ГЛАВА 14

Безопасность при пересылке данных

В ЭТОЙ ГЛАВЕ...

- Введение в безопасность при пересылке данных в Windows Server 2012
- Развертывание инфраструктуры открытых ключей с помощью Windows Server 2012
- Служба сертификации Active Directory в Windows Server 2012
- Служба управления правами AD CS
- Шифрование IPsec в Windows Server 2012

В прошлом сети представляли собой замкнутые среды, изолированные друг от друга и доступные только во внутренних сегментах. Обмен данными был ограничен отдельными сетями и редко выходил за их пределы. Со временем, когда появилась необходимость обмена информацией между этими сетями, были установлены соединения для передачи данных из одной сети в другую. Однако вначале передача этой информации была незащищенной, и в случае перехвата информация легко могла быть прочитана посторонними. Поэтому необходимость защиты такой информации стала одним из основных приоритетов и жизненно важным компонентом сетевой инфраструктуры.

Со временем была разработана как технология защиты этой информации, так и технология взлома и получения несанкционированного доступа к данным. Несмотря на эту опасность, продуманное проектирование и конфигурирование безопасных транспортных решений с помощью Windows Server 2012 способно существенно повысить безопасность сети. Во многих случаях применение таких решений совершенно обязательно, особенно для данных, которые пересылаются через неконтролируемые сегменты сети наподобие Интернета.

В этой главе основное внимание уделено существующим механизмам защиты и шифрования информации, пересылаемой между компьютерами сети. Особое внимание уделено новым и усовершенствованным средствам безопасности транспортного уровня в Windows Server 2012, с разбором конкретных ситуаций. Более подробно рассмотрены и проиллюстрированы возможности IPsec, инфраструктуры общедоступных ключей (PKI) и виртуальных частных сетей (VPN). Кроме того, здесь описаны специфические средства — служба сертификации Active Directory (Active Directory Certificate Services — AD CS) и служба управления правами Active Directory (Active Directory Rights Management Services — AD RMS) Windows Server 2012.

Введение в безопасность при передаче данных в Windows Server 2012

Защита данных при их передаче означает предотвращение несанкционированного доступа к данным в процессе обмена информацией между клиентом и сервером или между серверами. В дополнение к физической и сетевой защите, реализация безопасности на транспортном уровне является еще одним уровнем защиты, важным для проектирования и создания защищенной сетевой среды.

Необходимость безопасности транспортного уровня

В связи с природой взаимосвязанных сетей вся информация должна пересылаться в формате, доступном для перехвата любым клиентом в каком-либо физическом сегменте сети. Данные должны быть организованы в однотипные структуры, чтобы сервер-адресат мог преобразовать их в соответствующую информацию. Однако эта простота порождает и проблемы безопасности, поскольку перехваченные данные при попадании в чужие руки легко могут быть использованы в неблаговидных целях.

Необходимость обеспечения неприменимости информации в случае ее перехвата лежит в основе всех методов шифрования на транспортном уровне. Обе противоборствующие стороны предпринимают значительные усилия: специалисты по безопасности разрабатывают схемы шифрования и маскирования данных, а хакеры и другие специалисты по безопасности разрабатывают способы успешной расшифровки и перехвата данных. К счастью, технология шифрования разработана уже до такой степени, что правильно сконфигурированные среды могут достаточно успешно защитить свои данные при использовании надлежащих средств. Windows Server 2012 предоставляет большое количество средств безопасности транспортного уровня, и для надежной защиты важных данных рекомендуется использовать одну или несколько из этих технологий.

На современных предприятиях и необходимых для их работы технологиях существуют различные группы пользователей и прочие сущности, которые взаимодействуют с системами и надежны в разной степени. Такая разнообразная среда усложняет защиту данных в сети, и необходим дополнительный слой гибких и динамичных инструментов, которые могут защищать будет с учетом их внутреннего содержимого и внешнего контекста.

Обеспечение безопасности с помощью многоуровневой защиты

Поскольку даже наиболее защищенные инфраструктуры имеют уязвимые места, рекомендуется применять многоуровневую защиту особо важных сетевых данных. В случае взлома одного уровня защиты взломщику для получения доступа к важным данным придется преодолеть второй или даже третий уровень системы безопасности. Например, сложная, "не поддающаяся взлому" 256-битовая схема шифрования оказывается бесполезной, если взломщик просто выведает пароль или PIN-код у законного пользователя с помощью социотехнических приемов. Дополнение системы безопасности вторым или третьим уровнем сделает взлом всех уровней значительно более сложной задачей.

Средства защиты данных при их передаче в Windows Server 2012 используют несколько уровней аутентификации, шифрования и авторизации для повышения уровня безопасности сети. Возможности конфигурирования, предоставляемые Windows Server 2012, позволяют установить несколько уровней безопасности транспортного уровня, обеспечивающих защиту конфиденциальности и целостности данных.

НА ЗАМЕТКУ

Безопасность с несколькими уровнями защиты — концепция не новая, она заимствована из военной стратегии, которая справедливо утверждает, что несколько линий обороны более эффективны, нежели одна.

Понятие шифрования

В упрощенной формулировке шифрование — это процесс такого искажения осмысленной информации, чтобы она стала бессмысленной для любого, кроме пользователя или компьютера, для которого она предназначена. Если не слишком вникать в нюансы конкретных методов шифрования данных, то важно лишь понять, что правильное шифрование позволяет передавать данные по незащищенным сетям наподобие Интернета и преобразовывать их в пригодную для использования форму только в пункте назначения. В случае перехвата пакетов надежно зашифрованной информации они окажутся бесполезными, поскольку информация искажена до неузнаваемости. Все описанные в этой главе механизмы используют ту или иную форму шифрования для защиты содержимого пересылаемых данных.

Развертывание инфраструктуры открытых ключей с помощью Windows Server 2012

Понятие инфраструктуры открытых ключей (Public Key Infrastructure — PKI) употребляется везде и вовсю, но нечасто сопровождается подробным объяснением. Если говорить кратко, инфраструктура открытых ключей — это совокупность цифровых сертификатов, бюро регистрации и центров сертификации, которые проверяют подлинность каждого участника обмена зашифрованными сообщениями. По сути, сама по себе инфраструктура открытых ключей — просто концепция, которая определяет механизмы защиты данных от чтения при их передаче и проверки подлинности пользователя, передавшего эти данные. Реализации PKI широко распространены и становятся исключительно важным компонентом современных реализаций сетей. Как описано в последующих разделах, Windows Server 2012 полностью поддерживает развертывание нескольких конфигураций PKI.

Реализации PKI могут быть как простыми, так и сложными, а некоторые применяют массивы смарт-карт (или другие способы двухфакторной аутентификации) и сертификаты для проверки подлинности всех пользователей с высокой степенью достоверности. Поэтому каждая организация должна разобраться в возможностях PKI и выбрать нужную реализацию.

Сравнение шифрования секретным ключом и шифрования открытым ключом

Технологии шифрования можно разделить на симметричные и асимметричные. Симметричное шифрование требует, чтобы каждая сторона схемы шифрования владела копией секретного ключа (private key), используемого для шифрования и расшифровки информации, пересылаемой между сторонами. Проблема с шифрованием секретным ключом состоит в том, что секретный ключ нужно как-то передать второй стороне, чтобы он не был перехвачен и использован для расшифровки информации. Кроме того, каждая уникальная пара сторон должна использовать отдельный уникальный ключ для защиты данных. Результирующая сложность управления ключами является основным препятствием для реализации шифрования секретным ключом.

Шифрование открытым ключом (public key), или асимметричное шифрование, использует комбинацию двух ключей, которые математически связаны друг с другом. Первый ключ, являющий секретным ключом, хранится в строгой тайне и используется для цифровой подписи или расшифровки информации. Второй — открытый — ключ может использоваться для проверки цифровой подписи или шифрования информации. Целостность открытого ключа обеспечивается сертификатами, которые подробно описаны в последующих разделах этой главы. Асимметричный подход к шифрованию значительно облегчает управление ключами, т.к. открытый ключ не нужно защищать, и у каждого пользователя имеется лишь один секретный ключ. Правда, это упрощение управления достигается за счет снижения производительности из-за усложнения математических операций.

Многие реализации шифрования и асимметричных ключей (включая и большинство реализаций PKI) используют асимметричный процесс выбора секретного ключа, который затем применяется для защиты данных. При этом сочетаются преимущества обоих подходов.

Знакомство с цифровыми сертификатами

Сертификат (certificate) представляет собой цифровой документ, который выдается доверяемым центром (централизованным, внутренним или локальным) и используется им для подтверждения подлинности пользователя. Доверяемые центры сертификации, такие как VeriSign, широко используются в Интернете, чтобы, например, подтверждать, что программное обеспечение Microsoft действительно разработано компанией Microsoft, а не служит маскировкой какого-либо вируса.

Сертификаты применяются для выполнения нескольких функций, которые перечислены ниже.

- Защита электронной почты.
- Аутентификация во всемирной Сети.
- Защита данных в Интернете (IPsec).
- Подписание кода.
- Создание иерархий сертификации.

Все эти функции сводятся, в конечном счете, либо к шифрованию данных (при защите почтовых сообщений или веб-паролей и контента), либо к цифровой подписи данных для гарантии целостности и подлинности (при подписании кода или почтовых сообщений).

Сертификаты подписываются с помощью информации из открытого ключа субъекта и идентификационной информации — имя, адрес электронной почты и тому подобные сведения, — а также цифровой подписи организации, выпустившей сертификат, которая называется центром сертификации (Certificate Authority — CA). Если оба пользователя или компьютера доверяют одному и тому же центру сертификации, который выпустил сертификаты, они могут доверять и друг другу.

Служба сертификации Active Directory в Windows Server 2012

Windows Server 2012 содержит встроенную технологию CA, называемую службой сертификации Active Directory (Active Directory Certificate Services — AD CS). Первый вариант AD CS появился в Windows Server 2008, а раньше эта технология называлась просто службой сертификации (Certificate Services). AD CS может использоваться для создания сертификатов и последующего управления ими и отвечает за обеспечение их подлинности, отзыв и сроки годности. Зачастую AD CS в Windows Server 2012 используется без особой необходимости проверки сертификатов организации какой-либо независимой стороной. Поэтому если сертификаты требуются только для участников внутри организации, часто применяется развертывание внутреннего CA для нужд внутренних пользователей и систем. Широко используются и сторонние центры сертификации наподобие VeriSign, но они требуют дополнительного вложения средств.

НА ЗАМЕТКУ

Хотя в новом названии службы сертификации Windows упоминается Active Directory, следует понимать, что для работы AD CS совсем не требуется интеграция с существующей средой леса доменной службы Active Directory (Active Directory Domain Services (AD DS)). Обычно это все же так, но важно понимать, что AD CS не зависит от структуры леса AD DS. Более подробно об AD DS можно прочитать в главах 4 и 5.

В Windows Server 2012 добавлено несколько новых возможностей AD CS.

- **Веб-служба развертывания сертификатов и веб-служба политики развертывания сертификатов.** Это наиболее значительное усовершенствование, которое появилось в Windows Server 2008 R2, позволяет развертывать сертификаты непосредственно по протоколу HTTP и дает возможность клиентам, не принадлежащим домену или подключенным к Интернету, обращаться к серверу CA и запрашивать сертификаты.
- **Автоматическое обновление серверов, не входящих в домен.** В рамках расширения поддержки не членов домена веб-служба политик развертывания сертификатов (Certificate Enrollment Policy Web Service) в Windows Server 2012 теперь поддерживает автоматическое обновление.
- **Поддержка Windows Server 2012 Core Edition.** Теперь AD CS поддерживается на серверах, работающих в режиме Core Edition.
- **Поддержка развертывания сертификатов между лесами.** Платформа, появившаяся в Windows Server 2008 R2, позволяет консолидировать CA между несколькими лесами.

Обзор ролей центров сертификации в AD CS

AD CS для Windows Server 2012 можно установить в виде центра сертификации одного из перечисленных ниже типов.

- **Головной центр сертификации предприятия.** Головной CA предприятия является наиболее доверяемым CA в организации и должен быть установлен раньше всех остальных CA. Все остальные CA являются подчиненными по отношению к головному CA предприятия. Защите этого CA следует уделить самое пристальное внимание, т.к. компрометация CA предприятия означает компрометацию всей цепочки центров сертификации.
- **Подчиненный центр сертификации предприятия.** Подчиненный CA предприятия должен получить сертификат от головного CA предприятия, но после этого может выдавать сертификаты всем пользователям и компьютерам предприятия. Часто CA этого типа используются для создания масштабируемого набора CA с высокой степенью готовность и защиты головного CA предприятия.
- **Самостоятельный головной центр сертификации.** Самостоятельный головной CA служит вершиной иерархии, не связанной с информацией домена предприятия. В специальных случаях можно создать несколько самостоятельных CA. Самостоятельный головной CA часто используется в качестве корневого для других подчиненных CA предприятия — для повышения безопасности среды, т.к. самостоятельный головной центр можно вывести в автономный режим. То есть головной центр конфигурируется как самостоятельный, а подчиненные CA, интегрированные в домен предприятия, установлены в доменах леса, чтобы обеспечить автоматическое развертывание в масштабе предприятия.
- **Самостоятельный подчиненный центр сертификации.** Самостоятельные подчиненные CA получают свои сертификаты от самостоятельного головного CA, и затем могут использоваться для распространения сертификатов пользователям и компьютерам, связанным с этим самостоятельным CA.

ВНИМАНИЕ!

Принятие решений по структуре AD CS — задача нетривиальная, и к ней не следует подходить легкомысленно. Простое помещение AD CS на сервер в качестве CA предприятия и ее запуск — далеко не лучший подход с точки зрения безопасности, поскольку компрометация такого сервера может обернуться катастрофой. Поэтому, прежде чем приступить к развертыванию AD CS, важно тщательно обдумать ее структуру. Например, одной из лучших тактик является развертывание самостоятельного головного CA, затем нескольких подчиненных CA в предприятии, а затем физическое отключение самостоятельного головного CA и помещение в очень защищенное место, чтобы включать его, только если требуется обновление сертификатов подчиненных CA.

Описание служб ролей в AD CS

AD CS состоит из нескольких служб ролей, который выполняют для клиентов различные задачи. При необходимости одну или несколько этих ролей можно установить на сервере. Эти службы кратко описаны ниже.

- **Центр сертификации.** Данная служба устанавливает базовый компонент CA, позволяющий серверу издавать и отзывать сертификатами для клиентов и управлять ими. Эту роль можно установить на нескольких серверах в цепочке одного и того же головного CA.
- **Веб-включение центра сертификации.** Данная служба управляет распространением сертификатов клиентам через Интернет. Для ее работы нужно, чтобы на сервере была установлена служба информации Интернета (Internet Information Services — IIS).

- **Онлайновый ответчик.** Данная служба отвечает на запросы индивидуальных клиентов по поводу проверки конкретных сертификатов. Она применяется для сложных или больших сетей, которые должны выдерживать интенсивные периоды активности по отзыву или загрузку больших списков отзывов сертификатов (Certificate Revocation List — CRL).
- **Веб-служба развертывания сертификатов.** Эта новая служба позволяет пользователям и компьютерам выполнять удаленное развертывание сертификатов или развертывание из систем, не включенных в домен, по протоколу HTTP.
- **Веб-служба политики развертывания сертификатов.** Эта служба работает с соответствующей веб-службой развертывания сертификатов, но предоставляет информацию о политике, а не сертификаты.
- **Служба включения сетевых устройств.** Данная служба упрощает получение сертификатов сетевыми устройствами наподобие маршрутизаторов.

Установка AD CS

Для установки AD CS в Windows Server 2012 вначале нужно выбрать сервер, который будет работать в качестве головного CA. Не забывайте о настоятельных рекомендациях, что это должен быть выделенный сервер, защищенный физически и выключенный бо́льшую часть времени для обеспечения целостности цепочки сертификатов. Обратите внимание на важный момент: CA предприятия нельзя отключать, а вот самостоятельный головной центр с подчиненными CA предприятия отключить можно. Если выбран вариант самостоятельного головного центра с подчиненными CA предприятия, то вначале необходимо создать и сконфигурировать головной CA, а затем создать подчиненные CA предприятия.

В несложных ситуациях можно ограничиться головным CA предприятия, хотя во многих случаях небольшие предприятия также хотят иметь самостоятельный головной центр и подчиненные CA предприятия. Если все-таки принят вариант с одним головным CA предприятия, то для создания сервера сертификации можно выполнить следующие шаги:

ВНИМАНИЕ!

После установки AD CS на сервере имя и доменный статус этого сервера изменять нельзя. Кроме того, нельзя изменять имя сервера, пока он выполняет функции CA.

1. Откройте диспетчер серверов (Server Manager).
2. В меню Manage (Управление) выберите пункт Add Roles and Features (Добавление ролей и компонентов).
3. На странице Before You Begin (Первоначальные сведения) щелкните на кнопке Next (Далее).
4. Согласитесь с предложенным по умолчанию типом установки и щелкните на кнопке Next.
5. Выберите из списка нужный сервер AD CS и щелкните на кнопке Next.
6. На странице Select Server Roles (Выбор серверных ролей) отметьте флажок Active Directory Certificate Services (Служба сертификации Active Directory), а затем щелкните на кнопке Next.
7. Согласитесь со списком компонентов, щелкнув на кнопке Next.
8. На странице Introduction (Введение) просмотрите информацию об AD CS и щелкните на кнопке Next.

9. На странице Select Role Services (Выбор служб ролей), показанной на рис. 14.1, укажите нужные службы ролей. Для базовой установки необходима только роль Certificate Authority (Центр сертификации). Щелкните на кнопке Next.

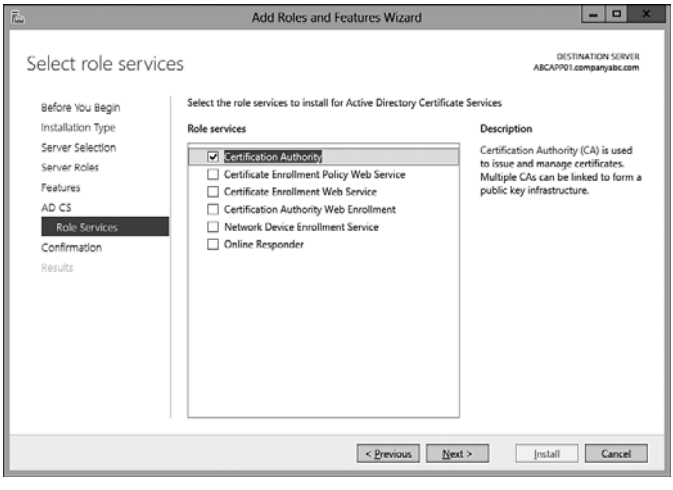

Рис. 14.1. *Установка AD CS*

10. Щелкните на кнопке Install (Установить).
11. После завершения установки щелкните на ссылке Configure Active Directory Certificate Services on the Destination Server (Настроить службу сертификации Active Directory на целевом сервере).
12. При необходимости щелкните на кнопке Change (Изменить), чтобы изменить входные полномочия, и щелкните на кнопке Next.
13. Выберите службу роли центра сертификации, которую нужно настроить, и щелкните на кнопке Next.
14. На следующей странице укажите, нужно ли устанавливать центр сертификации предприятия (Enterprise CA), интегрированный с AD CS, или самостоятельный центр сертификации (Stand-alone CA). Щелкните на кнопке Next.
15. На странице Specify CA Type (Укажите тип CA), показанной на рис. 14.2, выберите нужный тип CA. В данном случае мы устанавливаем на сервер головной CA (Root CA). Щелкните на кнопке Next.
16. На следующей странице Private Key (Секретный ключ) можно указать либо создание нового секретного ключа с нуля, либо использование существующего ключа из предыдущей реализации CA. В данном примере мы создаем новый ключ. Щелкните на кнопке Next.
17. На странице Configure Cryptography for CA (Настройка криптографии для CA) введите параметры шифрования секретным ключом, как показано на рис. 14.3. Обычно вполне годятся значения, предложенные по умолчанию, но бывают случаи, когда нужно изменить CSP, длину ключа и другие настройки. Щелкните на кнопке Next.
18. Выберите имя, которое будет использоваться для идентификации данного CA. Учтите, что это имя будет фигурировать на всех сертификатах, выпущенных данным CA. В нашем примере мы ввели имя `CompanyABC-CorpCA`. Щелкните на кнопке Next.

19. Укажите срок годности сертификата, который будет установлен на данном сервере CA. Если это головной CA, сервер должен будет повторно выпустить цепочку сертификатов после истечения срока годности. В данном примере мы выбрали 5-летний срок годности, хотя во многих реальных ситуациях для головного центра создается 20-летний CA. Щелкните на кнопке Next.
20. Укажите место хранения базы данных сертификатов и местоположения для хранения журналов, а затем щелкните на кнопке Next.
21. На странице подтверждения (рис. 14.4) просмотрите параметры предстоящей установки и щелкните на кнопке Configure (Настроить).
22. После завершения работы мастера щелкните на кнопке Close (Закрыть).

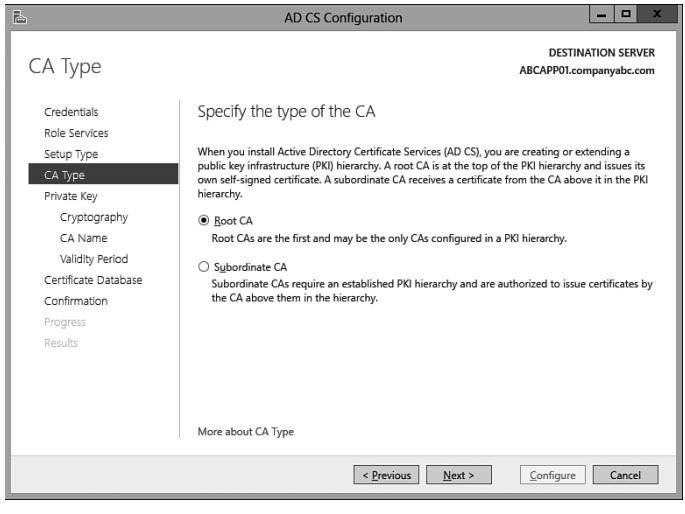

Рис. 14.2. *Указание типа CA*

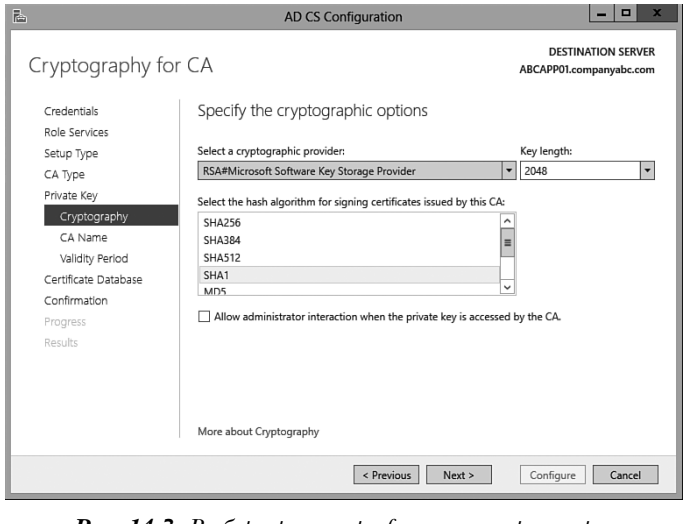

Рис. 14.3. *Выбор криптографических параметров*

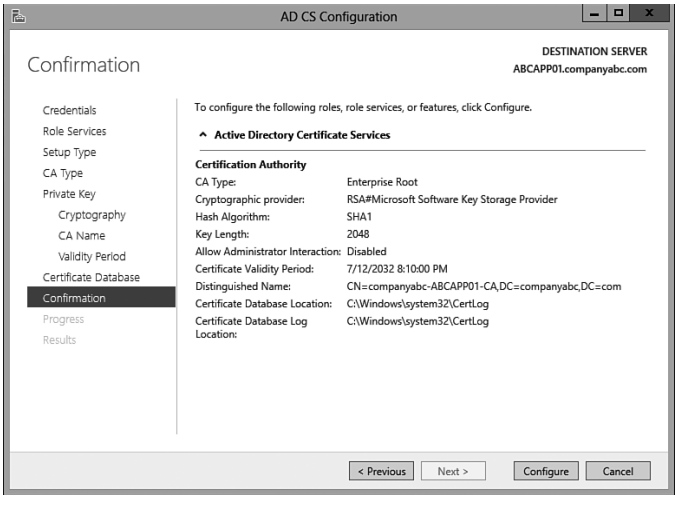

Рис. 14.4. *Просмотр параметров установки AD CS*

После установки AD CS можно установить дополнительные (подчиненные) CA и выполнять администрирование PKI с консоли центра сертификации. для этого в диспетчере серверов выберите пункт меню Tools⇨Certification Authority (Сервис⇨Центр сертификации).

Настройка автоматического развертывания

После установки CA можно приступить к выпуску сертификатов. Сертификаты для прикладных серверов — веб-серверов, серверов Microsoft Exchange, серверов Microsoft Lync и т.д. — часто развертываются администраторами. Но в более крупных развертываниях могут быть сотни, тысячи и даже больше сертификатов, поэтому нужен процесс автоматического развертывания. Такой автоматизированный процесс предусмотрен в Windows Server 2012, как для членов доменов, так и для не входящих в домен компьютеров.

Сейчас мы рассмотрим пример, демонстрирующий развертывание сертификата компьютеров для всех членов домена. Для этого будут выполнены следующие высокоуровневые шаги.

1. Назначение шаблонных прав доступа.
2. Активизация шаблона в CA.
3. Настройка объекта групповой политики (GPO) на автоматическое развертывание членов домена.
4. Настройка автоматического развертывания для не членов домена.

Для назначения нужных шаблонных прав доступа выполните перечисленные ниже шаги.

1. Щелкните на кнопке Start (Пуск), чтобы открыть экран Metro.
2. Введите текст mmc, чтобы открыть поле поиска и найти исполняемый файл mmc.
3. Запустите утилиту mmc из результата поиска.
4. Выберите пункт меню File⇨Add/Remove Snap-In (Файл⇨Добавление или удаление оснастки).
5. Добавьте оснастку Certificate Templates (Шаблоны сертификатов) и щелкните на кнопке OK.

6. Выберите корневую папку Certificate Templates.
7. В панели результатов щелкните правой кнопкой мыши на шаблоне Workstation Authentication и выберите в контекстном меню пункт Duplicate Template (Создать копию шаблона). Введите имя для создаваемого шаблона.
8. Перейдите на вкладку Security (Безопасность).
9. Выберите элемент Domain Computers (Компьютеры домена) и отметьте флажок Auto-Enroll (Авторазвертывание) в столбце Allow (Разрешить), как показано на рис. 14.5.
10. Щелкните на кнопке OK.

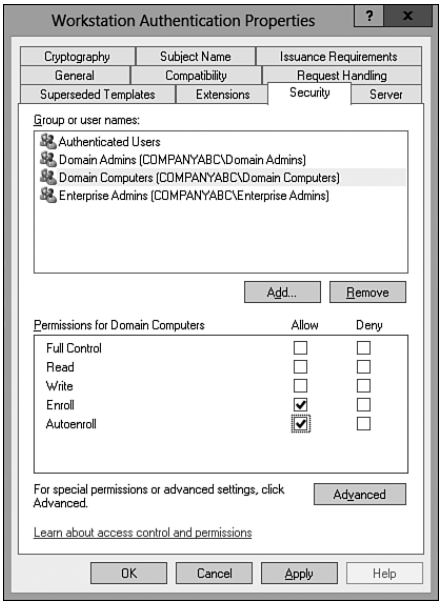

Рис. 14.5. *Настройка прав доступа шаблона для авторазвертывания*

Чтобы активиизровать шаблон в CA, выполните на сервере AD CS следующие шаги.

1. Откройте диспетчер серверов (Server Manager).
2. Выберите пункт меню Tools⇨Certification Authority (Сервис⇨Центр сертификации).
3. Раскройте папку головного центра.
4. Щелкните правой кнопкой мыши на папке Certificates Templates (Шаблоны сертификатов) и выберите в контекстном меню пункт New⇨Certificate Template (Создать⇨Шаблон сертификата).
5. Выберите только что созданную копию шаблона Workstation Authentication (Аутентификация рабочей станции) и щелкните на кнопке OK.

Для настройки GPO на автоматическое развертывание выполните на контроллере домена следующие шаги.

1. Откройте диспетчер серверов (Server Manager).
2. Выберите пункт меню Tools⇨Group Policy Management (Сервис⇨Управление групповыми политиками).
3. Раскройте папку леса Domains (Домены), в которой находятся папки с именами доменов.
4. Щелкните правой кнопкой мыши на нужном домене и выберите в контекстном меню пункт Create a GPO in This Domain, and Link It Here (Создать GPO в этом домене и привязать его к нему).
5. Введите имя для нового GPO — например, Computer certificate auto-enrollment (Авторазвертывание сертификатов) — и щелкните на кнопке OK.
6. Щелкните правой кнопкой мыши на только что созданном GPO и выберите в контекстном меню пункт Edit (Правка).
7. Разверните узел Computer Configuration \ Policies \ Windows Settings \ Security Settings \ Public Key Policies (Конфигурация компьютера \ Политики \ Параметры Windows \ Настройки безопасности \ Политики открытого ключа).

8. В панели результатов дважды щелкните на элементе Certificate Services Client — Auto-Enrollment (Клиент службы сертификатов — Авторазвертывание).
9. Смените значение параметра Configuration Model (Модель настройки) на Enabled (Включено).
10. Отметьте два флажка: Renew Expired Certificates, Update Pending Certificates, and Remove Revoked Certificates (Обновлять устаревшие сертификаты, обновлять ожидающие сертификаты и удалять отозванные сертификаты) и Update Certificates That Use Certificate Templates (Обновить сертификаты, использующие шаблоны сертификатов). Затем щелкните на кнопке OK.

Для проверки развертывания сертификатов выполните следующие шаги.

1. Щелкните на кнопке Start (Пуск), чтобы открыть экран Metro.
2. Введите текст mmc, чтобы открыть поле поиска и найти исполняемый файл mmc.
3. Запустите утилиту mmc из результата поиска.
4. Выберите пункт меню File⇨Add/Remove Snap-In (Файл⇨Добавление или удаление оснастки).
5. Выберите оснастку Certificate (Сертификаты) и щелкните на кнопке Add (Добавить).
6. Выберите вариант Computer Account Management Scope (Область управления учетными записями компьютера) и щелкните на кнопке Next (Далее).
7. Согласитесь с вариантом Local Computer (Локальный компьютер), щелкните на кнопке Finish (Готово), а затем на кнопке OK.
8. Раскройте папку Certificates (Local Computer) (Сертификаты (Локальный компьютер)), в ней папку Personal (Личные), а в ней — папку Certificates (Сертификаты).
9. Просмотрите и проверьте сертификат, который находится на панели результатов.

Смарт-карты в инфраструктуре открытых ключей

Надежным решением инфраструктуры открытых ключей может быть аутентификация пользователей с помощью смарт-карт. Смарт-карты — это пластиковые карточки со встроенным микрочипом, USB-ключи или другие устройства.

Смарт-карта может содержать информацию входной регистрации пользователя, а также сертификаты, выданные сервером CA. Когда пользователю нужно войти в систему, он вставляет карточку в специальное считывающее устройство или просто проводит по нему карточкой. Устройство считывает сертификат и предлагает пользователю ввести только уникальный PIN-код, присвоенный каждому пользователю. После проверки PIN-кода и сертификата пользователь может войти в домен.

Смарт-карты выполняют аутентификацию по двум факторам и обладают очевидными преимуществами по сравнению со стандартными формами аутентификации. При их использовании невозможно просто похитить или угадать чье-то имя пользователя и пароль, поскольку имя пользователя можно ввести только с помощью уникальной смарт-карты. Если смарт-карта похищена или утеряна, ее можно тут же отключить, а сертификат отозвать. Даже если функционирующая карточка попадет в чужие руки, для доступа к системе нужен еще и PIN-код. Смарт-карты быстро становятся все более распространенным способом сочетания защиты, предоставляемой сертификатами и PKI.

Использование шифрованной файловой системы (EFS)

Точно так же, как на транспортном уровне информация может быть зашифрована с помощью сертификатов и PKI, в Windows Server 2012 можно зашифровать файловую

систему Resilient File System (ReFS) для предотвращения несанкционированного доступа. Шифрованная файловая система (Encrypting File System — EFS) в Windows Server 2012 расширяет возможности предыдущей модели EFS, позволяя хранить наборы шифрования в автономных папках на сервере. Эта модель особенно удобна для пользователей ноутбуков, которые разъезжают с секретной информацией. В случае похищения ноутбука или его жесткого диска информация, хранящаяся в файлах, оказывается бесполезной, поскольку она искажена до неузнаваемости и может быть расшифрована только с помощью соответствующего ключа. Поэтому модель EFS — важная часть в реализациях инфраструктуры открытых ключей.

Технология Windows BitLocker идет еще дальше, чем EFS, и позволяет зашифровать весь жесткий диск, за исключением нескольких загрузочных файлов.

Интеграция PKI с зонами Kerberos

Компонент Active Directory из Windows Server 2012 может использовать инфраструктуру PKI, в которой применяются отношения доверия между зонами Kerberos и Active Directory. Инфраструктура PKI служит механизмом аутентификации для запросов на установление безопасных доверительных отношений между различными зонами, которые могут быть созданы в Active Directory.

Служба управления правами Active Directory

Служба управления правами Active Directory (Active Directory Rights Management Services — AD RMS) представляет собой технологию управления цифровыми правами (Digital Rights Management — DRM), позволяющую устанавливать ограничения на управление, пересылку и просмотр содержимого. В RMS используется технология PKI для шифрования такого содержимого, как документы и почтовые сообщения, а также для просмотра этой информации без возможности ее печати, копирования-вставки и/или перенаправления.

AD RMS в Windows Server 2012 является усовершенствованием технологии сервера управления правами Windows (Windows Rights Management Server), которая развивается уже несколько лет. Кроме уже существующих возможностей в ней усилена интеграция со службой доменов Active Directory (Active Directory Domain Services (AD DS) и повышена масштабируемость.

Зачем нужна AD RMS

Многие организации сталкиваются с проблемой управления их интеллектуальной собственностью после ее распространения. Несколько серьезных утечек внутренней секретной переписки в крупных корпорациях продемонстрировали необходимость управления и ограничения в случаях распространения конфиденциальной корпоративной информации.

Источник проблемы состоит в том, что исторически компьютерные системы хорошо справляются с ограничением доступа к информации для неавторизованных лиц, но после авторизации управление действиями с информацией теряется. Авторизованные лица могут копировать документы “на вынос”, отправлять секретную информацию по электронной почте, у них могут пропадать ноутбуки — и вообще может существовать множество различных способов утраты контроля над конфиденциальной информацией организации.

Служба Active Directory RMS предназначена для возврата возможностей контроля в такие организации. Она позволяет уполномоченному персоналу ограничивать возможности пересылки, печати, копирования и указания срока годности документов. Кроме того, интеграция со службой доменов Active Directory разрешает дешифровать информацию только лицам, специально указанным в политиках.

НА ЗАМЕТКУ

Для отображения изменений в документах, защищенных службой RMS, их необходимо "переопубликовать", а у клиентов наряду с наличием локальной копии такого документа должны быть кешированы лицензии на использование. Если срок годности лицензии на использование не истек, пользователи будут все так же иметь доступ к защищенным документам, которые либо не опубликованы заново, ли перемещены из места переопубликования документа.

В состав AD RMS входит также служба роли Identity Federation Support (Поддержка интегрированного контроля подлинности). Установка этой службы позволяет организациям делиться закрытой информацией с другими организациями.

Условия, необходимые для работы AD RMS

Прежде чем приступать к установке AD RMS, необходимо обеспечить выполнение следующих условий.

- Нужно создать в AD DS учетную запись службы для RMS. Она не должна совпадать с учетной записью, использованной для установки RMS.
- Сервер AD RMS должен быть членом домена пользовательских учетных записей, которые будут пользоваться этой службой.
- Необходимо создать корневой кластер AD RMS для сертификации и лицензирования.
- Нужно создать полностью определенное доменное имя (FQDN), известное в тех местах, где будут использоваться RMS-файлы. Например, можно создать доменное имя `rms.companyabc.com` для клиентов, которым нужно будет подключаться к серверу AD RMS для проверки своих RMS-прав.
- Необходим доступный работающий SQL Server для хранения баз данных AD RMS. Настоятельно рекомендуется использовать сервер, отличный от того сервера, на котором установлена служба AD RMS.

Установка AD RMS

Для установки AD RMS можно добавить на сервер роль AD RMS с помощью утилиты Server Manager.

1. Откройте диспетчер серверов (Server Manager).
2. В меню Manage (Управление) выберите пункт Add Roles and Features (Добавление ролей и компонентов).
3. Щелкните на кнопке Next (Далее) на странице приветствия, а затем на странице Installation Type (Тип установки).
4. Выберите из списка сервер AD RMS и щелкните на кнопке Next.
5. На странице Select Server Roles (Выбор ролей сервера) установите флажок Active Directory Rights Management Services (Служба управления правами Active Directory). Если появится сообщение о необходимости дополнительных компонентов, щелкните на кнопке Add Features (Добавить компоненты), чтобы согласиться с добавлением нужных служб ролей, а затем щелкните на кнопке Next.
6. Щелкните на кнопке Next, чтобы принять список компонентов.
7. На странице Introduction (Введение) просмотрите информацию об AD RMS и щелкните на кнопке Next.

8. На странице Select Role Services (Выбор служб ролей) укажите службы, которые нужно установить. В данном случае будет установлена только служба роли Active Directory Rights Management Server (Сервер управления правами Active Directory). Щелкните на кнопке Next.
9. Щелкните на кнопке Install (Установить) и наблюдайте за процессом установки, как показано на рис. 14.6.

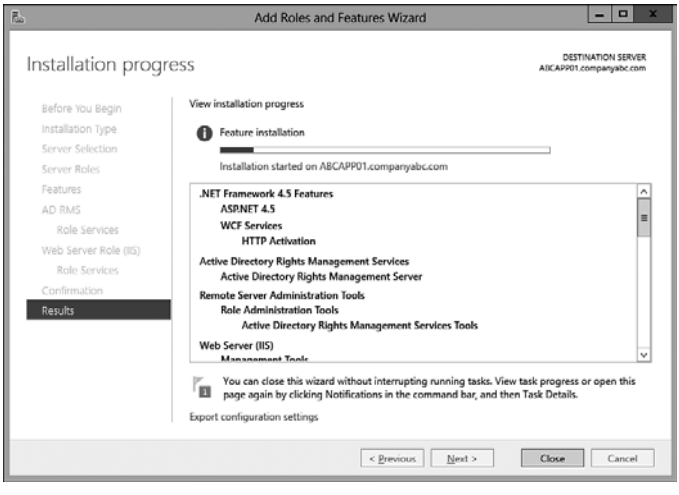

Рис. 14.6. *Установка AD RMS*

10. После завершения установки щелкните на ссылке Perform Additional Configuration (Выполнить дополнительную настройку).

Теперь завершите работу в мастере настройки следующим образом.

1. Просмотрите вводное описание и щелкните на кнопке Next (Далее).
2. Согласитесь со стандартным вариантом (создание нового кластера) и щелкните на кнопке Next.
3. Выберите вариант Use Windows Internal Database on This Server (Использовать на этом сервере внутреннюю СУБД Windows).

НА ЗАМЕТКУ

Внутренняя СУБД Windows годится для непроизводственных сред и для целей данного примера, однако она не пригодна для масштабирования и не поддерживает состояние высокой готовности. Поэтому в производственных развертываниях ее лучше не использовать.

4. Введите данные учетной записи службы и щелкните на кнопке Next.
5. Согласитесь с предложенным по умолчанию криптографическим режимом и щелкните на кнопке Next.
6. Согласитесь с предложенным по умолчанию централизованным хранилищем ключей и щелкните на кнопке Next.
7. Введите пароль для ключа и щелкните на кнопке Next.
8. Согласитесь с предложенным стандартным веб-сайтом и щелкните на кнопке Next.

9. Введите тип подключения безопасности, введите URL-адрес RMS и щелкните на кнопке Next.

НА ЗАМЕТКУ

В производственных развертываниях настоятельно рекомендуется для всех обращений к RMS использовать протокол HTTPS. В средах, где имеются лишь внутренние потребители контента, можно применять Интернет-сертификаты. А если требуется интеграция с внешними потребителями, следует использовать сторонние сертификаты.

10. Выберите нужный сертификат для кластера и щелкните на кнопке Next.
11. Введите описательное имя для сертификата, который будет удостоверять вашу подлинность в RMS. Рекомендуется применять в качестве имени хоста тот же URL-адрес. Затем щелкните на кнопке Next.
12. Выберите, когда нужно регистрировать точку подключения к службе AD (Service Connection Point — SCP). В проектах SCP обычно публикуется позже, после настройки и тестирования шаблонов RMS. Сразу после опубликования SCP компоненты и шаблоны RMS станут доступными для пользователей Office и Windows. Щелкните на кнопке Next.
13. Просмотрите выбранные параметры и щелкните на кнопке Install (Установить).
14. После завершения установки щелкните на кнопке Close (Закрыть).

Шифрование IPsec в Windows Server 2012

Протокол защиты данных в Интернете (IP Security — IPsec), уже упоминавшийся в предшествующих разделах, представляет собой механизм для оперативного шифрования всех пакетов, пересылаемых между компьютерами. IPsec действует на уровне 3 модели OSI и, значит, для передачи всего трафика между членами процесса использует пакеты.

Протокол IPsec часто считают одним из лучших способов защиты генерируемого в среде трафика: он удобен для защиты серверов и рабочих станций как в случаях небезопасного доступа к Интернету, так и в конфигурациях частных сетей для создания дополнительного уровня безопасности.

Принцип работы IPsec

Основной принцип IPsec таков: весь трафик между клиентами — инициируемый приложениями, операционной системой, службами и прочими элементами — полностью шифруется протоколом IPsec, который затем вставляет в каждый пакет свой заголовок и отправляет пакеты серверу назначения для расшифровки. Поскольку все фрагменты данных зашифрованы, это препятствует электронному прослушиванию сети для получения несанкционированного доступа к данным.

Возможно несколько функциональных реализаций IPsec. Некоторые из наиболее перспективных решений встроены непосредственно в сетевые интерфейсные платы (NIC) каждого компьютера, что позволяет выполнять шифрование и расшифровку без какого-либо участия операционной системы. Кроме этих вариантов, Windows Server 2012 по умолчанию содержит надежную реализацию IPsec, которую можно сконфигурировать для применения аутентификации с помощью сертификатов PKI.

Основные возможности IPsec

IPsec в Windows Server 2012 предоставляет следующие возможности, которые при их сочетании дают наиболее надежные решения шифрования для клиент-серверных систем.

- **Конфиденциальность данных.** Вся информация, пересылаемая с одного IPsec-компьютера на другой, полностью шифруется с помощью таких алгоритмов, как 3DES, что эффективно препятствует несанкционированному просмотру секретных данных.
- **Целостность данных.** Целостность пакетов IPsec обеспечивается с помощью заголовков ESP, которые позволяют проверить, что информация, содержащаяся внутри пакета IPsec, не была подменена.
- **Возможность предотвращения повторной передачи.** IPsec препятствует повторной передаче потоков перехваченных пакетов — т.е. атаке имитацией повторной передачи — блокируя получение несанкционированного доступа к системе путем имитации ответа законного пользователя на запросы сервера.
- **Проверка аутентичности каждого пакета.** IPsec использует сертификаты или аутентификацию Kerberos для проверки того, что отправителем пакета IPsec действительно является законный пользователь.
- **NAT Traversal или Teredo.** Теперь реализация IPsec в Windows Server 2012 допускает маршрутизацию пакетов IPsec через существующие реализации трансляции сетевых адресов (Network Address Translation — NAT). Подробнее эта концепция будет рассмотрена в последующих разделах.
- **Поддержка 2048-битного ключа Диффи-Хеллмана.** Реализация IPsec в Windows Server 2012 поддерживает применение практически недоступных для взлома 2048-битных ключей, что, по сути дела, обеспечивает невозможность взлома ключа IPsec.

NAT Traversal в IPsec

Как уже было сказано, теперь IPsec в Windows Server 2012 поддерживает концепцию прохождения с трансляцией сетевых адресов (Network Address Translation Traversal — NAT Traversal, или NAT-T). Чтобы понять, как работает NAT-T, вначале следует разобраться, для чего необходима сама трансляция сетевых адресов.

Трансляция сетевых адресов (Network Address Translation — NAT) была разработана по той простой причине, что в Интернете не хватало IP-адресов для всех клиентов. Поэтому были определены частные IP-диапазоны (10.x.x.x, 192.168.x.x и 172.16–31.x.x), чтобы всем клиентам в данной организации можно было присваивать уникальный IP-адрес в собственном частном адресном пространстве. Эти IP-адреса не предназначены для маршрутизации через пространство общедоступных IP-адресов, и для их преобразования в действующий уникальный общедоступный IP-адрес требовался специальный механизм.

В качестве этого механизма была разработана технология NAT. Обычно эта функция выполняется в серверах брандмауэров или маршрутизаторах, обеспечивая трансляцию сетевых адресов между частными и общедоступными сетями. Сервер RRAS Windows Server 2012 также предоставляет возможности NAT.

Поскольку в структуре пакета IPsec адреса NAT невозможны, раньше серверы NAT просто отсекали трафик IPsec, поскольку не существовало способа физической маршрутизации информации в соответствующий пункт назначения. Это и было основным барьером на пути повсеместного распространения IPsec, поскольку в настоящее время адресация многих клиентов в Интернете выполняется посредством NAT.

NAT Traversal (или NAT-T), присутствующий в реализации IPsec в Windows Server 2012 — это Интернет-стандарт, совместно разработанный компаниями Microsoft и Cisco Systems. NAT-T осуществляется посредством определения, требуется ли прохождение сети NAT, и последующей инкапсуляции всего пакета IPsec в пакет UDP (User Datagram Protocol — протокол пользовательских дейтаграмм) с обычным заголовком UDP. NAT беспрепятственно

выполняет обработку пакетов UDP, а затем они пересылаются по соответствующему адресу на другой конец NAT.

Для успешной работы NAT Traversal требуется, чтобы оба участника IPsec-транзакции поддерживали этот протокол и могли правильно извлекать пакет IPsec из пакета UDP. С появлением последних версий клиента и сервера IPsec NAT Traversal становится реальностью и создает предпосылки значительно более успешного применения технологии IPsec, чем в настоящее время.

НА ЗАМЕТКУ

Технология NAT-T была разработана для сохранения существующих технологий NAT без изменений. Однако в некоторых реализациях NAT были предприняты попытки своего преобразования пакетов IPsec без применения NAT-T. Но при использовании NAT-T, возможно, будет лучше отключить эту функцию: она может вступить в противоречие с IPsec, поскольку и NAT-T, и брандмауэр NAT будут пытаться преодолеть барьер NAT.

Резюме

В современных взаимосвязанных сетях безопасность транспортного уровня является важным (если не одним из главных) фактором обеспечения безопасности в любой организации. Защита коммуникаций между пользователями и компьютерами в сети — очень важное условие, а в некоторых случаях оно требуется законом. Система Windows Server 2012 построена на надежном фундаменте системы безопасности Windows Server 2003 и Windows Server 2008 и включает в себя поддержку таких механизмов безопасности транспортного уровня, как IPsec и PKI, с помощью технологий наподобие AD CS и AD RMS. Правильное конфигурирование и применение этих средств может эффективно защитить передачу данных в организации и обеспечить их использование только теми, для кого эти данные предназначены.

Полезные советы

Ниже перечислены полезные советы этой главы.

- Для защиты сетевой среды используйте одну или несколько доступных технологий безопасности транспортного уровня.
- Поскольку даже самые надежные инфраструктуры имеют уязвимые места, рекомендуется создать несколько уровней безопасности для особо важных сетевых данных.
- Настоятельно рекомендуется не устанавливать локально базу данных AD RMS на сервер RMS. Лучше используйте удаленный полный экземпляр SQL Server.
- Уделите самое серьезное внимание защите сервера головного CA службы сертификации Active Directory, т.к. брешь в безопасности этого сервера скомпрометирует всю цепочку CA.
- Храните самостоятельный головной сервер CA в физически запертом месте и выключайте его, если он в данный момент не нужен. Этот совет не относится к головным CA предприятия, которые нельзя отключать на длительное время.
- Используйте технологию IPsec для защиты сгенерированного в данной среде трафика и для защиты серверов и рабочих станций как в случаях небезопасного доступа к Интернету, так и в конфигурациях частных сетей.