Resolución de ID de dispositivos ZTNA duplicados en implementaciones de acceso seguro mediante imágenes doradas de SysPrep

Contenido

Problema

Varias máquinas físicas de Windows implementadas a partir de una imagen dorada de SysPrep están generando identificadores de dispositivo ZTNA idénticos, específicamente el mismo ztnaDeviceId en varios terminales. Esta duplicación provoca varios problemas críticos:

- Reinscripción repetida de dispositivos con el mismo ID de dispositivo ZTNA
- La clave pública se sobrescribe durante cada proceso de reinscripción
- Errores de comprobación de estado en todos los equipos, excepto en el dispositivo inscrito más recientemente
- Fallos de acceso a través de Secure Access para los terminales afectados

El comportamiento observado se produce cuando varias máquinas de la flota comparten el mismo ID de dispositivo ZTNA, lo que hace que cada inscripción sobrescriba la clave pública de la máquina anterior. Todas las máquinas, excepto la última en inscribirse, no pueden enviar comprobaciones de estado, lo que provoca la denegación de acceso a través de la infraestructura de acceso seguro.

Se identificaron varios pares de nombre de host e ID de usuario vinculados al mismo ID de dispositivo ZTNA, lo que demuestra el alcance del problema de duplicación a lo largo de la implementación.

Entorno

- Cisco Secure Access (implementación de ZTNA)

- Máquinas físicas de Windows (no máquinas virtuales)
- Metodología de implementación de imágenes de oro de SysPrep
- Herramientas de Windows ADK (Assessment and Deployment Kit) para la implementación de imágenes
- Formato de archivo ESD (Electronic Software Delivery) para la captura de imágenes
- Proceso de consolidación del SO estandarizado que incluye la instalación obligatoria del software
- Configuración de cuenta de invitado y administración local estándar

Resolución

El proceso de resolución entrañó un análisis exhaustivo de los registros y la identificación de la causa fundamental mediante una investigación detallada.

Identificar y resolver la causa raíz

La investigación reveló que el proceso SysPrep no generaba correctamente identificadores de dispositivos únicos durante la implementación de la imagen dorada.

El análisis consistió en:

Examen de las claves del Registro de Windows, concretamente:

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

Recopilación de información del identificador de seguridad del usuario mediante:

```
whoami /user
```

La resolución requería modificar el proceso SysPrep para garantizar que los identificadores

específicos de dispositivos se regeneraran correctamente durante la implementación, evitando la duplicación de ID de dispositivos ZTNA entre varias máquinas físicas.

- Al renovar el UDID ejecutando el comando dartcli.exe -nu, se cambia el valor de Nounce en la ruta de acceso del Registro "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Cisco\Cisco Secure Client\DeviceDetails".
- La eliminación del archivo JSON de C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments y el reinicio del servicio ZTA anula la inscripción del usuario. Debe inscribir manualmente al usuario. Esto genera un nuevo archivo JSON sin ningún otro impacto.
- La renovación de UDID en todos los extremos no debe tener ningún impacto mientras el valor no se verifique/evalúe en ningún servidor.

1. Inicie el símbolo del sistema como administrador y vaya al directorio "%ProgramFiles(x86)%\Cisco\Cisco Secure Client\DART".

2. Ejecute dartcli.exe -u para comprobar el valor del UDID actual.

3. Ejecute el comando dartcli.exe -nu. Este comando renueva el UDID.

4. Compruebe el nuevo valor repitiendo el comando en el paso 2.

5. Elimine el archivo JSON del directorio C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments

6. Reinicie los servicios VPN y ZTA. En este momento, ZTA debe estar en estado no inscrito.

7. Permita al usuario inscribir manualmente el ZTA

9. Compruebe el valor del nuevo ztnaDeviceId en el archivo JSON.

Supervisión y validación

Después de implementar las medidas correctivas para garantizar la generación de ID de dispositivo ZTNA único:

- Se supervisó el proceso de inscripción en varios equipos.
- Se verificó que cada máquina generaba ID de dispositivos ZTNA únicos
- Funcionalidad de verificación de estado correcta confirmada en todos los dispositivos inscritos
- Se ha comprobado que las sobrescrituras de clave pública ya no se producen durante la inscripción

Causa

La causa raíz se identificó porque el proceso de implementación de la imagen dorada de SysPrep no generaba correctamente identificadores de dispositivo únicos para la inscripción ZTNA. Cuando se implementan varias máquinas físicas de Windows a partir de la misma imagen de oro de SysPrep, ciertos identificadores específicos de dispositivos que se utilizan para generar el ID de dispositivo ZTNA siguen siendo idénticos en todas las máquinas implementadas.

El proceso SysPrep, aunque eficaz para estandarizar la configuración del sistema operativo y la implementación de software, no se configuró para regenerar los identificadores específicos que Cisco Secure Client utiliza para crear ID de dispositivos ZTNA únicos. Como resultado, todas las máquinas implementadas a partir de la misma imagen dorada heredan parámetros de identificación de dispositivos ZTNA idénticos, lo que da lugar a conflictos de inscripción y fallos de autenticación en la infraestructura de acceso seguro.

Contenido relacionado

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).