ГЛАВА 14

Безопасность на транспортном уровне

В ЭТОЙ ГЛАВЕ...

- Введение в безопасность на транспортном уровне в Windows Server 2008
- Развертывание инфраструктуры открытых ключей с помощью Windows Server 2008
- Служба сертификации Active Directory (AD CS) в Windows Server 2008
- Служба управления правами AD DS
- Шифрование IPSec в Windows Server 2008

В прошлом сети представляли собой замкнутые среды, изолированные одна от другой и доступные только во внутренних сегментах. 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 2008 способно существенно повысить безопасность сети. Во многих случаях применение таких решений совершенно обязательно, особенно для данных, которые пересылаются через неконтролируемые сегменты сети наподобие Internet.

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 2008, 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 2008.

Введение в безопасность на транспортном уровне в Windows Server 2008

Безопасность на транспортном уровне — это защита обмена информацией между клиентом и сервером или между серверами. Хотя в некоторых организациях применяются брандмауэры или шифрование файлов, 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 дешифровки 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 2008 предоставляет большое количество средств безопасности транспортного уровня, и для надежной защиты важных данных рекомендуется использовать одну или несколько из этих технологий.

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" 128-битная 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 безопасности транспортного уровня Windows 2008 используют несколько уровней аутентификации, шифрования и авторизации для повышения уровня безопасности сети. Возможности конфигурирования, предоставляемые Windows 2008, позволяют установить несколько уровней безопасности транспортного уровня.

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.

Основы шифрования

В упрощенной формулировке *шифрование* (encryption) — 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 Internet 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 2008

Термин *инфраструктура 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 подтверждения, что пользователь, сообщающийся по сети с другим пользователем или компьютером, является тем, за кого он себя выдает. Реализации PKI широко распространены и становятся исключительно важным компонентом современных реализаций сетей. Как описано в последующих разделах, Windows 2008 полностью поддерживает развертывание нескольких конфигураций PKI.

Реализации PKI могут быть как простыми, так и сложными, а некоторые применяют массивы смарт-карт 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 дешифровки 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 дешифровки информации.

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 дешифровки информации. Второй — открытый — ключ может использоваться для шифрования информации. Целостность открытого ключа обеспечивается сертификатами, которые подробно описаны в последующих разделах этой главы. Асимметричный подход к шифрованию гарантирует, что секретный ключ не попадет в чужие руки, и только законный получатель сможет дешифровать данные.

Знакомство с цифровыми сертификатами

Сертификат (certificate) представляет собой цифровой документ, который выдается доверяемым центром и используется им для подтверждения подлинности пользователя. Доверяемые центры сертификации наподобие VeriSign широко используются в Internet, чтобы, например, подтвердить, 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 в Web.
- Защита данных в Internet (IPSec).
- Подписание кода.
- Создание иерархий сертификации.

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).

Служба сертификации Active Directory (AD CS) в Windows Server 2008

Windows 2008 содержит встроенный центр сертификации (CA), называемый службой сертификации Active Directory (Active Directory Certificate Services — AD CS). До Windows Server 2008 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. Зачастую AD CS в Windows 2008 используется без особой необходимости проверки сертификатов организации какой-либо независимой стороной. Поэтому если сертификаты требуются только для участников внутри организации, часто применяется развертывание самостоятельного CA для шифрования сетевого трафика. 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.

Обзор ролей центров сертификации в AD CS

AD CS для Windows 2008 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 снятия части нагрузки с 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 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.

НА ЗАМЕТКУ

Принятие решений по структуре AD CS — задача нетривиальная, и к ней не следует подходить легкомысленно. Простое забрасывание 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 CA предприятия, затем нескольких подчиненных CA, а затем физическое отключение головного CA и помещение в очень защищенное место, чтобы включать его, только если требуется обновление сертификатов подчиненных CA. Эти соображения делают CA предприятия хорошим кандидатом на виртуализацию сервера Windows.

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 инсталлировать на сервере. Вот эти службы.

- **Центр сертификации.** Данная служба инсталлирует базовый компонент CA, позволяющий серверу издавать и отзывать сертификатами для клиентов и управлять ими. Эту роль можно инсталлировать на нескольких серверах в цепочке одного и того же корневого CA.
- **Web-включение центра сертификации.** Данная служба управляет распространением сертификатов клиентам через Internet. Для ее работы нужно, чтобы на сервере была инсталлирована служба информации Internet (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).
- **Служба включения сетевых устройств.** Данная служба упрощает получение сертификатов сетевыми устройствами наподобие маршрутизаторов.

Установка AD CS

Для установки AD CS в Windows 2008 вначале нужно выбрать сервер, который будет работать в качестве CA предприятия. Не забывайте о настоятельных рекомендациях, что это должен быть выделенный сервер, защищенный физически и выключенный бо́льшую часть времени для обеспечения целостности цепочки сертификатов. После выбора компьютера, который будет корневым CA предприятия, выполните следующие шаги для инсталляции AD CS в качестве CA предприятия.

НА ЗАМЕТКУ

После инсталляции AD CS на сервере имя и доменный статус этого сервера изменять нельзя. Например, его нельзя понизить с уровня контроллера домена или повысить до этого уровня, если это не так. Кроме того, нельзя изменять имя сервера, пока он выполняет функции CA.

1. Откройте Server Manager: Start⇨All Programs⇨Administrative Tools⇨Server Manager (Пуск⇨Все программы⇨Администрирование⇨Server Manager).
2. В панели узлов выберите узел Roles (Роли), а затем щелкните на ссылке Add Roles (Создать роли) в панели задач.
3. На странице приветствия щелкните на кнопке Next (Далее).
4. На странице Select Server Roles (Выбор серверных ролей) установите флажок Active Directory Certificate Services (Служба сертификации Active Directory), а затем щелкните на кнопке Next (Далее).
5. На странице Introduction (Введение) просмотрите информацию об AD CS и щелкните на кнопке Next (Далее).
6. На странице Select Role Services (Выбор служб ролей), показанной на рис. 14.1, укажите нужные службы ролей. Для базовой инсталляции нужна только роль Certificate Authority (Центр сертификации). Щелкните на кнопке Next (Далее).

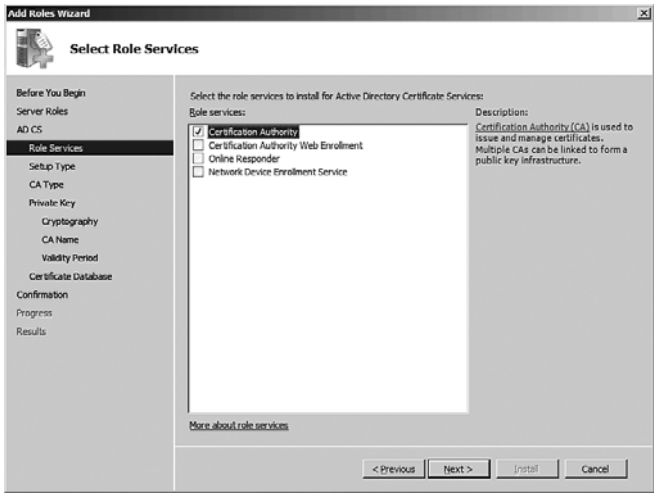

Рис. 14.1. *Установка AD CS*

7. На следующей странице укажите, нужно ли инсталлировать центр сертификации предприятия (Enterprise CA), интегрированный с AD CS, или самостоятельный центр сертификации (Stand-alone CA). Щелкните на кнопке Next (Далее).
8. На странице Specify CA Type (Укажите тип CA), показанной на рис. 14.2, выберите нужный тип CA. В данном случае мы устанавливаем на сервер корневой CA (Root CA). Щелкните на кнопке Next (Далее).

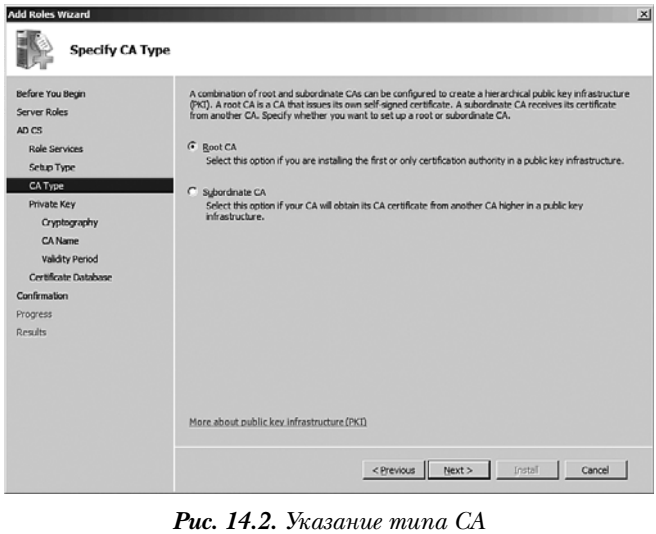

Рис. 14.2. *Указание типа CA*

9. На следующей странице Set Up Private Key (Создание секретного ключа) 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 (Далее).

10. 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 (Далее).

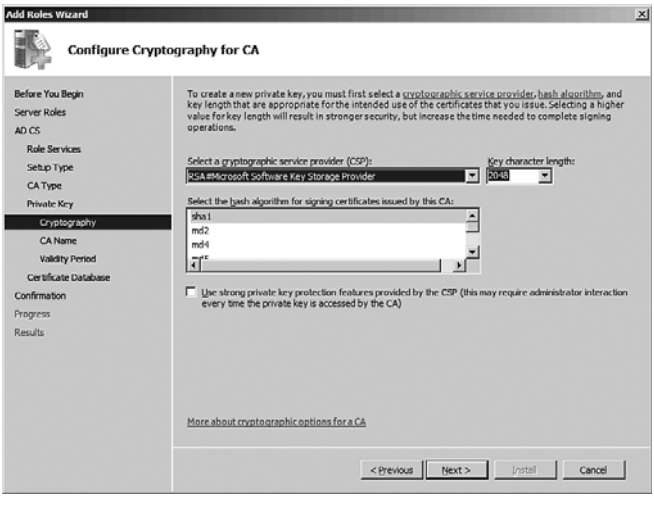

Рис. 14.3. *Выбор криптографических параметров*

11. 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 (Далее).
12. Укажите срок годности сертификата, который будет установлен на данном сервере CA. Если это корневой CA, сервер должен будет повторно выпустить цепочку сертификатов после истечения срока годности. В данном примере мы выбрали 5-летний срок годности. Щелкните на кнопке Next (Далее).
13. Укажите место хранения базы данных сертификатов и местоположения для хранения журналов, а затем щелкните на кнопке Next (Далее).
14. На странице подтверждения (рис. 14.4) просмотрите параметры предстоящей инсталляции и щелкните на кнопке Install (Установить).
15. После завершения работы мастера щелкните на кнопке Close (Закрыть).

После инсталляции AD CS можно инсталлировать дополнительные (подчиненные) CA и выполнять администрирование PKI с консоли центра сертификации: Start⇨All Programs⇨Administrative Tools⇨Certification Authority (Пуск⇨Все программы⇨Администрирование⇨Центр сертификации).

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 в них микрочипом. Этот чип позволяет хранить на каждой карточке уникальную информацию.

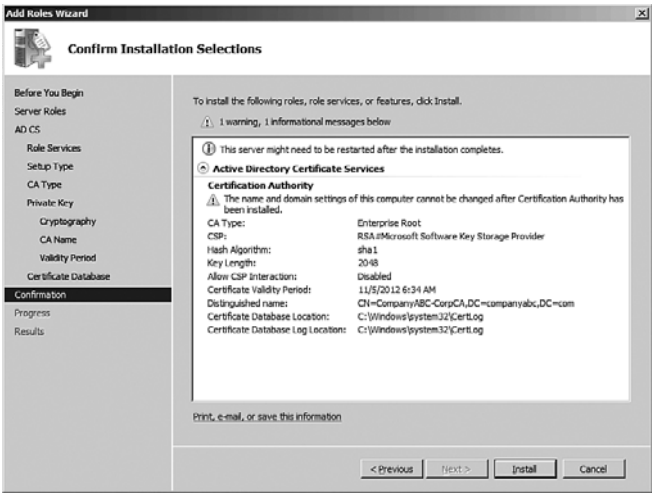

Рис. 14.4. *Просмотр параметров установки AD CS*

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 деактивизировать, 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 2008 можно зашифровать файловую систему NTFS для предотвращения несанкционированного доступа. Шифрованная файловая система (Encrypting File System — EFS) в Windows 2008 расширяет возможности модели EFS из Windows 2000, 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.

Интеграция PKI с зонами Kerberos

Компонент Active Directory Windows 2008 может использовать инфраструктуру PKI, в которой применяются отношения доверия между зонами (realm) 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 AD DS

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 2008 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 кэшированы 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 (Интегрированный контроль 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, 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.
- Нужен 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 Server Manager: Start⇨All Programs⇨Administrative Tools⇨Server Manager (Пуск⇨Все программы⇨Администрирование⇨Server Manager).
2. В панели узлов выберите узел Roles (Роли), а затем щелкните на ссылке Add Roles (Создание ролей) в панели задач.
3. На странице приветствия щелкните на кнопке Next (Далее).
4. 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 служб и возможностей, наподобие IIS или службы очередей сообщений, согласитесь с добавлением нужных служб ролей, а затем щелкните на кнопке Next (Далее).
5. Просмотрите страницу Introduction (Введение) и щелкните на кнопке Next (Далее).
6. На странице Select Role Services (Выбор служб ролей), показанной на рис. 14.5, укажите компоненты, которые нужно установить. В данном случае будет установлена только служба роли AD RMS. Щелкните на кнопке Next (Далее).
7. На странице AD RMS Cluster (Кластер AD RMS) выберите вариант Create a New AD RMS Cluster (Создать нового кластера AD RMS) и щелкните на кнопке Next (Далее).
8. На странице Select Configuration Database (Выбор базы данных конфигурации) укажите один из вариантов: установка ограниченной службы Windows Internal Database (не рекомендуется), либо создание базы данных RMS на отдельном сервере SQL Server 200x.

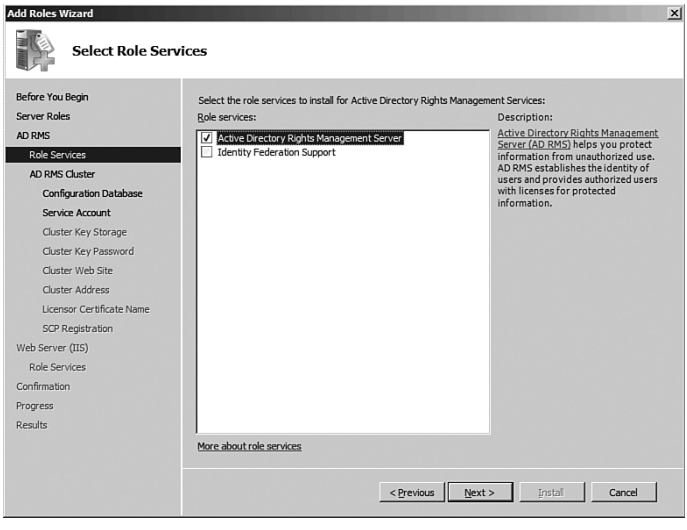

Рис. 14.5. *Установка AD RMS*

9. На странице Specify Service Account (Указание учетной записи службы), показанной на рис. 14.6, укажите с помощью кнопки Specify (Указать) учетную запись службы, которая будет использоваться для RMS. Она не должна совпадать с учетной записью, использованной для установки AD RMS.

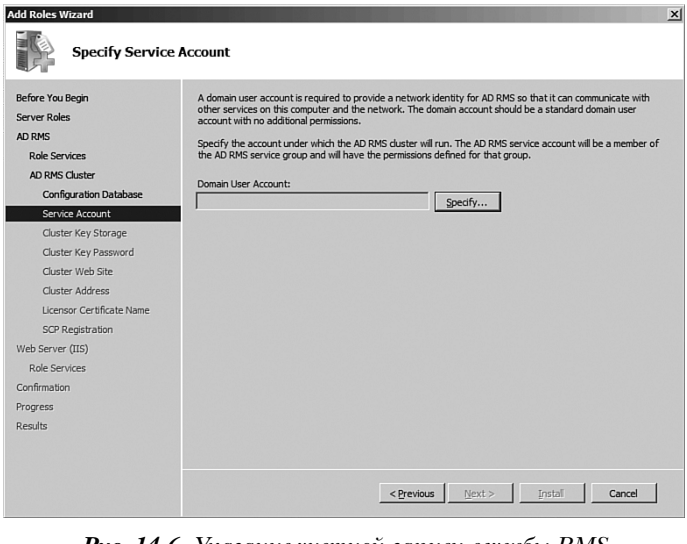

Рис. 14.6. *Указание учетной записи службы RMS*

10. На следующей странице выберите вариант Use AD RMS Centrally Managed Key Storage (Использовать централизованно управляемое хранилище ключей AD RMS) и щелкните на кнопке Next (Далее).
11. При появлении приглашения введите стойкий пароль и щелкните на кнопке Next (Далее).

12. Укажите, какой Web-сайт IIS будет содержать Web-службы RMS (Default Web Site (Web-сайт по умолчанию) для обособленной установки), и щелкните на кнопке Next (Далее).
13. Введите FQDN, которое будет применяться для службы AD RMS. В нашем примере введите `rms.companyabc.com`, а затем щелкните на кнопке Validate (Проверка). Это FQDN уже должно быть настроено для разрешения IP-адреса Web-сайта IIS на сервере RMS. Щелкните на кнопке Next (Далее).

НА ЗАМЕТКУ

Рекомендуется использование сертификата SSL для HTTPS-подключения к серверу RMS. Его можно активизировать в этом мастере.

14. Введите описательное имя для кластера RMS и щелкните на кнопке Next (Далее).
15. На странице AD RMS Service Connection Point Registration (Регистрация точки подключения службы AD RMS) щелкните на кнопке Next (Далее), чтобы зарегистрировать точку подключения службы (Service Connection Point — SCP) в AD DS.
16. Если одновременно выполняется установка IIS, то согласитесь с настройками по умолчанию, щелкнув на кнопке Next (Далее), и затем снова щелкните на кнопке Next (Далее).
17. Щелкните на кнопке Install (Установить), чтобы завершить работу мастера. Дождитесь окончания процесса инсталляции.
18. После завершения работы мастера щелкните на кнопке Finish (Готово). Перезапустите компьютер и снова войдите в систему, чтобы завершить установку.

Шифрование IPSec в Windows Server 2008

Протокол защиты данных в Internet (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 Internet, 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 дешифровки. 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 дешифровку без какого-либо участия операционной системы. Кроме этих вариантов, Windows 2008 по умолчанию содержит надежную реализацию IPSec, которую можно сконфигурировать для применения аутентификации с помощью сертификатов PKI.

Основные возможности IPSec

IPSec в Windows 2008 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.** Теперь реализация IPSec в Windows 2008 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 2008 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 2008 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 Internet не хватало IP-адресов для всех клиентов. Поэтому были определены частные IP-диапазоны (10.x.x.x, 192.168.x.x и т.д.), 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 2008 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 Internet выполняется посредством NAT.

Новая возможность в реализации IPSec в Windows 2008 — NAT Traversal — это стандарт Internet, 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 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, поскольку она может вступить в противоречие с IPSec, так как 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 2008 построена на надежном фундаменте системы безопасности Windows 2000 Server и Windows Server 2003 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 SQL Server.
- Уделите самое серьезное внимание защите сервера корневого CA службы сертификации Active Directory, т.к. брешь в безопасности этого сервера скомпрометирует всю цепочку CA.
- Храните сервер корневого CA в физически запертом месте и выключайте его, если он в данный момент не нужен — либо воспользуйтесь виртуализацией серверов Windows.
- Используйте технологию IPSec для защиты сгенерированного в данной среде трафика и для защиты серверов и рабочих станций как в случаях небезопасного доступа к Internet, так и в конфигурациях частных сетей.