

Risoluzione di ID di dispositivo ZTNA duplicati in distribuzioni ad accesso sicuro mediante immagini d'oro SysPrep

Sommario

Problema

Più computer fisici Windows distribuiti da un'immagine d'oro SysPrep generano ID di dispositivo ZTNA identici, in particolare lo stesso `ztnaDeviceId` su più endpoint. Questa duplicazione causa diversi problemi critici:

- Ripetuta ri-registrazione di dispositivi con lo stesso ID dispositivo ZTNA
- La chiave pubblica viene sovrascritta durante ogni processo di nuova registrazione
- Errori di verifica della postura in tutti i computer ad eccezione del dispositivo registrato più di recente
- Errori di accesso tramite accesso sicuro per gli endpoint interessati

Il comportamento osservato si verifica quando più computer della flotta condividono lo stesso ID dispositivo ZTNA, causando la sovrascrittura della chiave pubblica del computer precedente da parte di ogni registrazione. Tutti i computer, ad eccezione dell'ultimo da registrare, non sono in grado di inviare i controlli di postura, determinando il rifiuto dell'accesso attraverso l'infrastruttura Secure Access.

Sono state identificate più coppie di nome host e ID utente collegate allo stesso ID di dispositivo ZTNA, a dimostrazione dell'ambito del problema di duplicazione nell'intera distribuzione.

Ambiente

- Cisco Secure Access (implementazione ZTNA)

- Macchine fisiche Windows (non macchine virtuali)
- Metodologia di distribuzione dell'immagine finale SysPrep
- Strumenti di Windows ADK (Assessment and Deployment Kit) per la distribuzione di immagini
- Formato file ESD (Electronic Software Delivery) per l'acquisizione delle immagini
- Processo di protezione avanzata del sistema operativo standardizzato, inclusa l'installazione obbligatoria del software
- Configurazione dell'account guest e dell'amministratore locale standard

Risoluzione

Il processo di risoluzione ha richiesto un'analisi completa dei registri e l'identificazione della root cause attraverso un'analisi dettagliata.

Identificazione e risoluzione della root cause

L'indagine ha rivelato che il processo SysPrep non stava generando correttamente identificatori di dispositivo univoci durante la distribuzione dell'immagine dorata.

L'analisi ha riguardato:

Esame delle chiavi del Registro di sistema di Windows, in particolare:

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion`

Raccolta di informazioni sugli ID di sicurezza (SID) degli utenti mediante:

`whoami /user`

La risoluzione ha richiesto la modifica del processo SysPrep per garantire che gli identificatori

specifici del dispositivo vengano rigenerati correttamente durante la distribuzione, impedendo la duplicazione degli ID dei dispositivi ZTNA su più computer fisici.

- Il rinnovo dell'UDID eseguendo il comando `dartcli.exe -nu` modifica il valore di Nounce nel percorso del Registro di sistema
"HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Cisco\Cisco Secure Client\DeviceDetails".
- L'eliminazione del file JSON da `C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments` e il riavvio del servizio ZTA annullano la registrazione dell'utente. È necessario registrare manualmente l'utente. In questo modo viene generato un nuovo file JSON senza alcun altro impatto.
- Il rinnovo dell'UDID su tutti gli endpoint non deve avere alcun impatto finché il valore non viene verificato/valutato su alcun server.

1. Avviare il prompt dei comandi come amministratore e passare alla directory
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\DART".

2. Eseguire `dartcli.exe -u` per verificare il valore dell'UDID corrente.

3. Eseguire il comando `dartcli.exe -nu`. Questo comando rinnova l'UDID.

4. Verificare il nuovo valore ripetendo il comando al passaggio 2.

5. Eliminare il file JSON dalla directory `C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments`

6. Riavviare i servizi VPN e ZTA. A questo punto ZTA deve essere in stato di non registrazione.

7. Consentire all'utente di registrare manualmente la ZTA

9. Verificare il valore del nuovo `ztnaDeviceId` nel file JSON.

Monitoraggio e convalida

Dopo aver implementato le misure correttive per garantire la generazione univoca dell'ID del dispositivo ZTNA:

- Monitoraggio del processo di iscrizione su più computer
- È stato verificato che ogni computer ha generato ID di dispositivo ZTNA univoci
- Confermata la funzionalità di controllo della postura su tutti i dispositivi registrati
- La chiave pubblica non viene più sovrascritta durante la registrazione

Causa

La causa principale è stata identificata come processo di distribuzione dell'immagine finale SysPrep che non genera correttamente identificatori di dispositivo univoci per la registrazione ZTNA. Quando più computer fisici Windows vengono distribuiti dalla stessa immagine d'oro SysPrep, alcuni identificatori specifici del dispositivo utilizzati per generare l'ID del dispositivo ZTNA rimangono identici in tutti i computer distribuiti.

Il processo SysPrep, sebbene efficace per la standardizzazione della configurazione del sistema operativo e dell'installazione del software, non è stato configurato in modo da rigenerare gli identificatori specifici utilizzati da Cisco Secure Client per creare ID univoci per i dispositivi ZTNA. Di conseguenza, tutti i computer distribuiti dalla stessa immagine finale ereditano parametri di identificazione dei dispositivi ZTNA identici, causando conflitti di registrazione e errori di autenticazione nell'infrastruttura Secure Access.

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).