

Dupliceer ZTNA-apparaat-ID's in implementaties met beveiligde toegang oplossen met behulp van SysPrep Golden Images

Inhoud

uitgifte

Meerdere Windows-fysieke machines die worden geïmplementeerd vanuit een gouden SysPrep-image genereren identieke ZTNA-apparaat-ID's, met name dezelfde ztnaDeviceId op meerdere eindpunten. Deze duplicatie veroorzaakt verschillende kritieke problemen:

- Herhaalde herinschrijving van apparaten met dezelfde ZTNA-apparaat-ID
- Overschrijvingen van openbare sleutels tijdens elk herinschrijvingsproces
- Uitval van de houdingscontrole op alle machines, behalve het meest recent ingeschreven apparaat
- Toegang tot storingen via Secure Access voor getroffen eindpunten

Het waargenomen gedrag treedt op wanneer meerdere machines in de vloot dezelfde ZTNA-apparaat-ID delen, waardoor elke inschrijving de openbare sleutel van de vorige machine overschrijft. Alle machines, behalve de laatste die zich inschrijft, kunnen geen houdingscontroles verzenden, wat resulteert in toegangsweigering via de Secure Access-infrastructuur.

Meerdere hostnaam- en gebruikersnamen werden geïdentificeerd als gekoppeld aan dezelfde ZTNA-apparaat-ID, wat de reikwijdte van het duplicatieprobleem tijdens de implementatie aantoont.

milieu

- Cisco Secure Access (ZTNA-implementatie)

- Windows-fysieke machines (geen virtuele machines)
- Sysprep golden image-implementatiemethode
- Windows ADK (Assessment and Deployment Kit)-tools voor de implementatie van images
- ESD (Electronic Software Delivery)-bestandsindeling voor het vastleggen van images
- Gestandaardiseerd proces voor verharding van besturingssysteem, inclusief verplichte installatie van software
- Standaard configuratie van lokale admin- en gastaccount

resolutie

Het oplossingsproces omvatte een uitgebreide loganalyse en identificatie van de onderliggende oorzaak door middel van gedetailleerd onderzoek.

Identificeer en los de oorzaak op

Uit het onderzoek bleek dat het SysPrep-proces niet op de juiste manier unieke apparaat-id's genereerde tijdens de implementatie van het gouden image.

De betrokken analyse:

Onderzoek van Windows-registersleutels, met name:

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

Verzameling van informatie over de gebruikersidentificatie met behulp van:

`whoami /user`

De vereiste resolutie is dat het SysPrep-proces wordt gewijzigd om ervoor te zorgen dat apparaatspecifieke id's correct worden geregenereerd tijdens de implementatie, waardoor het

dupliceren van ZTNA-apparaat-id's op meerdere fysieke machines wordt voorkomen.

- Het vernieuwen van UDID door het uitvoeren van de opdracht `dartcli.exe -nu` wijzigt de waarde van Nounce onder het registerpad `"HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Cisco\Cisco Secure Client\DeviceDetails"`.
- Als u het JSON-bestand van `C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments` verwijdert en de ZTA-service opnieuw start, wordt de gebruiker ontschreven. U moet de gebruiker handmatig inschrijven. Dit genereert een nieuw JSON-bestand zonder enige andere impact.
- Het vernieuwen van UDID op alle eindpunten mag geen invloed hebben zolang de waarde op geen enkele server wordt geverifieerd/geëvalueerd.

1. Start de opdrachtprompt als beheerder en ga naar de directory `"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\DART"`.

2. Voer `dartcli.exe -u` uit om de waarde van de huidige UDID te controleren.

3. Voer de opdracht `dartcli.exe -nu` uit. Dit commando vernieuwt de UDID.

4. Controleer de nieuwe waarde door de opdracht in stap 2 te herhalen.

5. Verwijder het JSON-bestand uit de map `C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments`

6. Start de VPN- en ZTA-services opnieuw op. Op dit punt moet ZTA in niet-ingeschreven staat zijn.

7. Laat de gebruiker de ZTA handmatig inschrijven

9. Controleer de waarde van de nieuwe `ztnaDeviceId` in het JSON-bestand.

Monitoring en validatie

Na de uitvoering van de corrigerende maatregelen om de unieke generatie van ZTNA-apparaat-ID's te waarborgen:

- Bewaakt het inschrijvingsproces op meerdere machines
- Gecontroleerd of elke machine unieke ZTNA-apparaat-ID's heeft gegenereerd
- Bevestigde functionaliteit voor posturecontrole op alle ingeschreven apparaten
- Gevalideerd dat overschrijvingen van openbare sleutels niet meer plaatsvonden tijdens inschrijving

Oorzaak

De hoofdoorzaak werd geïdentificeerd als het SysPrep golden image-implementatieproces dat niet op de juiste manier unieke apparaat-id's genereert voor ZTNA-inschrijving. Wanneer meerdere Windows-fysieke machines worden geïmplementeerd vanuit hetzelfde SysPrep-gouden image, blijven bepaalde apparaatspecifieke id's die worden gebruikt om de ZTNA-apparaat-id te genereren, identiek op alle geïmplementeerde machines.

Het SysPrep-proces is weliswaar effectief voor het standaardiseren van de configuratie van het besturingssysteem en de implementatie van software, maar is niet geconfigureerd om de specifieke id's te regenereren die de Cisco Secure Client gebruikt om unieke ID's voor ZTNA-apparaten te maken. Dit resulteerde erin dat alle machines die werden geïmplementeerd vanuit hetzelfde gouden image identieke identificatieparameters van het ZTNA-apparaat erven, wat leidde tot inschrijvingsconflicten en verificatiefouten in de Secure Access-infrastructuur.

Gerelateerde inhoud

- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.