Публикуйте списки отозванных сертификатов для ISE на примере конфигурации Microsoft CA server

Содержание

Введение

Этот документ описывает конфигурацию Microsoft Certificate Authority (CA) сервер, который выполняет информационные сервисы интернета (IIS) для публикации обновлений Списка отозванных сертификатов (CRL). Это также объясняет, как настроить платформу Cisco Identity Services Engine (ISE) (версии 1.1 и позже) для получения обновлений для использования в проверке достоверности сертификата. ISE может быть настроен для получения CRL для различных корневых сертификатов CA, которые он использует в проверке достоверности сертификата.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Выпуск 1.1.2.145 платформы Cisco Identity Services Engine
- Microsoft Windows® Server® 2008 R2

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.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Конфигурации

Эти конфигурации используются в данном документе:

- Раздел 1. Создайте и настройте папку на CA для корпуса файлов CRL
- Раздел 2. Создайте узел в IIS для представления новой точки распространения списков CRL
- Раздел 3. Настройте Microsoft CA server для публикации файлов CRL в точке распространения
- Раздел 4. Проверьте, что Файл CRL Существует и Доступен через IIS
- Раздел 5. Настройте ISE для использования Новой точки распространения списков CRL

Раздел 1. Создайте и настройте папку на CA для корпуса файлов CRL

Первая задача состоит в том, чтобы настроить местоположение на сервере CA, чтобы хранить файлы CRL. По умолчанию Microsoft CA server публикует файлы в C:\Windows\system32\CertSrv\CertEnroll\. Вместо того, чтобы использовать эту системную папку, создайте новую папку для файлов.

1. На сервере IIS выберите местоположение на файловой системе и создайте новую папку. В данном примере создана папка C:\CRLDistribution.
2. Для CA для записи файлов CRL в новую папку должно быть включено совместное использование. Щелкните правой кнопкой мыши новую папку, выберите **Properties**, нажмите вкладку **Sharing**, и затем нажмите **Advanced Sharing**.
3. Для совместного использования папки проверьте **Ресурс общего доступа этот** флажок **папки** и затем добавьте знак доллара ($) до конца имени ресурса общего доступа в

поле Имени ресурса общего доступа для сокрытия ресурса общего доступа.
4. Нажмите **Permissions (1)**, **нажмите Add** (2), нажмите **Object Types (3)** и проверьте флажок (4) **Computers**.
5. Для возврата к Выбрать Users, Computers, Service Accounts или окну Groups, нажмите **OK**. Во Введении имен объекта для выбора поля введите имя компьютера сервера CA и нажмите **Check Names**. Если введенное имя допустимо, название обновляет и кажется подчеркнутым. **Нажмите кнопку OK.**
6. В Группе или поле имен пользователей, выберите компьютер CA. Проверка **Обеспечивает** Полное управление для предоставления полного доступа CA. **Нажмите кнопку OK.** Нажмите **OK** снова, чтобы закрыть окно Advanced Sharing и возвратиться к Окну свойств.
7. Чтобы позволить CA писать файлы CRL в новую папку, настройте соответствующие разрешения службы безопасности. Нажмите **Вкладку Безопасность** (1), нажмите **Edit (2)**, **нажмите Add** (3), нажмите **Object Types (4)** и проверьте флажок (5) **Computers**.
8. Во Введении имен объекта для выбора поля введите имя компьютера сервера CA и нажмите **Check Names**. Если введенное имя допустимо, название обновляет и кажется подчеркнутым. **Нажмите кнопку OK.**
9. Выберите компьютер CA в Группе или поле имен пользователей и затем проверьте**, Обеспечивают** Полное управление, чтобы допустить, что полный доступ к CA. Нажимает **OK** и затем нажимает**, Close to** выполняют задачу.

Раздел 2. Создайте узел в IIS для представления новой точки распространения списков CRL

Для ISE для доступа к файлам CRL сделайте каталог, который помещает файлы CRL, доступные через IIS.

1. На панели задач сервера IIS нажмите **Start**. Выберите **Administrative Tools> Internet Information Services (IIS) Manager**.
2. В левой панели (известный как Дерево консоли), разверните название сервера IIS и затем разверните **Узлы.**
3. Щелкните правой кнопкой мыши **Веб-сайт по умолчанию** и выберите **Add Virtual Directory**.
4. В поле Alias введите название сайта для CRL Distribution Point. В данном примере введен CRLD.
5. Нажмите замещающий знак (...) направо от поля Физического пути и переходят к папке, созданной в разделе 1. Выберите папку и нажмите **OK**. Нажмите **OK** для закрытия окна Add Virtual Directory.
6. Название сайта, введенное в шаг 4, должно быть выделено в левой панели. В противном случае выберите его теперь. В средней области дважды нажмите **Directory Browsing**.
7. В правой панели нажмите **Enable** к просмотру каталога enable.
8. В левой панели выберите название сайта снова. В средней области дважды нажмите **Configuration Editor**.
9. В выпадающем списке Раздела выберите **system.webServer/security/requestFiltering**. В allowDoubleEscaping выпадающем списке выберите **True**. В правой панели нажмите **Apply**.

Папка должна теперь быть доступной через IIS.

Раздел 3. Настройте Microsoft CA server для публикации файлов CRL в точке распространения

Теперь, когда новая папка была настроена для корпуса файлов CRL, и папка была представлена в IIS, настройте Microsoft CA server для публикации файлов CRL в новом местоположении.

1. На панели задач сервера CA нажмите **Start**. Выберите **Administrative Tools> Certificate Authority**.
2. В левой панели щелкните правой кнопкой мыши название CA. Выберите **Properties** и затем нажмите вкладку **Extensions**. Для добавления новой точки распространения списков CRL **нажмите Add**.
3. В поле Location введите путь к папке, созданной и совместно используемой в разделе 1. В примере в разделе 1, путь:`\\RTPAAA-DC1\CRLDistribution$\`
4. С заполненным полем Location выберите **<CaName>** из Переменного выпадающего списка и затем нажмите **Insert.**
5. От Переменного выпадающего списка выберите **<CRLNameSuffix>** и затем нажмите **Insert**.
6. В поле Location добавьте .crl до конца пути. В данном примере Местоположение:`\\RTPAAA-DC1\CRLDistribution$\<CaName><CRLNameSuffix>.crl`
7. Нажмите **OK** для возврата к вкладке Extensions. Проверьте **Публиковать CRL к этому флажку location (1)** и затем нажмите **OK (2)** для закрытия Окна свойств. Приглашение, кажется, для разрешений перезапускает Сервисы сертификации Active Directory. Нажмите **Yes (3)**.
8. В левой панели щелкните правой кнопкой мыши **Отозванные Сертификаты**. Выберите **All Tasks> Publish**. Гарантируйте, что Новый CRL выбран, и затем нажмите **OK.**

Microsoft CA server должен создать новый .crl файл в папке, созданной в разделе 1. Если новый файл CRL будет создан успешно то не будет никакого диалогового окна после того, как будет нажат OK. Если ошибка возвращена в отношении новой папки точки распространения, тщательно повторите каждый шаг в этот раздел.

Раздел 4. Проверьте, что Файл CRL Существует и Доступен через IIS

Проверьте, что новые файлы CRL существуют и что они доступны через IIS от другой рабочей станции перед началом этого раздела.

1. На сервере IIS откройте папку, созданную в разделе 1. Должен быть одиночный .crl файл, предоставляют форму <CANAME> .crl, где <CANAME> является названием сервера CA. В данном примере имя файла:`rtpaaa-CA.crl`
2. От рабочей станции в сети (идеально в той же сети как ISE основной узел Admin), откройте web-браузер и перейдите к http://<SERVER> / <CRLSITE>, где <SERVER> является именем сервера сервера IIS, настроенного в разделе 2, и <CRLSITE> название сайта, выбранное для точки распространения в разделе 2. В данном примере URL:`http://RTPAAA-DC1/CRLD`Показы индекса каталога, который включает файл, наблюдаемый в шаг 1.

Раздел 5. Настройте ISE для использования Новой точки распространения списков CRL

Прежде чем ISE настроен, чтобы получить CRL, определить интервал для публикации CRL. Стратегия определить этот интервал выходит за рамки этого документа. Потенциальные ценности (в Microsoft CA) составляют 1 час к 411 годам, включительно. Значение по умолчанию составляет 1 неделю. Как только соответствующий интервал для вашей среды был определен, установил интервал с этими инструкциями:

1. На панели задач сервера CA нажмите **Start**. Выберите **Administrative Tools> Certificate Authority**.
2. В левой панели расширьтесь, CA. Щелкают правой кнопкой мыши папку **Revoked Certificates** и выбирают **Properties.**
3. В полях interval публикации CRL введите нужное количество и выберите период времени. Нажмите **OK**, чтобы закрыть окно и применить изменение. В данном примере настроен интервал публикации 7 дней.Необходимо теперь подтвердить несколько значений регистра, которые помогут определять параметры настройки извлечения CRL в ISE.
4. Введите **certutil-getreg CA\Clock*** команда для подтверждения значения ClockSkew. Значение по умолчанию составляет 10 минут.Пример выходных данных:
```
Values:
    ClockSkewMinutes        REG_DWORS = a (10)
CertUtil: -getreg command completed successfully.
```
5. Введите **certutil-getreg КА\ЦРЛОВ*** команда, чтобы проверить, был ли вручную установлен CRLOverlapPeriod. По умолчанию значение CRLOverlapUnit 0, который указывает, что не было установлено никакое ручное значение. Если значение является значением кроме 0, сделайте запись значения и модулей.Пример выходных данных:
```
Values:
    CRLOverlapPeriod      REG_SZ = Hours
    CRLOverlapUnits        REG_DWORD = 0
CertUtil: -getreg command completed successfully.
```
6. Введите **certutil-getreg CA\CRLpe*** команда для проверки CRLPeriod, который был установлен в шаге 3.Пример выходных данных:
```
Values:
    CRLPeriod      REG_SZ = Days
    CRLUnits        REG_DWORD = 7
CertUtil: -getreg command completed successfully.
```
7. Вычислите Льготный период CRL следующим образом:Если CRLOverlapPeriod был установлен в шаге 5: НАЛОЖИТЕСЬ = CRLOverlapPeriod в минутах;Еще: НАЛОЖИТЕСЬ = (CRLPeriod / 10) в минутахЕсли НАЛОЖЕНИЕ> 720 тогда НАЛОЖЕНИЕ = 720Если НАЛОЖЕНИЕ <(1.5 * ClockSkewMinutes) тогда НАКЛАДЫВАЕТСЯ = (1.5 * ClockSkewMinutes)Если НАЛОЖЕНИЕ> CRLPeriod, в минутах тогда НАКЛАДЫВАЮТСЯ = CRLPeriod в минутахЛьготный период = 720 минут + 10 минут = 730 минутПример:
```
As stated above, CRLPeriod was set to 7 days, or 10248 minutes and
CRLOverlapPeriod was not set.

a. OVERLAP = (10248 / 10) = 1024.8 minutes
b. 1024.8 minutes is > 720 minutes : OVERLAP = 720 minutes
c. 720 minutes is NOT < 15 minutes : OVERLAP = 720 minutes
d. 720 minutes is NOT > 10248 minutes : OVERLAP = 720 minutes
e. Grace Period = 720 minutes + 10 minutes = 730 minutes
```
Вычисленный льготный период является периодом времени между тем, когда CA публикует следующий CRL и когда истекает текущий CRL. ISE должен быть настроен для получения CRL соответственно.
8. Войдите к основному узлу Admin и выберите **Administration> System> Certificates**. В левой панели выберите **Certificate Store**.

9. Проверьте флажок Certificate Store рядом с сертификатом CA, для которого вы намереваетесь настроить CRL. **Нажмите Edit.**
10. Около нижней части окна проверьте флажок **Download CRL**.
11. В поле CRL Distribution URL введите путь к CRL Distribution Point, который включает .crl файл, созданный в разделе 2. В данном примере URL:`http://RTPAAA-DC1/CRLD/rtpaaa-ca.crl`
12. ISE может быть настроен для получения CRL через определенные промежутки времени или на основе истечения (который, в целом, является также регулярным интервалом). То, когда CRL публикует интервал, статично, более своевременные обновления CRL получены, когда используется последняя опция. Нажмите кнопку с зависимой фиксацией **Automatically**.
13. Установите значение для извлечения к значению меньше, чем льготный период, вычисленный в шаге 7. Если заданное значение более длинно, чем льготный период, ISE проверяет CRL Distribution Point, прежде чем CA публиковал следующий CRL. В данном примере льготный период вычислен, чтобы быть 730 минутами, или 12 часами и 10 минутами. Значение 10 часов будет использоваться для извлечения.
14. Установите интервал между попытками как соответствующий вашей среде. Если ISE не может получить CRL в заданном интервале в предыдущем шаге, это повторит в этом более коротком интервале.
15. Проверьте **Обходную Проверку CRL, если CRL не является** флажком **Received**, чтобы позволить основанной на сертификате аутентификации обычно продолжаться (и без проверки CRL), если ISE был неспособен получить CRL для этого CA в его последней попытке загрузки. Если этот флажок не будет проверен, то вся основанная на сертификате аутентификация с сертификатами, выполненными этим CA, откажет, если не может быть получен CRL.
16. Проверьте**, что Игнорировать тот CRL еще не является допустимым или** флажком **с истекшим сроком**, чтобы позволить ISE использовать истекший (или еще не допустимый) файлы CRL, как будто они были допустимы. Если этот флажок не проверен, ISE полагает, что CRL недопустим до их Даты вступления в силу и после их Следующие Разы. Нажмите **Save** для завершения конфигурации.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

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

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация