Scripts de Windows GPO e Interoperabilidade de Cisco NAC

Índice

Introdução

Este documento fornece uma configuração de exemplo para Windows GPO no fazer logon da partida e do usuário PC ao domínio. Windows GPO pode ser configurado para executar vários scripts no fazer logon da partida e do usuário PC ao domínio. Os scripts são usados frequentemente pela empresa configurar variáveis de ambiente, traçar as movimentações etc. do telecontrole.

Cisco NAC controla o acesso à rede quando o usuário primeiramente conecta e tenta entrar à máquina de Windows.

Os scripts podem ser classificados como scripts da partida/parada programada e do fazer logon/fazer logoff.

Windows executa a partida e a parada programada passa pelo processo de script no contexto da máquina. Isto funciona somente se a ferramenta NAC abre os recursos de rede apropriados exigidos pelo script para o papel particular quando estes scripts estão executados na inicialização ou na parada programada PC, que são tipicamente o papel não autenticado.

Os scripts do fazer logon e do fazer logoff são executados no contexto do usuário, assim que significa que o script de logon executa depois que o usuário entrou através dos indicadores GINA. O script de logon pode não executa e/ou não termina a execução se a autenticação de usuário ou a avaliação da postura da máquina não terminam e o acesso de rede não está concedido a tempo. Estes scripts podem igualmente ser interrompidos pelo endereço IP de Um ou Mais Servidores Cisco ICM NT refrescam iniciado pelo agente NAC depois que um evento do fazer

logon OOB.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Recomendações gerais para scripts de GPOs

Estas são recomendações gerais para scripts GPO:

1. Execute os scripts no modo visível quando você debuga. Isto permite a indicação visual que os scripts de logon estão executados realmente.Esta política GPO pode ser configurada sob a **política de domínio > a configuração do usuário > moldes > sistema > scripts administrativos**.
2. Assegure-se de que o computador espere a rede para estar disponível na partida do computador e entre-se.Esta política GPO pode ser configurada sob a **política de domínio > a configuração de computador > moldes > sistema > fazer logon administrativos**.

Recomendações gerais para a instalação NAC

Estas são recomendações gerais para o NAC setup se usado junto com GPO:

1. Permita que o tráfego exigido flua através de CAS em um papel não autenticado para permitir o fazer logon do domínio do Windows e a cópia dos scripts de logon do AD à máquina cliente sobre a rede para a execução.`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.` **Nota:** Windows usa o processo de descoberta PING para encontrar o DC o mais próximo onde há mais de um DC para um domínio dado. Caso que o ICMP não são permitidos dois DC, o cliente pode tomar

mais por muito tempo para entrar desde que pegara um DC aleatório se a descoberta inicial falha.
2. Porque este é um ambiente de Windows AD, use ADSSO como o método de autenticação, se possível. Isto automatiza e acelera o processo do fazer logon do usuário, assim como aumenta a experiência total do usuário.

Configurar

Diversas encenações e configurações NAC sugeridas seguem.

Cenário 1

Os scripts de logon de Windows são executados do controlador AD e executados assincronamente.

A execução assíncrona do script é o comportamento padrão para Win2003 AD. Quando o script de logon de Windows for executado assincronamente, ele controle de transferências de volta ao processo do fazer logon de Windows depois que invoca o script. Não espera o script para terminar a execução. Isto permite que outros programas start-up e o agente NAC carreguem normalmente.

Se os scripts de logon exigem o acesso de rede, que estão controlados pela ferramenta NAC e são acessíveis depois que fazer logon bem sucedido do usuário ao NAC, o script de logon pode experimentar algum atraso. Verifique o script de logon para aprender a disponibilidade da rede antes que o script de logon real execute, por exemplo:

```
: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: Altere o script de acordo com a topologia de rede.

Porque esta ação alternativa é simples, trabalha muito bem enquanto os scripts de logon são executados assincronamente, e não há nenhuma mudança do endereço IP de Um ou Mais Servidores Cisco ICM NT envolvida em consequência fora do desenvolvimento da faixa NAC ou de outra maneira.

Se os scripts são executados synchronously, esta ação alternativa falha porque o agente NAC não carrega na memória antes que o script de logon termine a execução, e o script de logon nunca termina a execução porque espera a Disponibilidade de recursos de rede, que se torna disponível somente depois que o agente NAC autentica o PC cliente.

Este screen shot mostra que o PC cliente permanece neste estado de loop infinito devido à razão mencionada.

Esta encenação pode igualmente falhar em uma situação onde os scripts sejam executados

assincronamente sobre um enlace de WAN lento onde os scripts eles mesmos possam tomar um quando para transferir, e o NAC é distribuído na topologia OOB onde o IP refresca pode ser configurado. Um IP refresca no meio da execução do script pode potencialmente quebrar a execução do script. Como na encenação, Cisco recomenda fortemente que você executa scripts synchronously de modo que o IP refresque o processo não interfira com a execução do script. Esta encenação descreve tal situação.

Cenário 2

Os scripts de logon de Windows são executado do controlador AD synchronously.

Os scripts síncronos são recomendados no desenvolvimento NAC OOB onde o IP refresca ocorre.

A ideia básica é rachar a funcionalidade do script de logon original em dois scripts.

Passar pelo processo de script *um*, que é executado como um script de logon, apenas copia o segundo script à máquina local para a execução mais tarde quando o agente NAC autenticou, e o acesso de rede está concedido.

O segundo script pode ser chamado pelo programa startup de Windows automaticamente se você coloca o segundo script na pasta de inicialização do usuário, por exemplo:

Script 1:

O script de logon executado do AD copiou o script real chamado “mount.bat” à pasta de inicialização do usuário para uma execução mais atrasada.

```
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: Altere o script para serir a topologia de rede.

Nota: Permita que o tráfego exigido flua através de CAS em um papel não autenticado para permitir o fazer logon do domínio do Windows e a cópia dos scripts de logon do AD à máquina cliente sobre a rede para a execução.

Script 2

O script secundário, onde a ação real ocorre é executado localmente do sistema e suprimido após a execução por razões de segurança.

```
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"
```

Este screen shot descreve que o segundo script que é executado no fundo está lançado da pasta de inicialização do usuário, e o agente NAC faz um IP refresca depois que autentica. O segundo script dá laços e espera no agente para terminar a autenticação e o IP refresca o processo antes que termine e trace as movimentações.

Troubleshooting

O Troubleshooting tem que ser feito caso por caso na base, porém capturar pacotes fora do switchport em que o PC cliente é conectado é uma grande maneira de começar. Isto dar-lhe-á a introspecção sobre os eventos de rede e as atividades.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems