

Risoluzione DNS Secure Client ZTNA e perdita di connettività dopo la sospensione di macOS

Sommario

Problema

La ZTNA di Cisco SecureClient sugli endpoint macOS genera un errore di risoluzione DNS e una perdita di connettività ZTA dopo la ripresa del sistema dalla modalità di sospensione o ibernazione. Questo problema riguarda sia la funzionalità ZTNA IA (Identity Access) che ZTNA PA (Private Access). Mentre la connettività IP di base rimane funzionale (il ping ICMP su indirizzi IP esterni come 8.8.8.8 e 208.67.222.22 funziona correttamente), la risoluzione dei nomi DNS ha esito completamente negativo, impedendo l'accesso sia alle risorse Internet che alle risorse private configurate tramite ZTNA.

I sintomi specifici osservati includono:

- Le ricerche DNS hanno esito negativo utilizzando i comandi nslookup (ad esempio, nslookup di www.cisco.com tramite 8.8.8.8 e 208.67.222.22 non funziona).
- Le connessioni ZTNA IA e ZTNA PA non sono disponibili.
- Il problema si verifica in modo coerente dopo la sospensione dell'endpoint e i cicli di riattivazione.
- Il problema può inoltre verificarsi in modo casuale quando il dispositivo è in uso.
- L'interruzione del processo ZTNA determina il riavvio immediato, ma il problema di connettività in genere persiste.
- Solo un riavvio completo del sistema ripristina la risoluzione DNS completa e la connettività ZTNA.

Ambiente

- Sistema operativo: macOS (versione 26.3 documentata nel caso)

- Cisco SecureClient: Versione 5.1.14.x (versioni interessate precedenti alla 5.1.16)
- Modulo ZTNA: Attiva con entrambe le configurazioni di Identity Access (IA) e Private Access (PA)
- Monitoraggio della rete: Può includere soluzioni di sicurezza di terze parti come Sentinel One
- Software di sicurezza aggiuntivo: Può includere Cisco Secure Endpoint
- Server DNS: Server DNS esterni (8.8.8.8, 208.67.222.222) accessibili tramite ICMP ma la risoluzione DNS non riesce
- Modulo UMB: Non in uso

Risoluzione

Il problema è stato risolto tramite una correzione software fornita da Cisco Engineering. Il processo di risoluzione ha comportato i passi descritti nelle sezioni seguenti.

Passaggio 1: Identificazione dei problemi e tracciabilità dei bug

Cisco Engineering ha identificato questo problema come noto e lo ha registrato con l'ID bug Cisco CSCwt24392 con la descrizione "macOS: Il DNS smette di funzionare con ZTA SIA-all e NVM attivi".

Passaggio 2: Raccolta dati di diagnostica

Queste informazioni di diagnostica sono state raccolte per supportare l'analisi tecnica:

- Pacchetti DART (Diagnostic and Reporting Tool) dagli endpoint interessati.
- File di acquisizione pacchetti (ZTNA Issue1.pcapng).
- Schermate che mostrano l'errore di connettività.
- Registrazioni su schermo che mostrano la riproduzione del problema.

- Elabora i log di interazione che mostrano il comportamento del processo `com.cisco.secureclient.zta.app.service` e dell'estensione di sistema.

Passaggio 3: Sviluppo Correzioni Tecniche

Cisco Engineering ha sviluppato una correzione mirata per CSCwt24392 e l'ha inclusa nella versione 5.1.16 di SecureClient. La correzione affronta in modo specifico l'errore di risoluzione DNS che si verifica quando ZTA SIA-all e NVM sono attivi sui sistemi macOS dopo i cicli di sospensione/ibernazione.

Passaggio 4: Installazione aggiornamenti software

Installare Cisco SecureClient versione 5.1.16 o successiva sugli endpoint macOS interessati. Questa versione contiene la correzione per i problemi di risoluzione DNS e connettività ZTA.

Passaggio 5: Test di convalida

Dopo aver installato SecureClient 5.1.16, eseguire i seguenti passaggi di convalida:

- 1.- Consentire all'endpoint macOS di entrare in modalità di sospensione o ibernazione.
- 2.- Riattivare il sistema dalla modalità di sospensione o ibernazione.
- 3.- Testare la risoluzione DNS utilizzando i comandi `nslookup`.
- 4.- Verificare la connettività IA e PA ZTNA per le risorse configurate.
- 5.- Verificare che l'accesso a Internet e l'accesso alle risorse private funzionino correttamente senza che sia necessario riavviare il sistema.

Soluzione per le versioni precedenti

Per gli ambienti in cui non è possibile eseguire l'aggiornamento immediato a SecureClient 5.1.16, è possibile utilizzare questa soluzione temporanea:

- Eseguire un riavvio completo del sistema dopo ogni ciclo di sospensione/ibernazione per ripristinare la risoluzione DNS e la connettività ZTNA.
- Prendere in considerazione l'eventualità di annullare temporaneamente la registrazione a ZTNA se il problema di sospensione/ibernazione influisce in modo significativo sulla produttività (notare che questo rimuove la protezione ZTNA).

Causa

La causa principale di questo problema è un problema software nelle versioni di Cisco SecureClient precedenti alla 5.1.16, identificato specificamente come Cisco bug ID CSCwt24392. Il problema si verifica quando i componenti ZTA (Zero Trust Access) SIA-all (Secure Internet Access) e NVM (Network Visibility Module) sono attivi sui sistemi macOS. Durante la sospensione o l'ibernazione e il ciclo di riattivazione, questi componenti non ripristinano correttamente la funzionalità di risoluzione DNS, mantenendo la connettività IP di base. Questo crea uno stato in cui il traffico ICMP (ping) funziona normalmente, ma le query DNS hanno esito negativo, bloccando di fatto l'accesso alle risorse Internet e alle risorse private protette da ZTNA. Il problema riguarda l'interazione non corretta tra il processo `com.cisco.secureclient.zta.app.service` e il processo di estensione del sistema durante le transizioni dello stato del sistema.

Contenuto correlato

- Cisco ID bug CSCwt24392 - macOS: Il DNS smette di funzionare con ZTA SIA-all e NVM attivi
- [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).