

Resolva IDs de dispositivo ZTNA duplicadas em implantações de acesso seguro usando imagens douradas SysPrep

Contents

Problema

Várias máquinas físicas Windows implantadas a partir de uma imagem dourada SysPrep estão gerando IDs de dispositivo ZTNA idênticas, especificamente o mesmo `ztnaDeviceId` em vários endpoints. Essa duplicação causa vários problemas críticos:

- Repetição do registro de dispositivos com a mesma ID de dispositivo ZTNA
- A chave pública é substituída durante cada processo de reinscrição
- Falhas de verificação de postura em todas as máquinas, exceto no dispositivo registrado mais recentemente
- Falhas de acesso por meio do acesso seguro para endpoints afetados

O comportamento observado ocorre quando várias máquinas no conjunto compartilham a mesma ID de dispositivo ZTNA, fazendo com que cada registro substitua a chave pública da máquina anterior. Todas as máquinas, exceto a mais recente a ser inscrita, falham ao enviar verificações de postura, resultando em negação de acesso por meio da infraestrutura de Acesso Seguro.

Vários pares de nome de host e ID de usuário foram identificados como sendo vinculados à mesma ID de dispositivo ZTNA, demonstrando o escopo do problema de duplicação na implantação.

Ambiente

- Cisco Secure Access (implementação ZTNA)

- Máquinas físicas do Windows (não máquinas virtuais)
- Metodologia de implantação da imagem de ouro SysPrep
- Ferramentas do Windows ADK (Kit de Avaliação e Implantação) para implantação de imagem
- Formato de arquivo ESD (Electronic Software Delivery) para captura de imagem
- Processo padronizado de proteção do SO, incluindo instalação obrigatória de software
- Configuração de conta de convidado e administrador local padrão

Resolução

O processo de resolução envolveu uma análise de registro abrangente e a identificação da causa raiz por meio de uma investigação detalhada.

Identificar e solucionar a causa raiz

A investigação revelou que o processo SysPrep não estava gerando corretamente identificadores de dispositivos exclusivos durante a implantação da Golden Image.

A análise envolveu:

Exame das chaves de registro do Windows, especificamente:

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

Coleta de informações do Identificador de Segurança do usuário usando:

```
whoami /user
```

A resolução exigiu a modificação do processo SysPrep para garantir que os identificadores específicos do dispositivo sejam regenerados corretamente durante a implantação, evitando a

duplicação de IDs de dispositivo ZTNA em várias máquinas físicas.

- A renovação do UDID executando o comando `dartcli.exe -nu` altera o valor de Nounce no caminho do Registro "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Cisco\Cisco Secure Client\DeviceDetails".
- Excluir o arquivo JSON de `C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments` e reiniciar o serviço ZTA cancela o registro do usuário. Você precisa inscrever o usuário manualmente. Isso gera um novo arquivo JSON sem nenhum outro impacto.
- A renovação do UDID em todos os endpoints não deve ter nenhum impacto, contanto que o valor não seja verificado/avaliado em nenhum servidor.

1. Inicie o prompt de comando como um administrador e vá para o diretório `"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\DART"`.

2. Execute `dartcli.exe -u` para verificar o valor do UDID atual.

3. Execute o comando `dartcli.exe -nu`. Esse comando renova o UDID.

4. Verifique o novo valor repetindo o comando na etapa 2.

5. Exclua o arquivo JSON do diretório `C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments`

6. Reinicie os serviços VPN e ZTA. Neste ponto, o ZTA deve estar no estado não inscrito.

7. Permitir que o usuário inscreva manualmente o ZTA

9. Verifique o valor do novo `ztnaDeviceId` no arquivo JSON.

Monitoramento e validação

Após implementar as medidas corretivas para garantir a geração exclusiva de ID de dispositivo ZTNA:

- Monitorado o processo de registro em vários computadores
- Verificado se cada máquina gerou IDs de dispositivo ZTNA exclusivas

- Funcionalidade de verificação de postura bem-sucedida confirmada em todos os dispositivos registrados
- Validado que as substituições de chave pública não ocorreram mais durante a inscrição

Causa

A causa raiz foi identificada como o processo de implantação da imagem de ouro SysPrep que não está gerando corretamente identificadores de dispositivo exclusivos para registro ZTNA. Quando várias máquinas físicas do Windows são implantadas a partir da mesma imagem dourada do SysPrep, determinados identificadores específicos do dispositivo que são usados para gerar o ID do dispositivo ZTNA permanecem idênticos em todas as máquinas implantadas.

O processo SysPrep, embora eficaz para padronizar a configuração do SO e a implantação de software, não foi configurado para gerar novamente os identificadores específicos que o Cisco Secure Client usa para criar IDs de dispositivo ZTNA exclusivas. Isso resultou em todas as máquinas implantadas a partir da mesma imagem de ouro herdando parâmetros de identificação de dispositivo ZTNA idênticos, levando a conflitos de registro e falhas de autenticação na infraestrutura Secure Access.

Conteúdo relacionado

- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.