Взаимодействие сценариев GPO Windows и Cisco NAC

Содержание

Введение

Этот документ предоставляет пример конфигурации для Windows GPO при запуске ПК, и пользователь входят в систему к домену. Windows GPO может быть настроен для выполнения различных сценариев при запуске ПК, и пользователь входят в систему к домену. Сценарии часто используются предприятием, чтобы настроить переменные среды, подключить удаленные диски и т.д.

Доступ средств управления за NAC Cisco к сети, когда пользователь сначала подключает и пытается войти в систему к машине Windows.

Сценарии могут быть классифицированы как сценарии запуска/завершения и входа в систему/выхода из системы.

Windows выполняет запуск и сценарии завершения в контексте машины. Это только функционирует, если NAC-устройство открывает соответствующие сетевые ресурсы, требуемые сценарием для специальной роли, когда эти сценарии выполняются в загрузке ПК или завершении, которое, как правило, является неаутентифицированной ролью.

Войдите в систему и выйдите из системы, сценарии выполняются в пользовательском контексте, что означает, что сценарий входа в систему выполняется после того, как пользователь вошел через окна GINA. Сценарий входа в систему может быть не в состоянии выполнять и/или завершать выполнение, если оценка положения проверки подлинности пользователя или машины не завершает, и доступ к сети не предоставляют вовремя. Эти сценарии могут также быть прерваны обновлением IP-адреса, инициируемым

агентом NAC после события входа в систему OOB.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

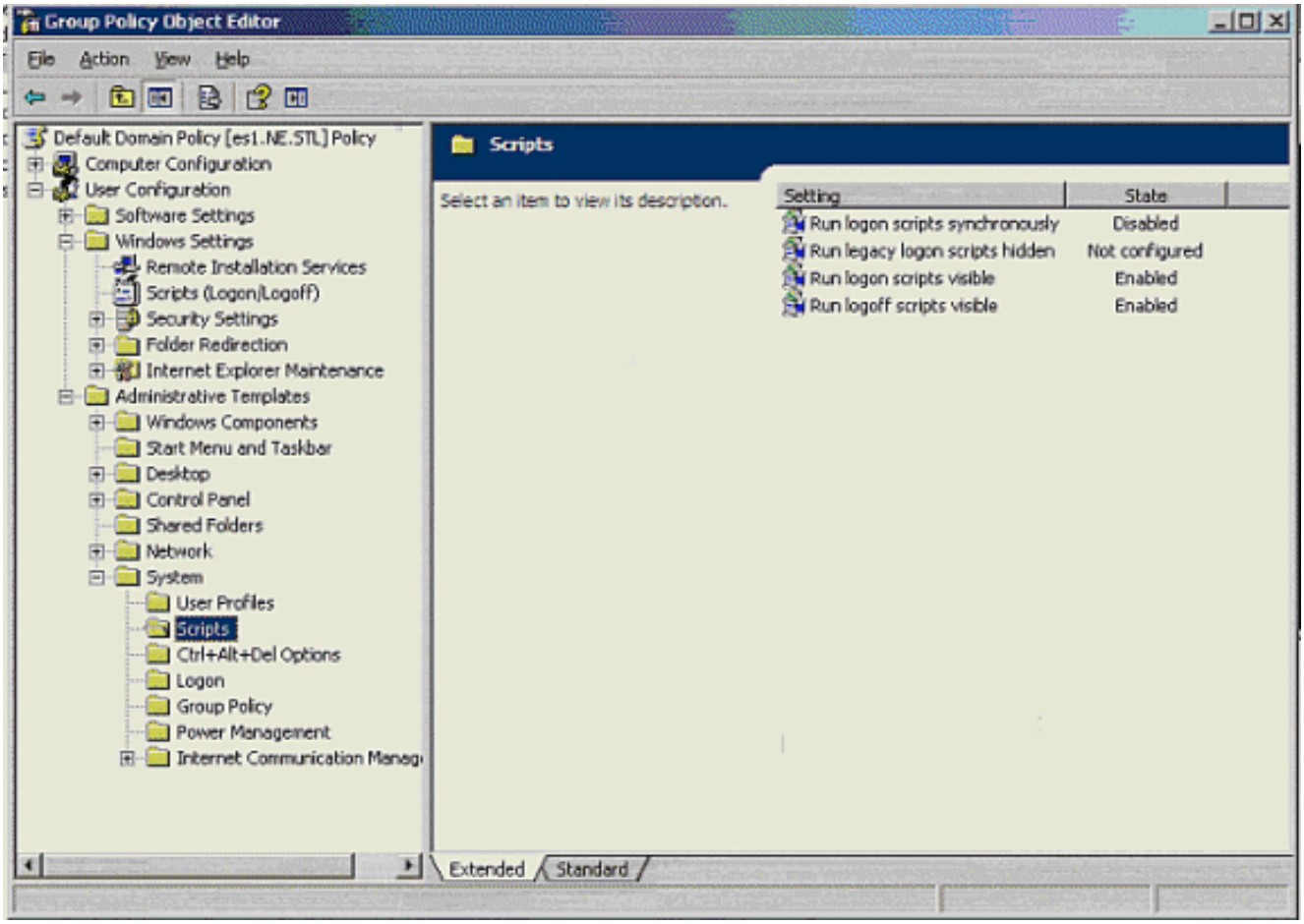
Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

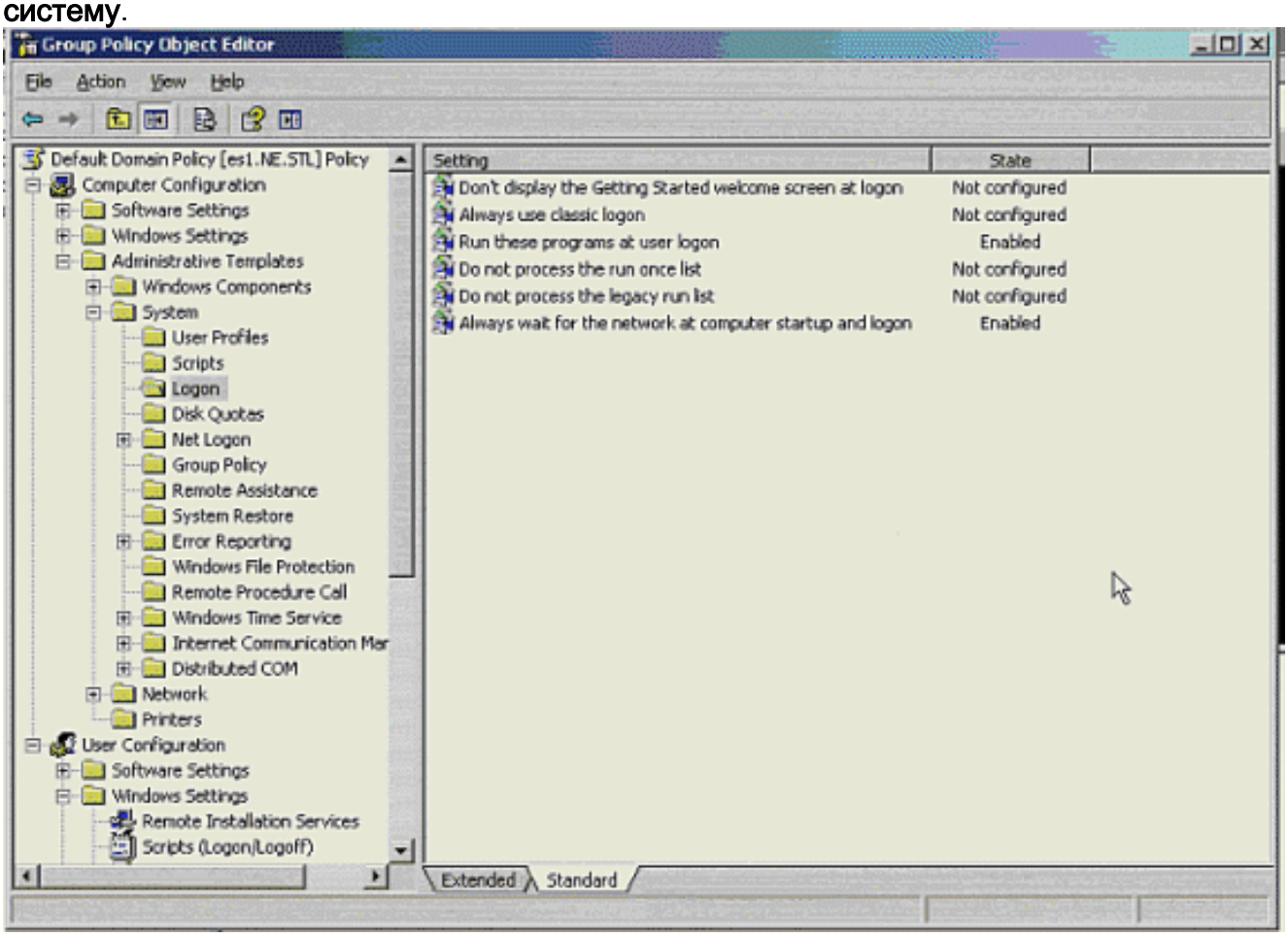
Общие рекомендации для сценариев GPOS

Это общие рекомендации для сценариев GPO:

1. Выполните сценарии в видимом режиме, когда вы отладите. Это позволяет визуальную индикацию, что фактически выполняются сценарии входа в систему.Эта политика GPO может быть настроена под **Политикой домена> Пользовательская конфигурация> Административные Шаблоны> Система>**
Сценарии.



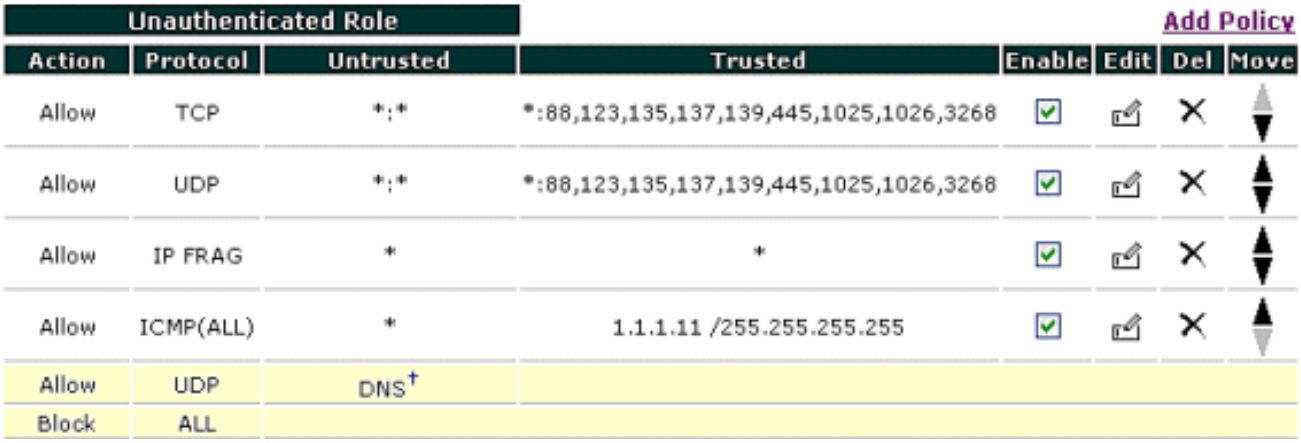
2. Гарантируйте, что компьютер ждет сети, чтобы быть доступным при компьютерном запуске и входе в систему.Эта политика GPO может быть настроена под **Политикой домена> Конфигурация компьютера> Административные Шаблоны> Система> Вход в систему**.



Общие рекомендации для настройки NAC

Это общие рекомендации для настройки NAC, если используется наряду с GPO:

1. Позвольте необходимому трафику течь через CAS в неаутентифицированной роли для разрешения входа в систему Домена Windows и копии сценариев входа в систему с AD на клиентский компьютер по сети для выполнения.`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						

Примечание: Windows использует процесс обнаружения PING для обнаружения самого близкого DC, где существует несколько DC для данного домена. В случае, если ICMP не позволяют два DC, клиент может занять больше времени для входа в систему, так как он берет случайный DC, если отказывает первоначальное обнаружение.
2. Поскольку это - среда Windows AD, используйте ADSSO в качестве метода аутентификации, если это возможно. Это автоматизирует и ускоряет пользовательский процесс входа в систему, а также улучшает полный пользовательский опыт.

Настройка

Несколько сценариев и предложенных конфигураций NAC придерживаются.

Сценарий 1

Сценарии входа в систему Windows выполняются от AD контроллера и выполнены асинхронно.

Асинхронное выполнение сценария является поведением по умолчанию для Win2003 AD. Когда сценарий входа в систему Windows выполнен асинхронно, он возвращает контроль к процессу входа в систему Windows после того, как он вызывает сценарий. Это не ждет сценария для завершения выполнения. Это позволяет другим программам запуска и агенту NAC обычно загружаться.

Если сценарии входа в систему требуют доступа к сети, которые управляются NAC-устройством и доступны после того, как успешный пользовательский вход в систему NAC, сценарий входа в систему может испытать некоторую задержку. Проверьте сценарий входа в систему для обучения доступности сети, прежде чем фактический сценарий входа в систему выполнится, например:

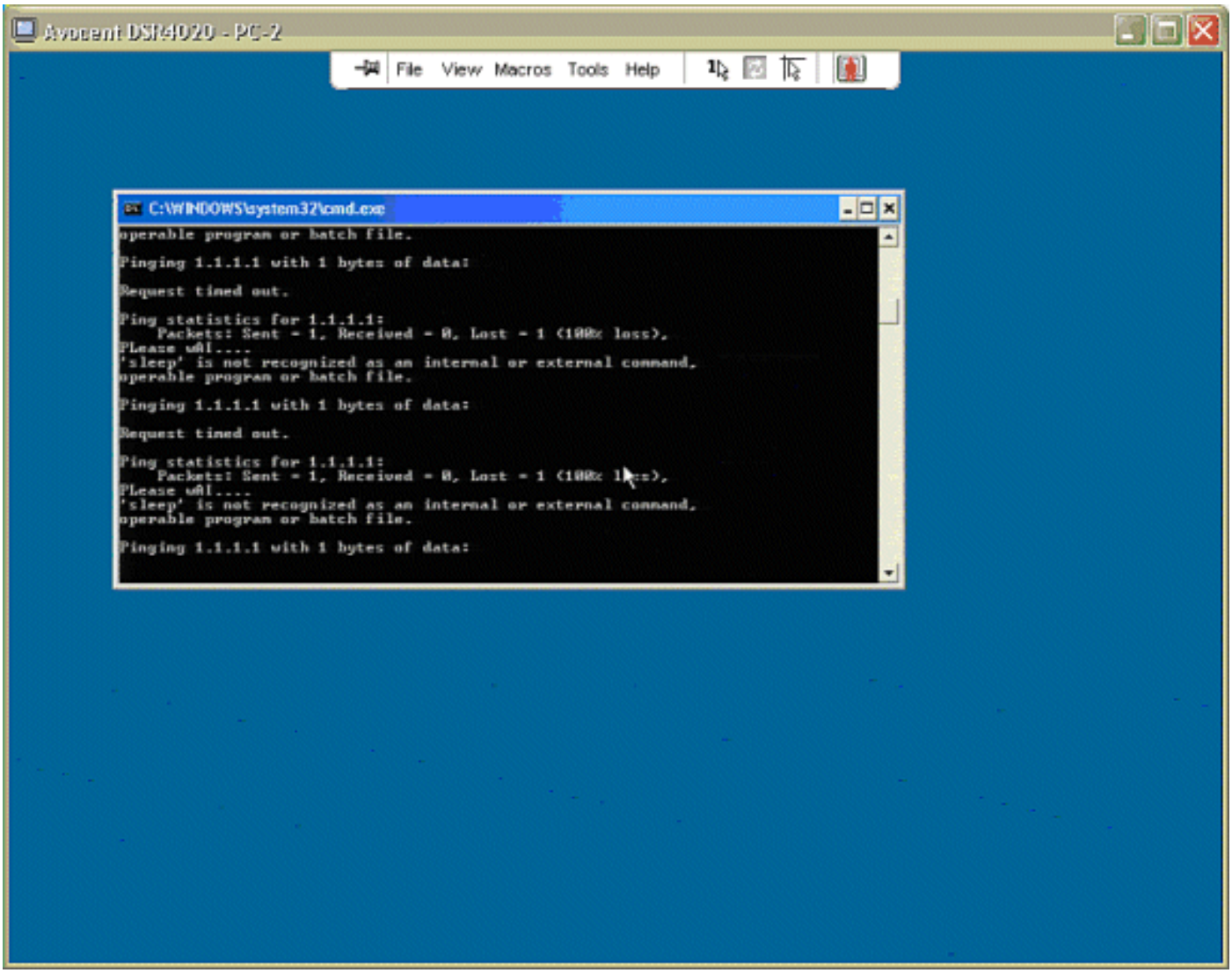
```
:CHECK
@echo off
echo Please wait....
ping -n 1 -l 1 10.10.10.10
if errorlevel 1 goto CHECK
@echo on

# Now the actual Logon script:

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

Примечание: Модифицируйте сценарий в соответствии с топологией сети.

Поскольку этот обходной путь прост, он хорошо работает, пока сценарии входа в систему выполнены асинхронно, и существует изменение no IP address, включенное в результате Внеполосных развертываний NAC или иначе.

Если сценарии выполнены синхронно, этот обходной путь отказывают, потому что агент NAC не загружается в память перед выполнением концов сценария входа в систему, и сценарий входа в систему никогда не завершает выполнение, потому что это ждет доступности сетевого ресурса, которая становится доступной только после того, как агент NAC аутентифицирует клиентский компьютер.

Этот снимок экрана показывает, что клиентский компьютер остается в этом состоянии бесконечного цикла из-за упомянутой причины.



Этот сценарий может также отказать в ситуации, куда сценарии выполнены асинхронно по соединению медленной глобальной сети (WAN), где сами сценарии могут требовать времени к загрузке, и NAC развернут в топологии OOB, где может быть настроено обновление IP. Обновление IP посреди выполнения сценария может потенциально сломать выполнение сценария. В таком как сценарий Cisco строго рекомендует выполнить сценарии синхронно так, чтобы процесс обновления IP не вмешивался в выполнение сценария. Этот сценарий изображает такую ситуацию.

Сценарий 2

Сценарии входа в систему Windows, выполненные от AD контроллера синхронно.

Синхронные сценарии рекомендуются в NAC развертывания OOB, где обновление IP имеет место.

Основная идея должна разделить функциональность исходного сценария входа в систему в два сценария.

Сценарий *один*, который выполняется как сценарий входа в систему, просто копирует второй сценарий к локальному компьютеру для выполнения в более позднее время, когда агент NAC аутентифицировался, и доступ к сети предоставляют.

Второй сценарий может вызвать программа запуска Windows автоматически при размещении второго сценария в загрузочный каталог пользователя, например:

Сценарий 1:

Сценарий входа в систему, выполняемый от AD, скопировал фактический сценарий, названный “mount.bat” к загрузочному каталогу пользователя для более позднего выполнения.

```
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"
```

Примечание: Модифицируйте сценарий для удовлетворения топологии сети.

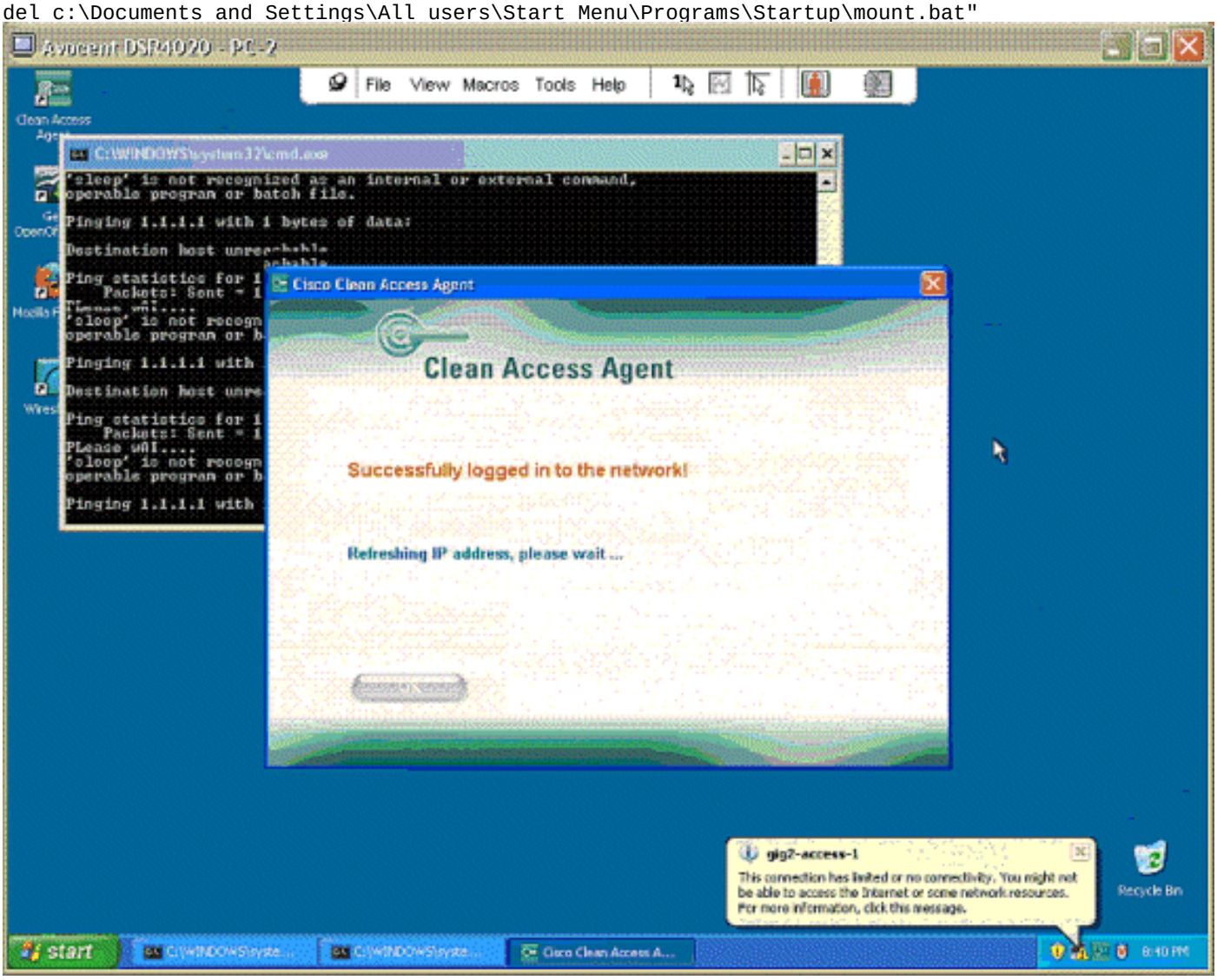
Примечание: Позвольте необходимому трафику течь через CAS в неаутентифицированной роли для разрешения входа в систему Домена Windows и копии сценариев входа в систему с AD на клиентский компьютер по сети для выполнения.

Сценарий 2

Вторичный сценарий, где реальное действие происходит, выполнен локально от системы и удален после выполнения из соображений безопасности.

```
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"
```



Этот снимок экрана изображает это второй сценарий, который выполняется, в фоновом режиме запущен от загрузочного каталога пользователя, и агент NAC делает обновление IP после того, как это аутентифицируется. Вторые петли сценария и ждут агента для завершения аутентификации и процесса обновления IP, прежде чем это завершит и подключит диски.

Устранение неполадок

Устранение проблем должно быть сделано на индивидуальной основе, однако перехватив пакеты от порта коммутатора, на котором связан клиентский компьютер, отличный способ запуститься. Это даст вам понимание о сетевых событиях и действиях.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация