Windows GPO脚本和Cisco NAC互操作性

目录

简介

本文为Windows GPO提供一配置示例在PC启动和用户登录给域。Windows GPO可以配置运行多种脚本在PC启动和用户登录到域。脚本由企业是常用的配置环境变量，映射远程驱动等。

当用户首先连接并且设法注册到Windows机器时，思科美洲台控制对网络的访问。

脚本可以分类作为启动/被关闭的和登录/注销脚本。

Windows在计算机上下文运行启动和关闭脚本。这只作用，如果NAC设备打开特定的角色的脚本要求的适当的网络资源，当这些脚本被执行在PC启动或关闭时，典型地是未经鉴定的角色。

登录和注销脚本在用户上下文被执行，因此意味着在用户以后的登录脚本执行通过windows姬娜登陆。登录脚本可以不能执行并且/或者完成执行，如果用户认证或计算机状态评估不完成，并且网络访问没有授权及时。这些脚本可能被美洲台代理程序启动的IP地址刷新也中断在OOB登录事件以后。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

GPOs脚本的一般建议

这些是GPO脚本的一般建议：

1. 当您调试时，请运行在可视模式的脚本。这允许视觉暗示登录脚本实际上被执行。此GPO策略可以配置在**域策略>用户配置>Administrative下模板>System >脚本**。
2. 保证计算机等待网络是可用的在计算机启动和登录。此GPO策略可以配置在**域策略>计算机Configuration>管理模板>System >登录下**。

美洲台设置的一般建议

若被采用这些是与GPO一起设置的美洲台的一般建议：

1. 允许需要的流量在CAS间流在一个未经鉴定的角色允许登录脚本的Windows登陆和复制从AD的到在网络的客户端机器执行。`Ports are TCP : 88,123,135,137,139,389,445,1025,1026,3268 Ports are UDP : 88,123,135,137,139,389,445,1025,1026,3268 Allow Fragmented packets and ICMP to all domain controllers.` **注意：** Windows使用PING发现过程查找有超过一个给的域的一个DC的最近的DC。万一ICMP没有允许两DC，客户端能采取更加长登陆，因为拾起随机的DC，如果初始发现发生故障。
2. 由于这是Windows AD环境，若可能请使用ADSSO作为认证方法。这自动化并且加速用户登录进程，以及提高整体用户体验。

配置

几方案和建议的美洲台配置跟随。

场景 1

Windows登录脚本从AD控制器被执行和运行异步地。

异步脚本执行是Win2003 AD的默认行为。当Windows登录脚本运行异步地，它回到Windows登录进程的传递控制权，在调用脚本后。它不等待脚本完成执行。这允许其他起始程序和美洲台代理程序通常装载。

如果登录脚本要求网络访问，是由NAC设备控制的并且在成功的用户登录以后是可访问对美洲台，登录脚本能体验某延迟。例如检查登录脚本在实际登录脚本执行前学习网络可用性，：

```
:CHECK
@echo off
echo Please wait....
ping -n 1 -l 1 10.10.10.10
if errorlevel 1 goto CHECK
@echo on

# Now the actual Logon script:

net use L: \\fileserver\share
```

注意： 修改脚本符合网络拓扑。

由于此应急方案简单，良好工作，只要登录脚本运行异步地，并且没有由于出于波段美洲台部署介入的IP地址更改或。

如果脚本同步地运行，此应急方案发生故障，因为美洲台代理程序不装入内存，在登录脚本完成执行前，并且登录脚本从未完成执行，因为等待网络资源可用性，变得可用，在美洲台代理程序验证客户端PC之后。

此屏幕画面显示客户端PC留在死环路的此状态由于被提及的原因。

此方案可以也失效脚本在慢速广域网链路运行异步地脚本能需要一会儿下载的情况，并且美洲台在IP刷新可以配置的OOB拓扑方面部署。IP刷新在脚本执行中间能潜在中断脚本执行。在例如方案中，思科强烈建议您运行脚本同步地，以便IP刷新进程不干涉脚本执行。此方案表示这样一个情况。

场景 2

Windows登录脚本从AD控制器同步地运行。

同步脚本在美洲台IP刷新发生的OOB部署推荐。

基本想法是拆分原始登录脚本的功能到两份脚本。

写脚本一，被执行作为登录脚本，以后复制第二份脚本到执行的本地设备，当美洲台代理程序验证时，并且网络访问授权。

第二份脚本可以由Windows起始程序自动地呼叫，如果放置第二份脚本到用户的起始文件夹，例如：

脚本1 ：

从AD执行的登录脚本复制实际脚本呼叫“mount.bat”对用户的起始文件夹最新执行的。

```
echo Please wait....
sleep 20
copy \\1.1.1.11\SHARE\mount.bat
   "c:\Documents and Settings\All users\Start Menu\Programs\Startup\mount.bat"
```

注意： 修改脚本配合网络拓扑。

注意： 允许需要的流量在CAS间流在一个未经鉴定的角色允许登录脚本的Windows登陆和复制从AD的到在网络的客户端机器执行。

脚本2

由于安全原因附属脚本，实际操作发生从系统被执行本地并且在执行以后删除。

```
ipconfig
:CHECK
@echo off
echo Please wait....
sleep 10
Ping -n 1 -l 1 10.10.10.10
if errorlevel 1 goto CHECK
@echo on
# Now the actual Logon script:

net use L: \\fileserver\share
del c:\Documents and Settings\All users\Start Menu\Programs\Startup\mount.bat"
```

此屏幕画面表示在背景运行的第二份脚本从用户的起始文件夹启动，并且美洲台代理程序执行IP刷新，在验证后。在完成并且映射驱动前，第二份脚本循环并且等待代理程序完成验证和IP刷新进程。

故障排除

故障排除必须依个执行根据基本类型，然而捕获客户端PC连接的switchport的数据包是一个巨大方式开始。这将给予您关于网元和活动的洞察力。

相关信息

- 技术支持和文档 - Cisco Systems