- Eseguire un'acquisizione di pacchetti sul connettore di risorse per osservare i tentativi di connessione dell'ultimo miglio verso l'applicazione. L'utilità tcpdump è disponibile in Resource Connector. Fare riferimento alla guida [Run tcpdump on Resource Connectors](#).



Suggerimento: Per rendere l'acquisizione deterministica in una distribuzione di un gruppo di connettori, mantenere temporaneamente abilitato un solo connettore di risorse nel gruppo in modo che tutte le sessioni per la risorsa lo attraversino, quindi eseguire l'acquisizione filtrata sul server applicazioni e sulla porta.

-
- Ad esempio:

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

(dove x.x.x.x è l'indirizzo IP del server applicazioni e 443 è la porta dell'applicazione)

- Interpretare i risultati: i SYN in uscita senza SYN-ACK indicano una caduta del firewall o l'app non è in ascolto; un RST immediato indichi che l'host è raggiungibile ma che non vi è alcun collegamento al porto; nessun pacchetto verso l'app indica che la sessione non sta raggiungendo questo connettore o che il DNS è stato risolto in un indirizzo imprevisto.
- Riattivate i connettori rimanenti nel gruppo al termine dell'acquisizione.

Causa

- Blocco del firewall sul traffico da connettore ad app: Un firewall di rete o basato su host blocca la porta richiesta tra l'indirizzo IP dell'host del connettore e l'indirizzo IP del server applicazioni.
- Configurazione della risorsa privata non corrispondente in Secure Access: L'indirizzo IP, il nome FQDN o la porta configurata nella definizione della risorsa privata (Risorse > Risorse private) non corrisponde a ciò su cui l'applicazione è effettivamente in ascolto (ad esempio, l'applicazione è stata spostata in un nuovo indirizzo IP o è in ascolto su 8443 mentre è configurato 443).
- Errore di risoluzione DNS per il connettore: La risorsa privata è definita dal nome di dominio completo, ma i server DNS del connettore non risolvono i nomi di dominio completi delle applicazioni private.
- Server applicazioni inattivo o non in ascolto: Il server risulta integro da altre misure ma non è associato alla porta prevista oppure il servizio si è arrestato in modo anomalo mentre l'host era in stato attivo.
- Raggiungibilità parziale in un pool di connettori: Uno o più connettori del pool si trovano in un segmento di rete che non può raggiungere l'applicazione, pertanto solo le sessioni assegnate a tali connettori avranno esito negativo.

Contenuto correlato

- [Risoluzione dei problemi e raccolta di informazioni di base per Cisco Secure Access](#)
- [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).