

使用SysPrep Golden Images解决安全访问部署中重复的ZTNA设备ID

目录

问题

从SysPrep金色映像部署的多台Windows物理计算机正在生成相同的ZTNA设备ID，尤其是在多个终端上生成相同的ztnaDeviceId。这种重复会导致几个严重的问题：

- 重复重新注册具有相同ZTNA设备ID的设备
- 在每次重新注册过程中都覆盖公钥
- 除最近注册的设备外，所有计算机上的状况检查失败
- 通过受影响终端的安全访问发生访问故障

当队列中的多台计算机共享同一个ZTNA设备ID时，将发生观察到的行为，导致每次注册都覆盖前一台计算机的公钥。除最新注册的计算机以外的所有计算机均无法发送状况检查，从而导致通过安全访问基础设施拒绝访问。

多个主机名和用户ID对被标识为链接到同一ZTNA设备ID，展示了复制问题在整个部署中的范围。

环境

- 思科安全访问（ZTNA实施）
- Windows物理机（非虚拟机）
- SysPrep金色映像部署方法
- 用于映像部署的Windows ADK（评估和部署套件）工具
- 用于图像捕获的ESD（电子软件交付）文件格式

- 标准化的操作系统加固流程，包括强制软件安装
- 标准本地管理员和访客帐户配置

分辨率

解决过程包括全面的日志分析和通过详细调查确定根本原因。

确定并解决根本原因

调查发现，SysPrep流程在金色映像部署期间无法正确生成唯一设备标识符。

分析内容包括：

检查Windows注册表项，特别是：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion

使用下列方式收集用户安全标识符信息：

```
whoami /user
```

解决方法需要修改SysPrep流程，以确保在部署期间正确重新生成设备特定的标识符，从而防止多个物理计算机上的ZTNA设备ID重复。

- 通过运行dartcli.exe -nu命令续订UDID会更改“HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Cisco\Cisco Secure Client\DeviceDetails”注册表路径下Nounce的值。
- 从C:\ProgramData\Cisco\Cisco删除JSON文件安全客户端\ZTA\enrollments并重新启动ZTA服务取消注册用户。您需要手动注册用户。这样会生成新的JSON文件，而不会产生任何其他影响。
- 在所有终端上续订UDID不得有任何影响，只要值未在任何服务器上验证/评估。

1.以管理员身份启动命令提示符，然后转到“%ProgramFiles(x86)%\Cisco\Cisco Secure Client\ Dart”目录。

2.运行dartcli.exe -u以检查当前UDID的值。

3.运行dartcli.exe -nu命令。此命令将更新UDID。

4.重复步骤2中的命令，检验新值。

5.从C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments目录删除JSON文件

6.重新启动VPN和ZTA服务。此时，ZTA必须处于未注册状态。

7.让用户手动注册ZTA

9.验证JSON文件中新ztnaDeviceId的值。

监控和验证

在实施纠正措施以确保生成唯一的ZTNA设备ID后：

- 监控多台计算机的注册过程
- 已验证每台计算机生成的唯一ZTNA设备ID
- 确认所有已注册设备上的状态检查功能成功
- 已验证在注册期间不再发生公钥覆盖

原因

根本原因是未正确为ZTNA注册生成唯一设备标识符的SysPrep金色映像部署过程。当从同一SysPrep金牌映像部署多个Windows物理计算机时，用于生成ZTNA设备ID的特定设备标识符在所有已部署计算机上保持相同。

SysPrep流程虽然对标准化操作系统配置和软件部署有效，但并未配置为重新生成思科安全客户端用于创建唯一ZTNA设备ID的特定标识符。这导致从同一黄金映像部署的所有计算机继承相同的ZTNA设备识别参数，从而导致安全访问基础设施中的注册冲突和身份验证失败。

相关内容

- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。