Interoperabilidad del NAC de los scripts y de Cisco de Windows GPO

Contenido

Introducción

Este documento proporciona una configuración de muestra para Windows GPO en el inicio del lanzamiento y del usuario PC al dominio. Windows GPO se puede configurar para funcionar con los diversos scripts en el inicio del lanzamiento y del usuario PC al dominio. Los scripts son de uso frecuente por la empresa configurar las variables de entorno, asociar las unidades etc. del telecontrol.

El NAC de Cisco controla el acceso a la red cuando el usuario primero conecta e intenta abrir una sesión a la máquina de Windows.

Los scripts se pueden clasificar como lanzamiento/apagan y abren una sesión/los scripts del cierre de sesión.

Windows funciona con el lanzamiento y apaga los scripts en el contexto de la máquina. Esto funciona solamente si el dispositivo NAC abre a los recursos de red apropiados requeridos por el script para el rol específico cuando estos scripts se ejecutan en el bootup PC o apagan, que es típicamente el papel del unauthenticated.

Los scripts del inicio y del cierre de sesión se ejecutan en el contexto del usuario, así que significa que la secuencia de comandos de inicio ejecuta después de que el usuario haya abierto una sesión a través de las ventanas GINA. La secuencia de comandos de inicio puede no poder ejecutar y/o completar la ejecución si la autenticación de usuario o la evaluación de la postura de la máquina no completa y el acceso a la red no se concede a tiempo. Estos scripts se pueden también interrumpir por la dirección IP restauran iniciado por el agente del NAC después OOB de

un evento de inicio de sesión.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

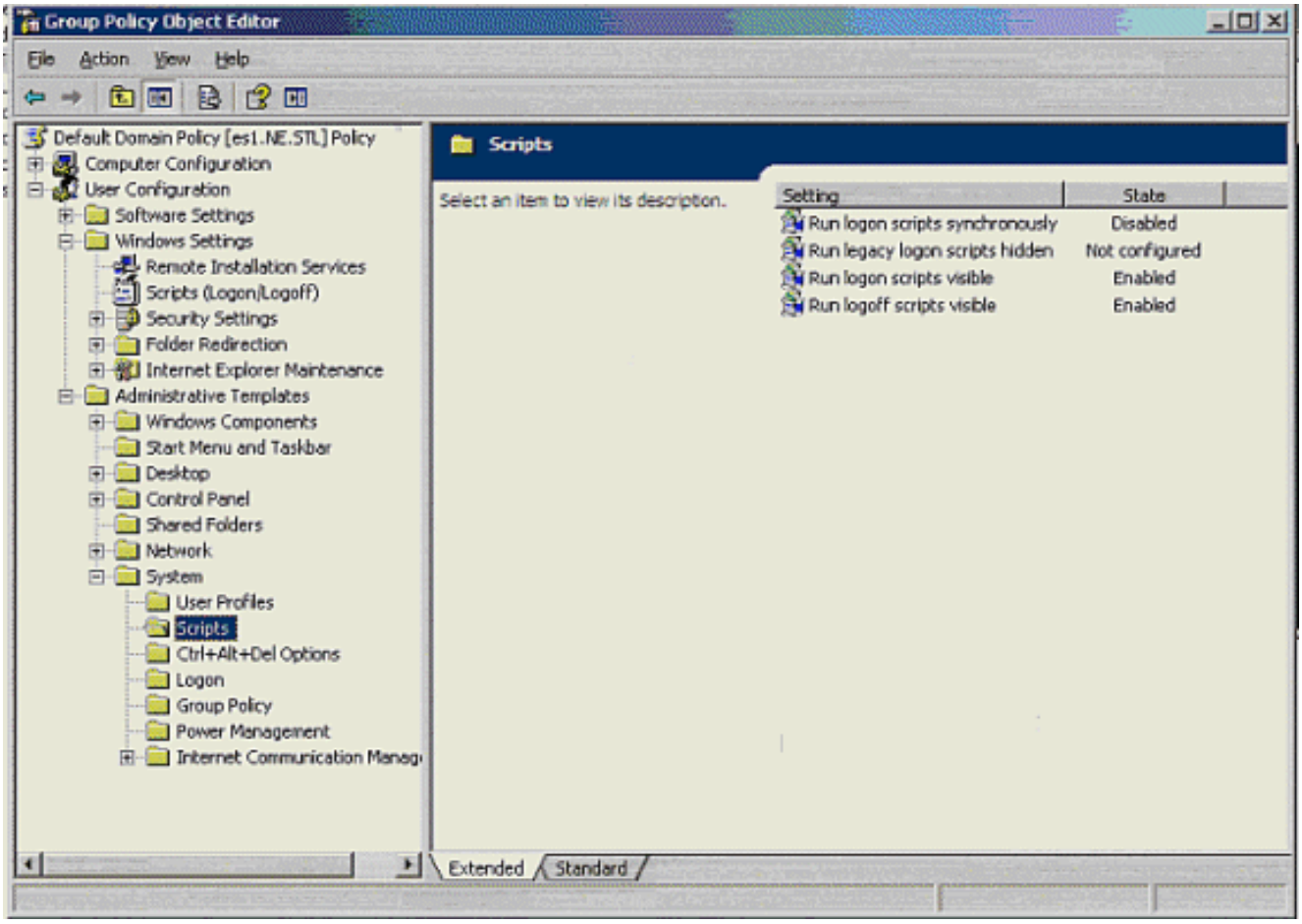
Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

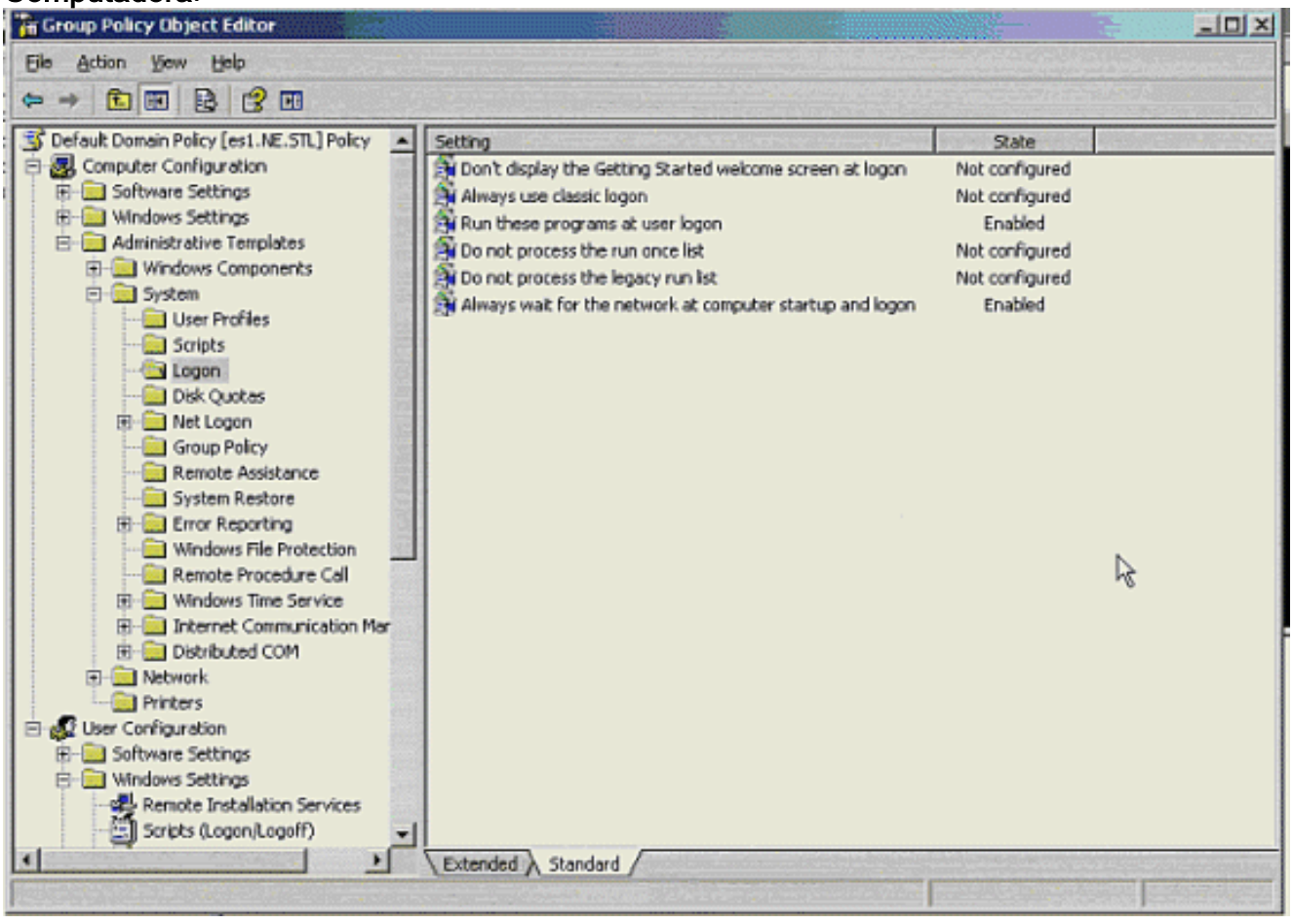
Recomendaciones generales para los scripts de GPOs

Éstas son recomendaciones generales para los scripts GPO:

1. Funcione con los scripts en el modo visible cuando usted hace el debug de. Esto permite la indicación visual que las secuencias de comandos de inicio estén ejecutadas realmente.Esta directiva GPO se puede configurar bajo la **política de dominio > la configuración de usuario > las plantillas administrativas > el sistema > scripts**.



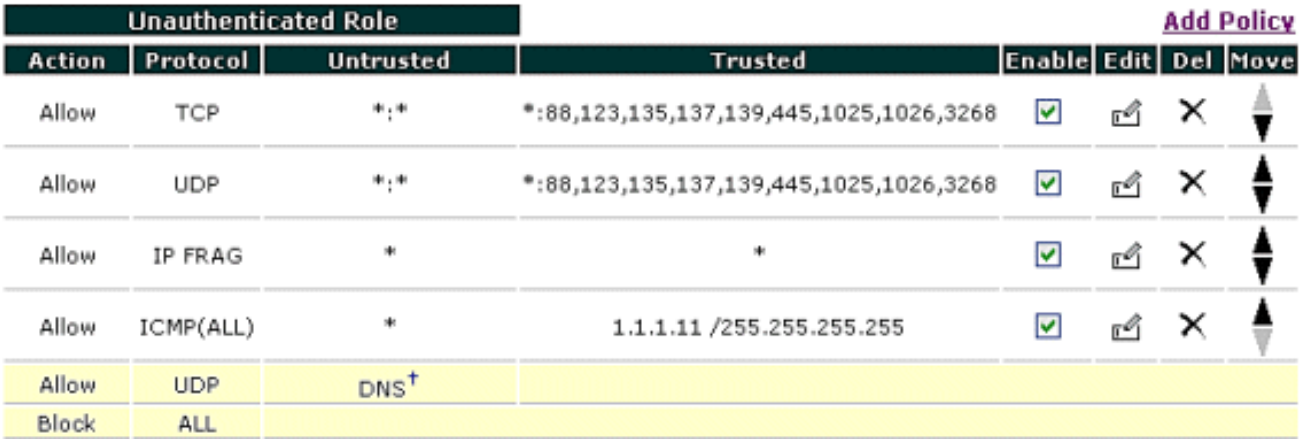
2. Asegúrese de que el ordenador espere la red para estar disponible en el lanzamiento del ordenador y abra una sesión.Esta directiva GPO se puede configurar bajo la **política de dominio > la configuración > las plantillas administrativas > el sistema > inicio de Computadora**.



Recomendaciones generales para la configuración del NAC

Éstas son recomendaciones generales para el NAC puesto si está utilizado junto con GPO:

1. Permita que el tráfico requerido fluya a través de CAS en un papel del unauthenticated para permitir el inicio del Dominio de Windows y la copia de las secuencias de comandos de inicio del AD a la máquina del cliente sobre la red para la ejecución.`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.`



Unauthenticated Role — Add Policy

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Allow	TCP	*:*	*:88,123,135,137,139,445,1025,1026,3268	☑	✎	✕	▲▼
Allow	UDP	*:*	*:88,123,135,137,139,445,1025,1026,3268	☑	✎	✕	▲▼
Allow	IP FRAG	*	*	☑	✎	✕	▲▼
Allow	ICMP(ALL)	*	1.1.1.11 /255.255.255.255	☑	✎	✕	▲▼
Allow	UDP	DNS†					
Block	ALL						

Nota: Windows utiliza el proceso de detección del PING para encontrar DC más cercano donde hay más de un DC para un dominio dado. En caso de que el ICMP se prohiba dos DCS, el cliente puede durar para iniciar sesión puesto que coge DC al azar si la detección inicial falla.
2. Porque esto es un entorno de Windows AD, utilice ADSSO como el método de autentificación, si es posible. Esto automatiza y acelera el proceso del inicio del usuario, así como aumenta la experiencia total del usuario.

Configurar

Varios escenarios y configuraciones de NAC sugeridas siguen.

Escenario 1

Las secuencias de comandos de inicio de Windows se ejecutan del regulador AD y son asynchronously ejecutado.

La ejecución asíncrona del script es el comportamiento predeterminado para Win2003 AD. Cuando la secuencia de comandos de inicio de Windows es asynchronously ejecutado, él control de transferencias de nuevo al proceso del inicio de Windows después de que invoque el script. No espera el script para acabar la ejecución. Esto permite que otros programas de lanzamiento y el agente del NAC carguen normalmente.

Si las secuencias de comandos de inicio requieren el acceso a la red, que son controladas por el dispositivo NAC y son accesibles después de que inicio acertado del usuario al NAC, la secuencia de comandos de inicio puede experimentar un cierto retardo. Marque la secuencia de comandos de inicio para aprender la disponibilidad de la red antes de que la secuencia de comandos de inicio real ejecute, por ejemplo:

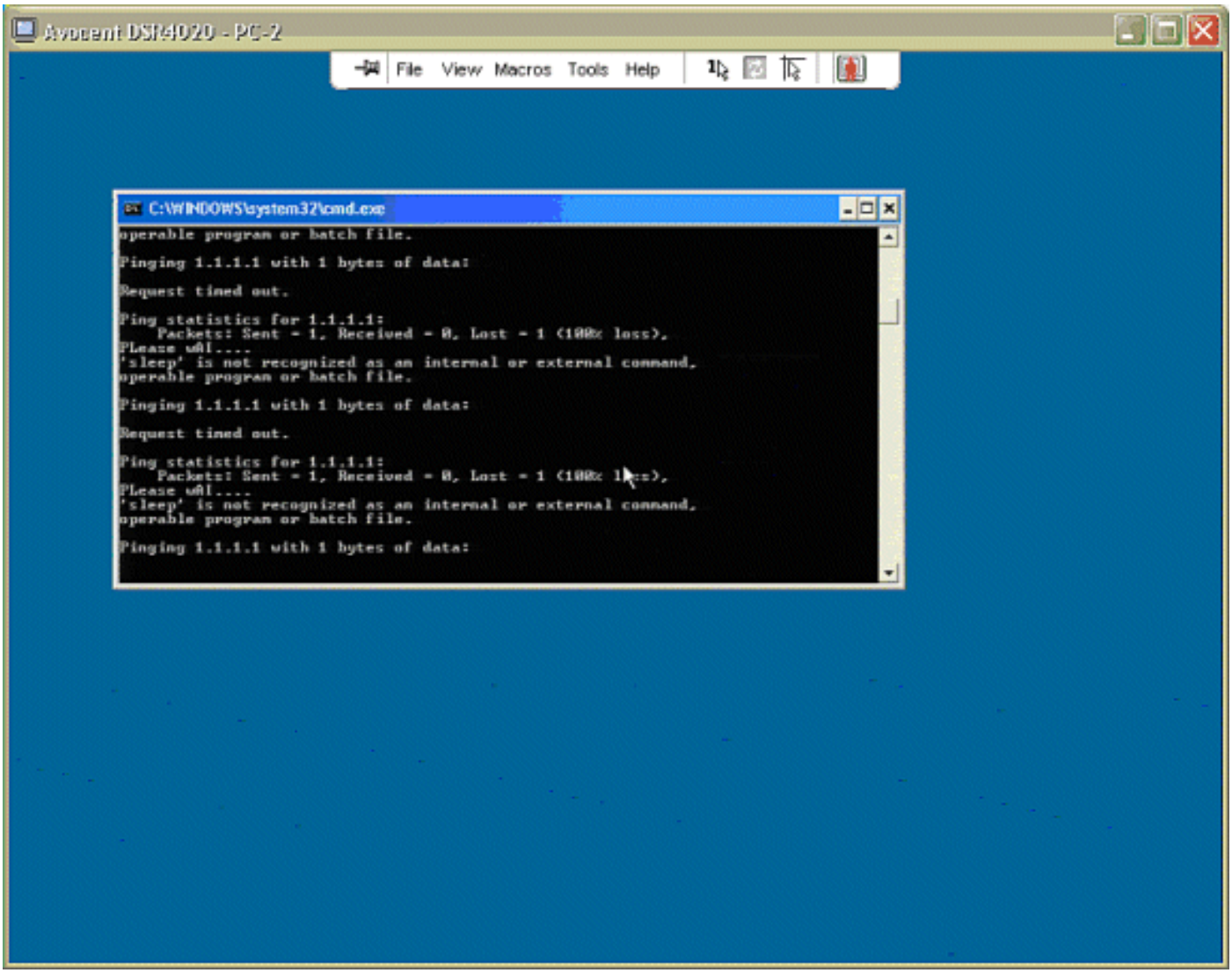
```
:CHECK
@echo off
echo Please wait....
ping -n 1 -l 1 10.10.10.10
if errorlevel 1 goto CHECK
@echo on

# Now the actual Logon script:

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

Nota: Modifique el script de acuerdo con la topología de red.

Porque esta solución alternativa es simple, trabaja muy bien mientras las secuencias de comandos de inicio sean asynchronously ejecutado, y no hay cambio de la dirección IP implicado como resultado fuera del despliegue del NAC de la banda o de otra manera.

Si los scripts se funcionan con síncrono, esta solución alternativa falla porque el agente del NAC no carga en la memoria antes de que la secuencia de comandos de inicio acabe la ejecución, y la secuencia de comandos de inicio nunca completa la ejecución porque espera la Disponibilidad de recurso de red, que está disponible solamente después que el agente del NAC autentica PC del cliente.

Esta captura de pantalla muestra que PC del cliente permanece en este estado del Loop infinito debido a la razón mencionada.



Este escenario puede también fallar en una situación donde están asynchronously los scripts ejecutado sobre un link WAN lento donde los scripts ellos mismos pueden tardar un rato para descargar, y el NAC se despliega en OOB la topología donde el IP restaura puede ser configurado. Un IP restaura en el medio de la ejecución del script puede potencialmente romper la ejecución del script. En por ejemplo el escenario, Cisco recomienda fuertemente que usted funciona con los scripts síncrono de modo que el IP restaure el proceso no interfiera con la ejecución del script. Este escenario representa tal situación.

Escenario 2

Las secuencias de comandos de inicio de Windows se ejecutan del regulador AD síncrono.

Los scripts síncronos se recomiendan en el despliegue del NAC OOB donde ocurre el IP restaura.

La idea básica es partir las funciones de la secuencia de comandos de inicio original en dos scripts.

El script *uno*, que se ejecuta como secuencia de comandos de inicio, apenas copia el segundo script a la máquina local para la ejecución en otro momento cuando el agente del NAC ha autenticado, y se concede el acceso a la red.

El segundo script se puede llamar por el programa de lanzamiento de Windows automáticamente si usted coloca el segundo script en la carpeta Startup (Inicio) del usuario, por ejemplo:

Script 1:

La secuencia de comandos de inicio ejecutada del AD copió el script real llamado “mount.bat” a la carpeta Startup (Inicio) del usuario para la ejecución posterior.

```
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"
```

Nota: Modifique el script para adaptarse a la topología de red.

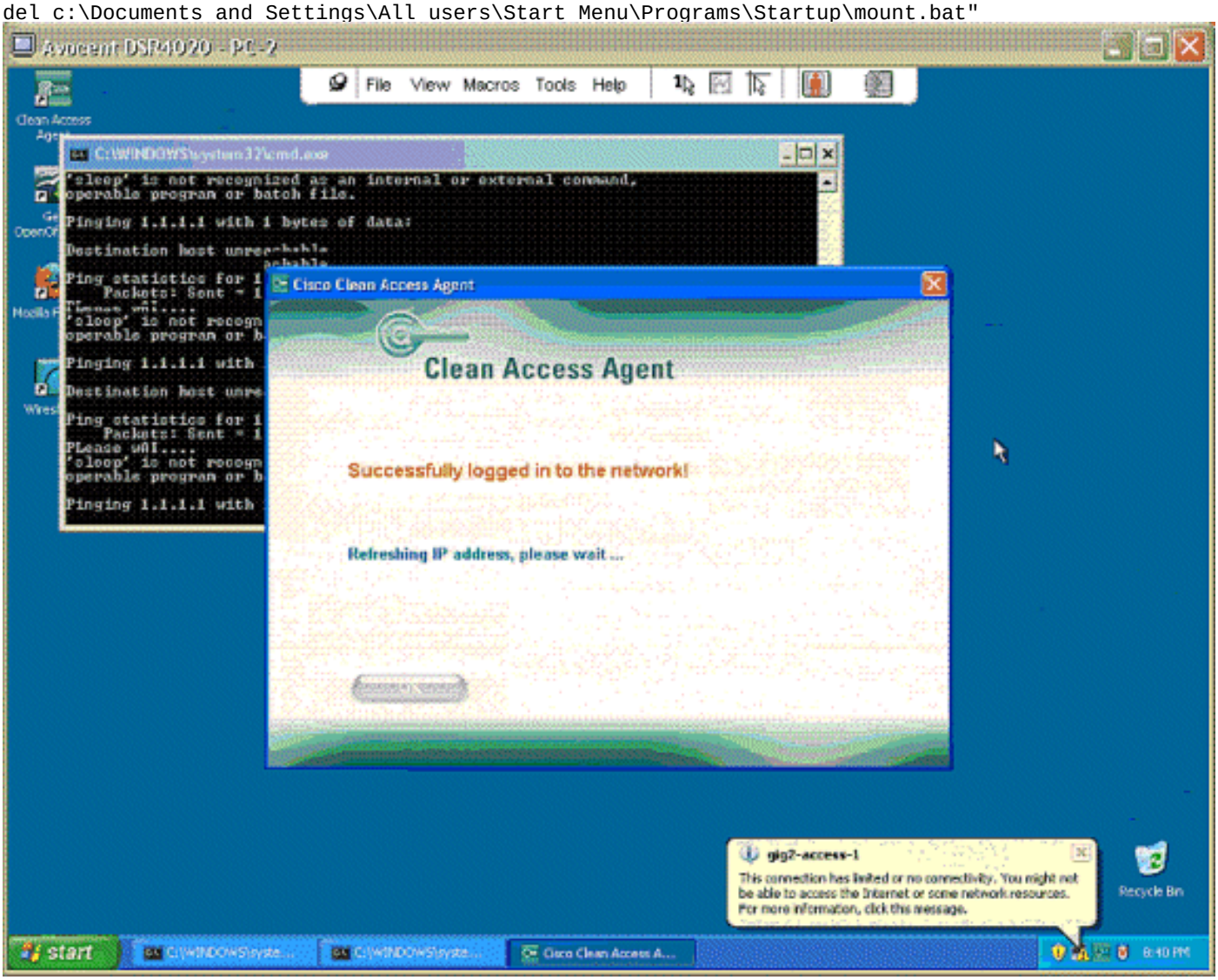
Nota: Permita que el tráfico requerido fluya a través de CAS en un papel del unauthenticated para permitir el inicio del Dominio de Windows y la copia de las secuencias de comandos de inicio del AD a la máquina del cliente sobre la red para la ejecución.

Script 2

El script secundario, donde ocurre la acción real se ejecuta localmente del sistema y se borra después de la ejecución por razones de seguridad.

```
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"
```



Esta captura de pantalla representa que el segundo script que se ejecuta en el fondo está iniciado de la carpeta Startup (Inicio) del usuario, y el agente del NAC hace un IP restaura después de que autentique. El segundo script coloca y espera el agente para completar la autenticación y el IP restaura el proceso antes de que complete y asocie las unidades.

Troubleshooting

El troubleshooting tiene que ser hecho sobre caso por caso la base, no obstante la captura de los paquetes del switchport en el cual PC del cliente está conectado es una gran manera de comenzar. Esto le dará la penetración sobre los eventos de red y las actividades.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems