Настройте WMI на контроллере домена Windows для CEM

Содержание

Введение

Этот документ описывает шаги для настройки инструментария управления Windows (WMI) на контроллере домена Windows для Менеджмента Cisco Energywise (CEM). WMI используется, чтобы удаленно обратиться к машинам окон к сбору данных и выполнить команды. Несмотря на то, что сценарий доступен, который выполняет все обязательные действия сразу, если контроллер домена используется для применения политики по доменным устройствам, рекомендуется изменить настройки в политике домена, поскольку устройства отвергли бы локальные изменения. Этот документ представляет шаги для настройки групповой политики на контроллере домена Windows для подготовки доменных устройств к опросу WMI.

> **Примечание:** Несмотря на то, что WMI доступен в Windows 2000 с SP2, приложение CEM не поддерживает Windows 2000. Для использования WMI приложение CEM требует Microsoft Windows XP Professional SP2 или позже.

Предварительные условия

Требования

Cisco рекомендует иметь доступ к контроллеру домена Windows, Системе управления Cisco Energywise и Удаленным машинам (активы).

Используемые компоненты

Сведения в этом документе основываются на среде CEMS 5.2, в которой разъём актива

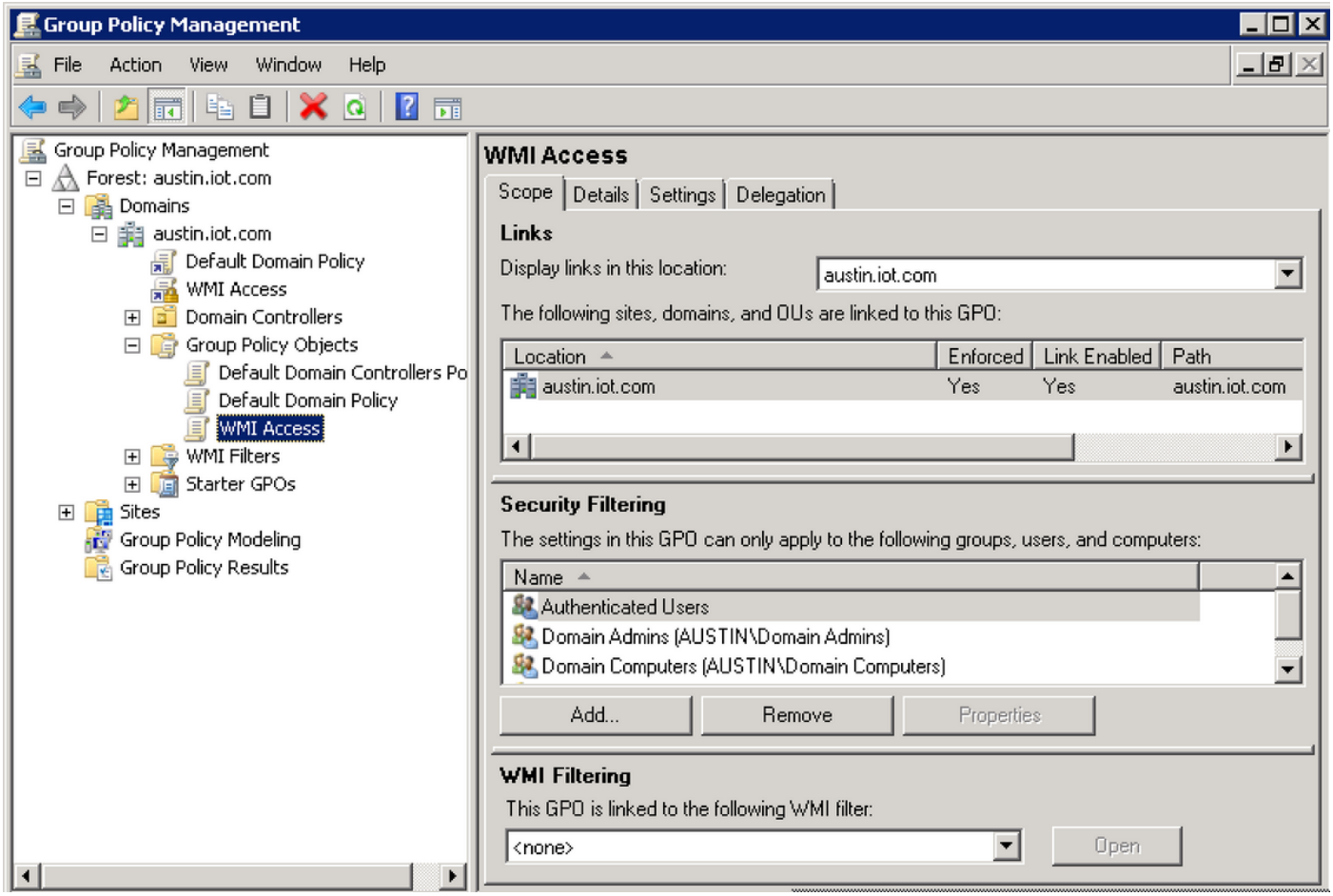
Active Directory (AD) используется для получения по запросу информации о WMI от удаленных устройств.

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.

Настройка

Создайте новый Объект Групповой политики

Первый шаг должен создать новый объект групповой политики. Объект групповой политики может быть создан на контроллере домена под менеджментом Групповой политики как показано:



Объект групповой политики

WMI: Настройте безопасность COM

Для выполнения запросов WMI удаленно определенные разрешения COM требуются. Выберите объект Групповой политики, созданный в предыдущем шаге, щелкните правой кнопкой и выберите**, редактируют** и затем переходят к этому местоположению:

Консоль управления групповой политики (GPMC)> Компьютер Опции Configuration\Windows Settings\Security Settings\Local Policies\Security

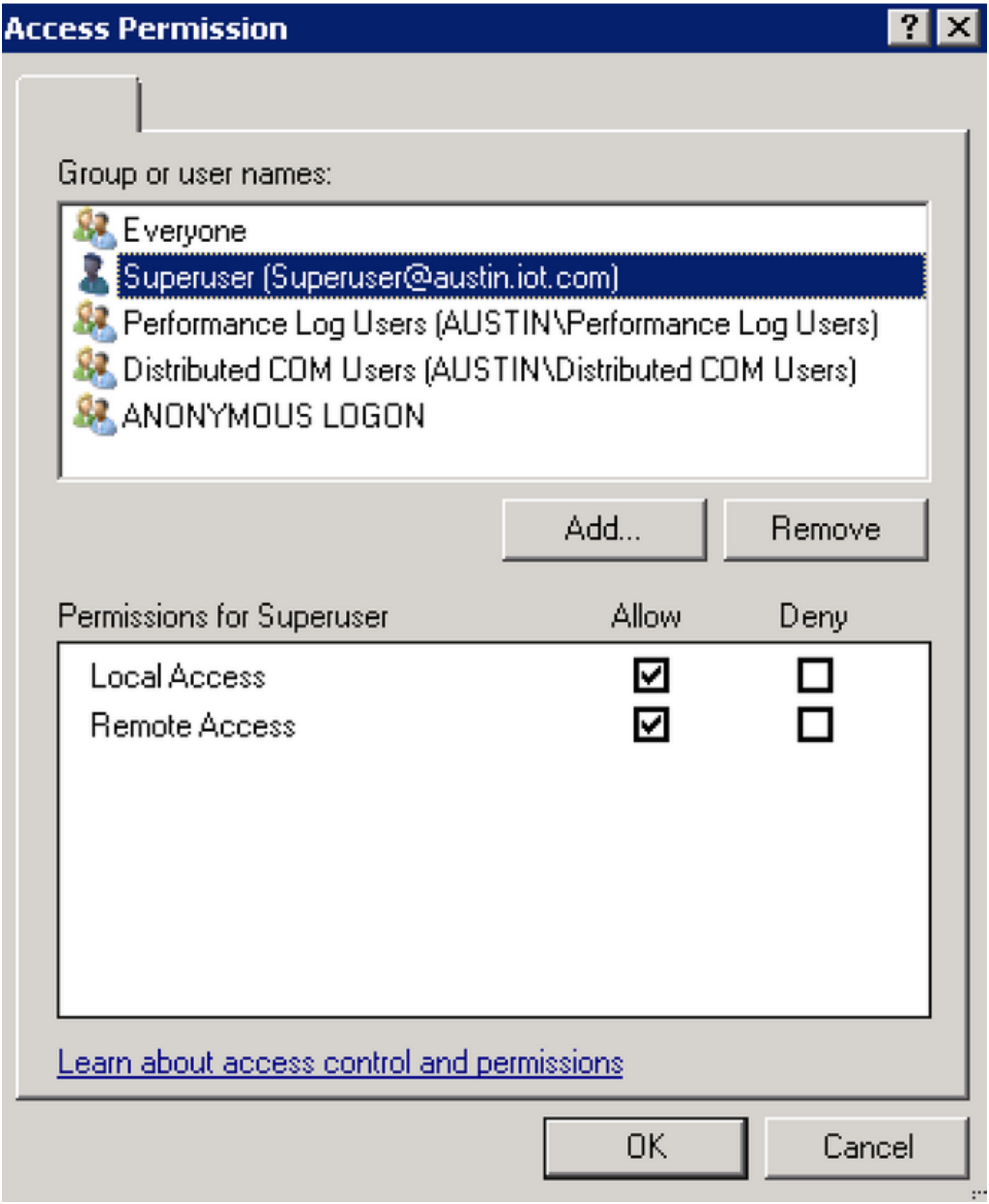
Найдите, что снимки экрана настраивают разрешения удаленного доступа для пользователя Администраторов для разрешений COM для:

DCOM: Ограничения доступа Машины в синтаксисе Языка определения дескриптора безопасности (SDDL)

DCOM: ограничения запуска машины на Языке определения дескриптора безопасности (SDDL)

Разрешения DCOM

Выберите **Define это значение политики** и щелкните **по Edit Security**. Предоставьте разрешения локального и удаленного доступа учетной записи, которую вы хотите использовать для WMI.



Разрешения доступа DCOM

Присвоение прав пользователя

Приложение CEM требует, чтобы и Резервные файлы и каталоги и файлы Восстановления и каталоги загрузили профиль пользователя, когда это пытается вызвать процесс. Это также требует завершения Силы от удаленной привилегии завершения позволить действию ПАУЭР_ОФФ работать.

Эти изменения должны быть внесены в параметрах настройки присвоения прав пользователя в этом Объекте Групповой политики. Эти права должны быть предоставлены учетной записи, используемой для WMI.

SeRemoteShutdownPrivilege - Вызовите завершение от удаленной системы

SeBackupPrivilege - Файлы резервного копирования и каталоги

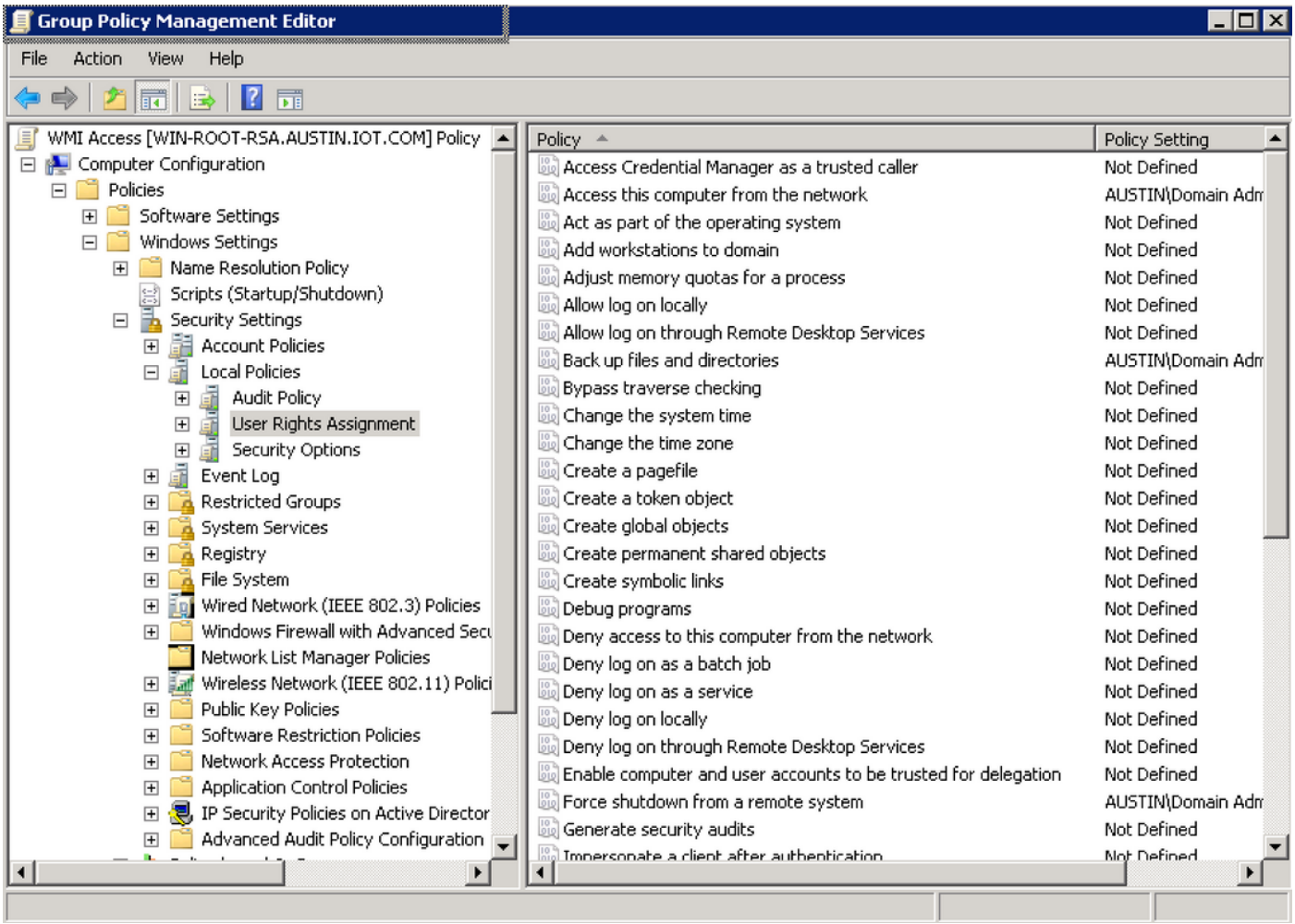
SeRestorePrivilege - Файлы восстановления и каталоги

SeNetworkLogonRight - Обратитесь к этому компьютеру от сети

SeSecurityPrivilege - Выберите контроль Manage и Журнал мониторинга безопасности

Эти параметры настройки могут быть настроены под этим путем:

Группа Консоль PolicyManagement (GPMC)> Компьютер Присвоение Прав Configuration\Windows Settings\Security Settings\Local Policies\User



Присвоение прав пользователя

Конфигурация межсетевого экрана

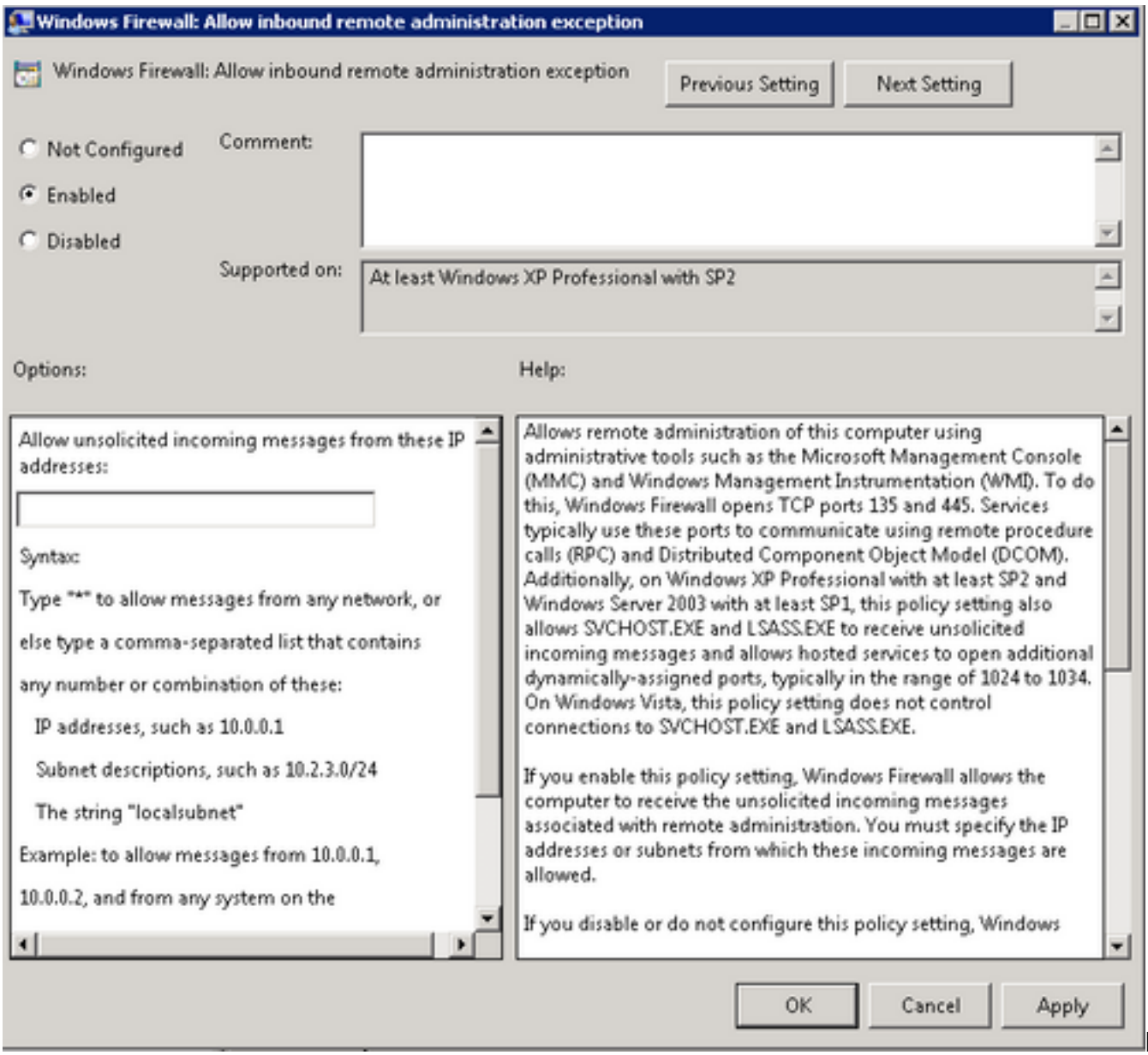
Для выполнения вызовов WMI к компьютеру порт RPC (TCP 135) должен быть доступным внешне. Это может быть сделано с использованием Редактора менеджмента Групповой политики, от дерева меню, перейти к **Конфигурации компьютера> Политика> Административные Шаблоны: Определения политики> Сеть> Сетевые подключения> Windows Firewall**

Выберите **Domain Profile** и дважды нажмите **Windows Firewall: Позвольте входящее исключение удаленного администрирования**. Windows Firewall: Позвольте, что появляется входящее окно исключения удаленного администрирования.

Нажмите **Enabled**.

Гарантируйте, что вы указываете, что IP-адрес в Позволяет незапрашиваемые входящие сообщения от этих IP-адресов поле.

Можно войти *, чтобы позволить сообщения от любой сети или иначе ввести список разделенных запятой значений, который содержит определенные IP-адреса или Подсети.



Конфигурация межсетевого экрана

Безопасность пространства имен WMI

Для включения доступа WMI к машине определенные разрешения WMI должны быть включены для используемой учетной записи. Эта конфигурация не может быть реализована через Групповую политику на контроллере домена Windows, это должно быть сделано на удаленных машинах с программным средством WmiSetNsSecurity.

Установите безопасность WMI и выполните команду (замените %account % учетной записью пользователя, вы хотите установить безопасность для) на программном средстве командной строки Windows.

```
WmiSetNsSecurity Root\CIMV2 -r %account%

WmiSetNsSecurity Root\CIMV2\power -r %account%

WmiSetNsSecurity Root\Default -r %account%

WmiSetNsSecurity Root\WMI -r %account%
```

Эта конфигурация должна быть выдвинута ко всем удаленным машинам, которые остаются. Этот шаг может также быть выполнен, когда вы создаете сценарий пакетной обработки и выдвигаете его через сценарий входа в систему admin или сценарий запуска машины под групповой политикой.

Системные разрешения файла конфигурации.

Приложение CEM требует полных полномочий обратиться к подпапке **Cisco** в папке Windows (например, C : \Windows\Cisco), чтобы сохранить и выполнить сценарии. Этот шаг должен быть выполнен на удаленных активах, и подробные данные конфигурации могут быть найдены в этой статье под разделом разрешений удаленной файловой системы.

https://обновление cem. cisco . com/download/files/5.0/docs/CEM_Online_Help/aa1808350.html

Настройте разрешения реестра

Для приложения CEM нужен доступ к реестру устройства, чтобы хранить различные данные. См. раздел, настраивающий разрешения реестра в этой статье.

https://обновление cem. cisco . com/download/files/5.0/docs/CEM_Online_Help/aa1808350.html

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Проверьте WMI, функционирующий запуском диагностики на одном из доменных устройств от GUI CEMS. Успешная конфигурация не должна показывать связанные ошибки WMI.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.