ГЛАВА 8

Создание федеративных лесов и каталогов с облегченным доступом

В ЭТОЙ ГЛАВЕ...

- Поддержание распределенной среды в синхронизированном состоянии
- Технология Active Directory Federation Services
- Синхронизация информации каталогов с помощью Forefront Identity Manager (FIM)
- Использование мощи и потенциала FIM

В Windows Server 2008 R2 поставляется не только традиционная версия служб каталогов под названием Active Directory Domain Services (Доменные службы Active Directory), или, сокращенно, AD DS, но и версия, предназначенная специально для определенных приложений и меньших приложений с облегченным доступом. Эта версия служб каталогов называется Active Directory Lightweight Directory Services (Службы Active Directory облегченного доступа к каталогам), или AD LDS.

Поддержка информации и идентификационных данных между такими каталогами в синхронизированном состоянии — задача непростая. По этой причине в состав Windows Server 2008 R2 входит версия служб каталогов Active Directory Federation Services (Службы федерации Active Directory), или AD FS, и средство для синхронизации метакаталога под названием ForeFront Identity Manager (FIM), помогающее при работе с федерациями. В настоящей главе рассматриваются вопросы создания для каталогов и приложений предприятия федеративных лесов и каталогов с облегченным доступом.

Поддержание распределенной среды в синхронизированном состоянии

Когда в Microsoft первоначально разрабатывали Active Directory для Windows 2000 Server, предполагалось, что это будет единственный каталог, требуемый организации. Идея состояла в том, чтобы предоставить организациям возможность разместить все службы централизованным образом внутри среды Active Directory и затем позволить приложениям использовать ее в качестве их собственного каталога.

Развитие этой технологии привело к совершенно противоположному эффекту, а именно: количество каталогов в организациях начало неуклонно расти. Организации стали создавать не только множество каталогов внутри приложений, но и множество лесов Active Directory для усиления безопасности.

С усовершенствованием Active Directory, в Microsoft увидели необходимость в объединении всех таких каталогов вместе в единственный федеративный метакаталог, а также возможность предоставления приложений с собственными каталогами, основанными на модели AD.

В настоящей главе рассматриваются все эти технологии и показано, как объединить множество лесов AD DS в единственный федеративный лес и затем обеспечить синхронизацию подобной структуры с другими внешними платформами каталогов. Кроме того, здесь подробно рассказывается о предлагающем такие возможности продукте Microsoft Forefront Identity Manager, а также о технологиях AD LDS (Active Directory Lightweight Directory Services — службы Active Directory облегченного доступа к каталогам) и AD FS (Active Directory Federation Services — службы федерации Active Directory).

Технология AD LDS

Одной из новых среди связанных с Active Directory технологий в Windows Server 2008 R2 является Active Directory Lightweight Directory Services (Службы Active Directory облегченного доступа к каталогам), или AD LSD. Эта технология раньше называлась ADAM (Active Directory in Application Mode — Active Directory в режиме приложений). Она представляет собой технологию каталогов, очень похожую на AD DS (Active Directory Domain Services — доменные службы Active Directory), но имеющую возможность запускать отдельные экземпляры самой себя в виде уникальных служб. AD LDS позволяет специализированным приложениям использовать AD LDS в качестве собственной службы каталогов, тем самым исключая необходимость в применении службы каталогов нового вида для каждого критически важного приложения в организации.

AD LDS использует тот же механизм репликации и ту же структуру X.500, что и AD DS, и имеет достаточно схожие с AD DS функциональные возможности, что позволяет ее устанавливать в качестве испытательной системы для разработчиков, которые занимаются проектированием приложений AD DS. Однако, несмотря на все сходства, AD LDS работает как отдельная от операционной системы служба, имеющая собственную схему и структуру.

Главным преимуществом AD LDS является ее способность использовать структуру защиты производственного домена (или доменов), поддерживая при этом собственную структуру каталогов.

Необходимость в AD LDS

Служба AD LDS была разработана для непосредственного устранения одного из главных ограничений AD DS, а именно — сильной зависимости каталога от сетевой ОС, ограничивавшей потребности, связанные с каталогами, даже тех приложений, которым не требовалась дополнительная функциональность сетевой ОС. AD LDS позволяет каждому приложению иметь собственный отдельный лес каталогов AD DS, а также собственные персональные настройки для каталогов, например, расширения схемы, характеристики репликации (или ее отсутствие) и другие ключевые для каталогов параметры.

Одно из главных преимуществ AD LDS заключается в том, что на одной машине может функционировать множество экземпляров AD LDS, каждый с собственным уникальным именем, номером порта и отдельным набором бинарных файлов. Вдобавок, служба AD LDS может быть запущена под управлением любой версии Windows Server 2008 R2 и даже в среде Windows 7 или Vista Professional (например, для целей разработки). Каждый экземпляр AD LDS может использовать отдельную, специальную схему.

AD LDS практически не отличается от обычного экземпляра AD DS, предполагающего применение сетевой ОС, и, следовательно, может обслуживаться с помощью стандартных для AD средств, таких как программа ADSIEdit, утилита `LDP.exe` и приложение MMC (Microsoft Management Console — консоль управления Microsoft). Кроме того, для специальной копии леса AD LDS могут быть созданы учетные записи пользователей и уникальные топологии репликации, а также применяться все обычные функциональные возможности AD DS.

В общем, AD LDS предоставляет приложениям преимущества среды AD DS, но без ограничений сетевой ОС, которые ранее вынуждали создавать множество невыгодных по стоимости каталогов. Теперь разработчики могут пользоваться всеми функциональными возможностями Windows Server 2008 R2 AD DS без ограничений, не теряя при этом многочисленных преимуществ интеграции в общую структуру безопасности.

Краткий обзор функциональных возможностей AD LDS

Ниже перечислены основные особенности AD LDS, о которых следует знать, прежде чем устанавливать эту технологию в организации.

- В отличие от AD DS, AD LDS не поддерживает глобальных каталогов, объектов групповой политики, доменов, лесов и отношений доверия между доменами.
- AD LDS не обязательно устанавливать на контроллерах доменов. В действительности AD LDS совершенно не зависит от операционной системы, и на каждом сервере может существовать более одного экземпляра AD LDS.
- Управление AD LDS нельзя производить привычными средствами AD DS, такими как оснастка Active Directory Users and Computers (Active Directory — пользователи и компьютеры). Вместо этого должны использоваться либо утилиты ADSIEdit и LDP.exe, либо специальный интерфейс.

Установка AD LDS

На одном сервере можно устанавливать как множество, так и один экземпляр AD LDS, и тогда просто настраивать репликацию его данных на другие серверы для обеспечения избыточности. Ниже перечислены шаги, необходимые для выполнения установки первого экземпляра AD LDS.

1. Откройте на сервере приложение Server Manager (Диспетчер сервера) (выбрав в меню Start (Пуск) пункт All Programs⇨Administrative Tools⇨Server Manager (Все программы⇨Администрирование⇨Диспетчер сервера)).
2. Перейдите к узлу Roles (Роли) и щелкните на ссылке Add Roles (Добавить роли).
3. На странице Before You Begin (Перед началом работы) просмотрите отображающиеся предварительные сведения и для продолжения щелкните на кнопке Next (Далее).
4. В списке ролей сервера (рис. 8.1) выберите вариант Active Directory Lightweight Directory Services (Службы Active Directory облегченного доступа к каталогам) отметив соответствующий ему флажок, и щелкните на кнопке Next.
5. На странице Introduction to Active Directory Lightweight Directory Services (Вводные сведения о службах Active Directory облегченного доступа к каталогам) просмотрите предлагаемую информацию и щелкните на кнопке Next.
6. Ознакомьтесь с дополнительными информационными сообщениями о необходимости запуска мастера установки и щелкните на кнопке Install (Установить).
7. Когда мастер добавление ролей (Add Roles Wizard) завершит процесс установки, щелкните на кнопке Close (Закрыть).
8. Запустите мастер установки служб Active Directory облегченного доступа к каталогам (Active Directory Lightweight Directory Services Setup Wizard) из меню Administrative Tools (Администрирование).
9. На экране приветствия щелкните на кнопке Next.

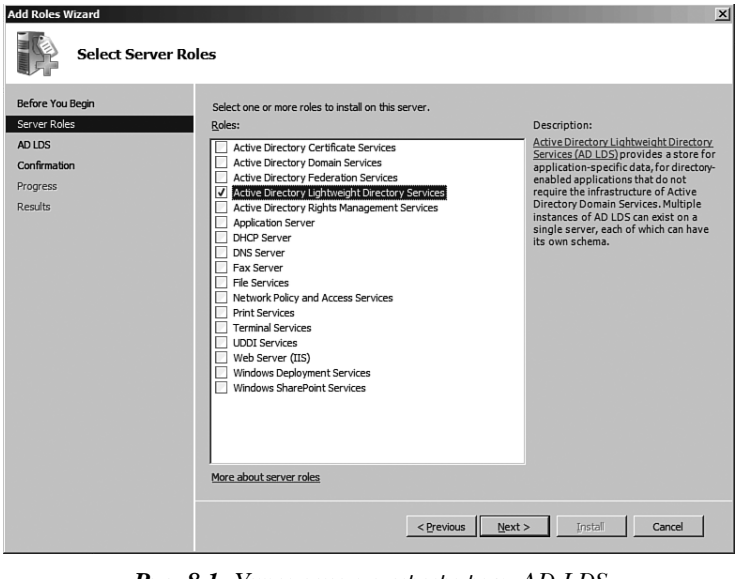

Рис. 8.1. *Установка на сервере роли AD LDS*

10. В диалоговом окне, которое показано на рис. 8.2, укажите, требуется создать новый уникальный экземпляр или копию какого-то существующего экземпляра. В рассматриваемом примере создается новый экземпляр с нуля. Щелкните на кнопке Next.

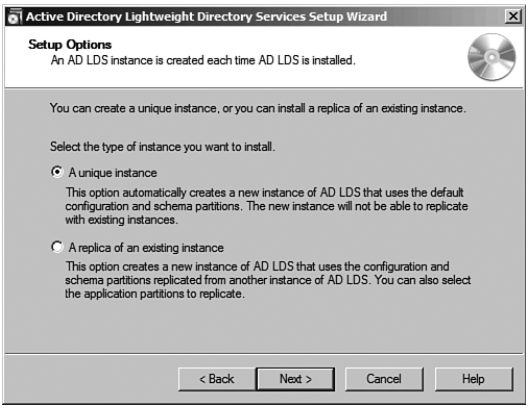

Рис. 8.2. *Установка экземпляра AD LDS*

11. Введите желаемое имя для экземпляра. Это имя должно отражать предназначение экземпляра. Для продолжения щелкните на кнопке Next.
12. Укажите порты LDAP и LDAPS, которые должны использоваться для данного экземпляра. Если стандартные для LDAP и LDAPS порты 389 и 639 уже заняты (например, из-за того, что на сервере уже функционирует AD DS или существует другой экземпляр AD LDS), выберите другие уникальные порты. В рассматриваемом примере предлагается выбрать для LDAP порт 50000, а для LDAPS — порт 50001. Для продолжения щелкните на кнопке Next.
13. На странице Application Directory Partition (Раздел каталогов приложений), которая показана на рис. 8.3, укажите, требуется ли создавать раздел каталогов приложений. Если приложение, которое планируется устанавливать, предусматривает создание собственного раздела, оставьте выбранным переключатель No, do not create and application directory partition (Нет, не создавать раздел каталогов приложений). Если раздел для хранения объектов приложения должен быть создан вручную, выберите переключатель Yes, create and application directory partition (Да, создать раздел каталогов приложение) и в отображаемом ниже поле введите желаемое имя этого раздела в уточненном формате (т.е. `CN=PartitionName,DC=domain,DC=com`). Для продолжения щелкните на кнопке Next.
14. На странице File Locations (Размещение файлов) выберите, где должны храниться данные и файлы восстановления данных для AD LDS, и щелкните на кнопке Next.
15. На странице Service Account Selection (Выбор учетной записи службы) укажите, должна ли в качестве учетной записи службы для данного экземпляра AD LDS использоваться учетная запись сетевой службы (она применяется по умолчанию), и щелкните на кнопке Next.
16. На следующей странице выберите конкретного пользователя или группу пользователей, которые должны являться администраторами для данного экземпляра AD LDS. Рекомендуется выбрать группу. После установки переключателя This Account (Эта учетная запись) и добавления группы щелкните на кнопке Next.

Рис. 8.3. *Настройка раздела каталогов приложений для AD LDS*

17. На странице Importing LDIF Files (Импорт LDIF-файлов), которая показана на рис. 8.4, выберите специальные LDIF-файлы для импорта. Эти LDIF-файлы предназначены для специфических сценариев, требующих AD LDS, таких как сценарий создания в AD LDS пользователей. В рассматриваемом примере будет импортироваться файл `MS-User.LDF`, чтобы потом иметь возможность создавать в данном экземпляре AD LDS объекты классов. Отметив соответствующий флажок, щелкните на кнопке Next.

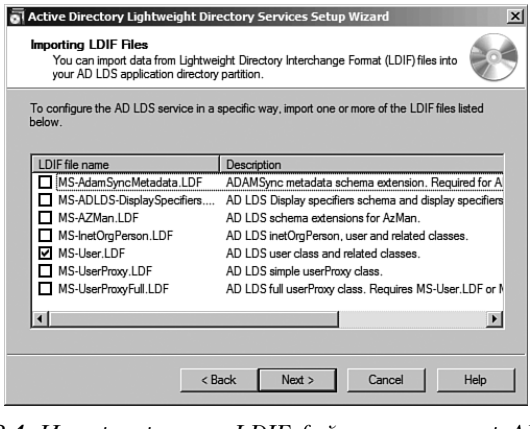

Рис. 8.4. *Импортирование LDIF-файлов в экземпляр AD LDS*

18. На итоговой странице проверьте выбранные варианты и параметры и щелкните на кнопке Next, чтобы запустить процесс создания экземпляра AD LDS.
19. По завершении мастером процесса создания экземпляра AD LDS щелкните на кнопке Finish (Готово).

После создания экземпляра AD LDS для его администрирования можно использовать низкоуровневую утилиту для работы с каталогами под названием ADSIEdit, которая доступна в меню Administrative Tools (Администрирование). В этой утилите необходимо выбрать в меню Action (Действие) пункт Connect To (Подключиться к) и ввести для установки подключения имя нужного экземпляра (в рассматриваемом примере `ADLDS1`). Затем сле-

дует ввести контекст именования для той точки подключения, которая была создана для экземпляра во время прохождения шагов мастера (`CN=adlds1,DC=companyabc,DC=com`), а также имя локального сервера и специальный порт, который был указан для компьютера (`dc2:50000`), как показано на рис. 8.5.

Хотя пользоваться утилитой ADSIEdit гораздо труднее, чем полнофункциональной оснасткой Active Directory Users and Computers (Active Directory — пользователи и компьютеры), она является очень мощной и позволяет выполнять все необходимые процедуры по администрированию контекста именования экземпляров AD LDS. Кроме того, для работы с AD LDS могут применяться интерфейсы специальных приложений, которые позволяют более просто выполнять администрирование экземпляров AD LDS.

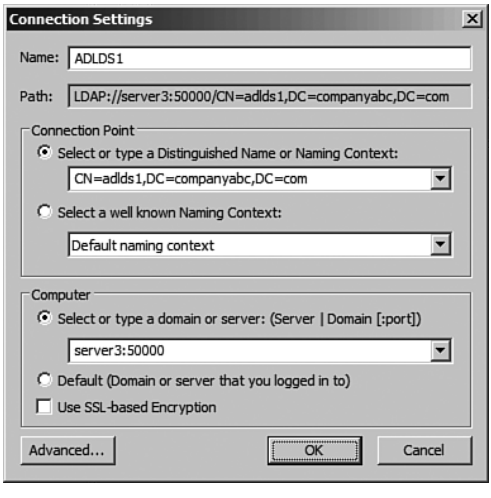

Рис. 8.5. *Подключение к экземпляру AD LDS*

Технология Active Directory Federation Services

Технология Active Directory Federation Services (Службы федерации Active Directory), или AD FS, обеспечивает возможность единого входа (Single Sign-On — SSO) между несколькими платформами, включая среды, отличные от Microsoft. Управляя используемыми идентификационными данными входа в систему и связывая их вместе посредством применяемой для входа в Windows системы аутентификации, организации могут более легко управлять доступом клиентов к веб-приложениям без компрометации внутренней инфраструктуры безопасности.

Для работы с AD FS применяется консоль администрирования MMC, которая показана на рис. 8.6 и может устанавливаться только на системе, функционирующей под управлением либо Windows Server 2008 R2 Enterprise Edition, либо Windows Server 2008 R2 Datacenter Edition.

AD FS не заменяет собой такую технологию, как Forefront Identity Manager (ILM), которая представляет собой продукт для синхронизации каталогов и более подробно рассматривается позже в этой главе. Вместо того чтобы синхронизировать идентификационные данные между различными каталогами, как это делает FIM, ADS FS управляет предпринимаемыми из различных каталогов попытками получения доступа к веб-приложениям. Это очень важно понимать, поскольку AD FS и FIM исполняют в среде организации совершенно разные роли.

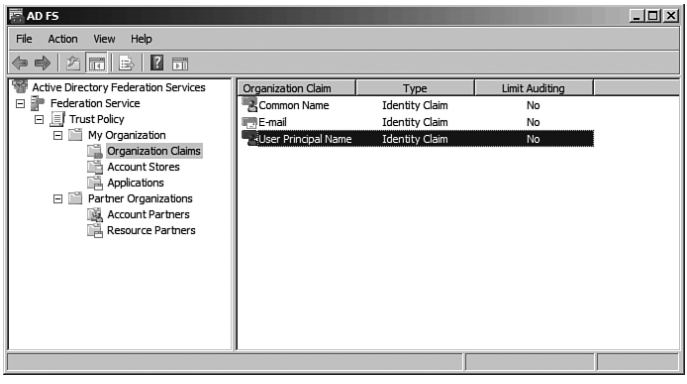

Рис. 8.6. *Просмотр AD FS в консоли MMC*

Обзор ключевых компонентов AD FS

AD FS состоит из трех следующих серверных компонентов.

- **Компонент Federation Server (Сервер федерации)**. Этот компонент является главным компонентом AD FS, в котором содержится роль Federation Service (Служба федерации). Он позволяет серверам маршрутизировать аутентификационные запросы между связанными каталогами.
- **Компонент Federation Proxy Server (Прокси-сервер федерации)**. Этот компонент позволяет серверам выступать в роли инвертированных прокси-серверов для аутентификационных запросов AD FS. Серверы такого типа обычно размещаются в демилитаризованной зоне брандмауэра и применяются для защиты прикладных серверов AD FS от прямого воздействия со стороны ненадежных узлов Интернета.
- **Компонент AD FS Web Agents (Веб-агенты служб федерации AD FS)**. Этот компонент AD FS отвечает за обслуживание агентов, поддерживающих утверждения (Claims-aware Agent), и агентов, использующих маркеры безопасности Windows (Windows Token-based Agent) и управляющих аутентификационными cookie-наборами, которые отправляются приложениям веб-серверов.

Эти компоненты могут устанавливаться как по отдельности в структуре AD FS, так и все вместе на одной и той же системе.

Установка AD FS в Windows Server 2008 R2

Ниже перечислены шаги, необходимые для выполнения установки роли AD FS на сервере Windows Server 208 R2.

1. Откройте на сервере приложение Server Manager (Диспетчер сервера) (выбрав в меню Start (Пуск) пункт All Programs⇨Administrative Tools⇨Server Manager (Все программы⇨Администрирование⇨Диспетчер сервера)).
2. Щелкните на узле Roles (Роли), а затем на ссылке Add Roles (Добавить роли).
3. На странице Before You Begin (Перед началом работы) просмотрите все отображающиеся примечания и для продолжения щелкните на кнопке Next (Далее).
4. В списке ролей сервера выберите вариант Active Directory Federation Services (Службы федерации Active Directory), отметив соответствующий флажок, и щелкните на кнопке Next.

5. На странице Introduction to Active Directory Federation Services (Вводные сведения о службах федерации Active Directory) просмотрите отображающуюся информацию и для продолжения щелкните на кнопке Next.
6. На странице Select Role Services (Выбор служб ролей) выберите подлежащие установке роли, как показано на рис. 8.7. При выполнении щелчка на ролях может появляться сообщение с приглашением установить дополнительные компоненты, необходимые для работы этой роли. Например, для своей работы роль Federation Service (Служба федерации) требует IIS и несколько других компонентов. Если подобное приглашение появится, щелкните в нем на соответствующей кнопке, чтобы установить все необходимые дополнительные компоненты. После выбора всех требуемых ролей щелкните на кнопке Next.

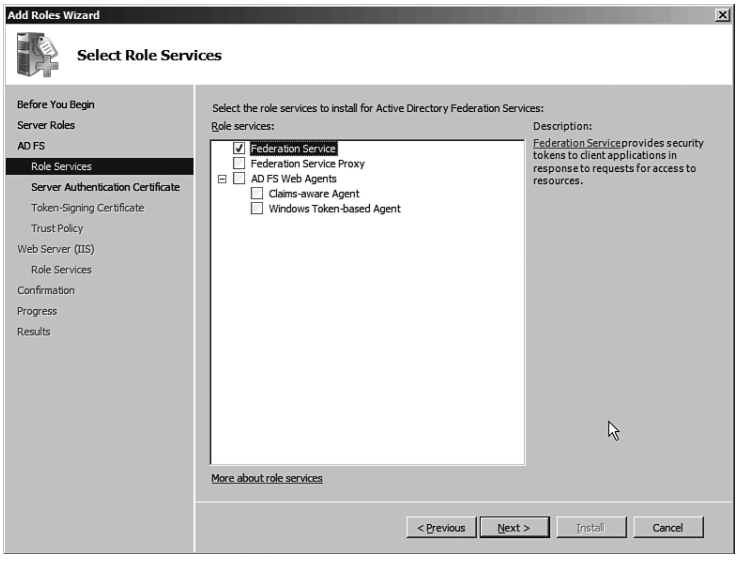

Рис. 8.7. *Установка роли Active Directory Federation Services*

7. На следующей странице укажите, должен ли быть создан новый аутентификационный сертификат для сервера или необходимо использовать какой-то существующий. Поскольку SSL-шифрование является обязательным для AD FS, для установки AD FS нужно использовать сертификат, заверенный либо надежным внутренним центром сертификации, либо проверенным внешним органом сертификации (последний вариант является наиболее распространенным). Если подходящий сертификат уже доступен и его требуется просто установить на сервере локальным образом, щелкните на кнопке Import (Импортировать). Сделав выбор, щелкните на кнопке Next. В случае установки AD FS только в целях тестирования выберите переключатель Create a Self-Signed Certificate (Создать самозаверяющий сертификат) и щелкните на кнопке Next.
8. На следующей странице выберите сертификат для подписи маркера (token-signing certificate), выполнив ту же процедуру, что и в предыдущем шаге. Этот сертификат тоже можно получить как от внутреннего центра сертификации (если таковой доступен), так и от внешнего поставщика сертификатов путем импорта. В случае установки AD FS только в целях тестирования выберите переключатель Create a Self-Signed Token-Signing Certificate (Создать самозаверяющий сертификат для подписи маркера). Сделав выбор, щелкните на кнопке Next.

9. На странице Select Trust Policy (Выбор политики доверия) укажите, должна ли быть создана совершенно новая политика доверия для типа применяемых в организации утверждений (claims) или же использоваться существующая (рис. 8.8), и щелкните на кнопке Next.

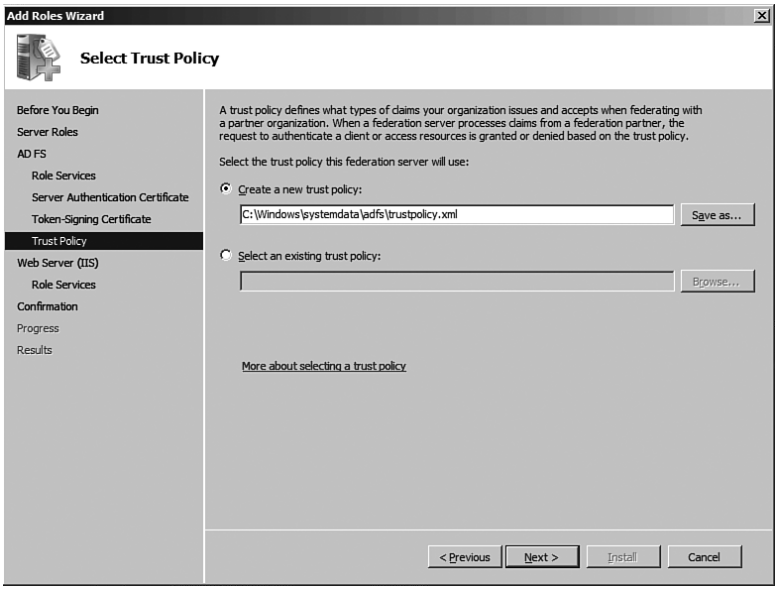

Рис. 8.8. *Выбор политики доверия для AD FS*

10. Если для установки были также выбраны какие-то дополнительные компоненты вроде IIS, мастер добавления ролей (Add Roles Wizard) далее начнет предлагать на выбор варианты для этих ролей. Следуйте шагам мастера до тех пор, пока в мастере не появится кнопка Install (Установить), после чего щелкните на этой кнопке, чтобы запустить процесс установки AD FS.
11. Когда мастер завершит процесс установки AD FS, щелкните на кнопке Close (Закрыть).

Работа с AD FS

AD FS работает за счет ввода информации о подключаемых партнерах, таких как леса AD или организации AD LDS, и сведений о конкретных партнерах и приложениях. Каждый фрагмент информации может вводиться путем запуска соответствующих мастеров, которые автоматически устанавливаются AD FS и описаны ниже.

- **Мастер добавления партнеров по ресурсам (Add Resource Partner Wizard)**. Этот мастер позволяет либо создавать партнеров по ресурсам вручную, либо импортировать их автоматически за счет использования файла XML (Extensible Markup Language — расширяемый язык разметки). В партнерах по ресурсам содержится информация о конкретных веб-приложениях, к которым пользователи могут получать доступ.
- **Мастер добавления партнеров по учетным записям (Add Account Partner Wizard)**. Этот мастер позволяет добавлять информацию о конкретных партнерах по учетным записям, которые представляют собой подключаемые запросчики маркеров доступа (security token issuers), такие как контроллеры доменов.

- **Мастер добавления приложений (Add Applications Wizard)**. Этот мастер позволяет добавлять в AD FS специфические поддерживающие утверждения (claims-aware) приложения.

Благодаря вводу информации о различных веб-приложениях и о том, каким каталогам и пользователям должен предоставляться доступ, AD FS обеспечивает возможность единого входа в разные каталоги. Это очень ценное преимущество для организации, желающей обмениваться корпоративной информацией с проверенными партнерами, не подвергая при этом свои важные внутренние активы нежелательному обозрению.

Синхронизация информации каталогов с помощью Forefront Identity Manager (FIM)

Сегодня на большинстве предприятий у каждого отдельного приложения или системы имеется собственная база данных пользователей или каталог для отслеживания того, кому разрешено пользоваться ресурсом. Данные, касающиеся идентификации и управления доступом, размещаются в разных каталогах. Это же относится и к таким приложениям, как специализированные каталоги сетевых ресурсов, почтовые серверы, программы для отдела кадров, обработки голосовой почты, генерации платежных ведомостей и т.д.

На каждом предприятии под идентификационными данными пользователя подразумевается что-то свое (например, имя пользователя, должность, идентификационные номера, роли и информация о членстве в группах). На многих предприятиях для аутентификации пользователей применяется собственная подсистема паролей и процессов. На каждом имеется свое собственное средство для управления учетными записями пользователей, а иногда даже отдельный ответственный за это администратор. Помимо этого, на большинстве предприятий применяется множество процессов для запроса ресурсов и для предоставления и модификации прав доступа. Некоторые из этих процессов являются автоматизированными, но многие все-таки выполняются вручную. В каждом подразделении они выглядят по-разному, даже несмотря на то, что исполняют одну и ту же функцию.

Администраторам этих многочисленных репозиториев зачастую приходится тратить массу времени и излишних усилий на их администрирование и подготовку к работе. Пользователям это также доставляет неудобства, поскольку им приходится запоминать множество идентификаторов и паролей для различных приложений и систем. Чем больше организация, тем потенциально больше количество различных репозиториев и усилий, которые требуется прикладывать для их поддержания в актуальном состоянии.

В ответ на эту проблему в Microsoft разработали продукт под названием Microsoft Metadirectory Services (Службы метакаталогов), или MMS, который призван обеспечивать синхронизацию идентификационной информации между различными каталогами. После усовершенствования этот продут был выпущен под новым названием Microsoft Identity Integration Server (Сервер интеграции идентификационных данных Microsoft), или MIIS. Чуть позже он был снова переименован, на этот раз в Identity Lifecycle Manager (Диспетчер жизненного цикла идентификационных данных), или ILM. Последнее, четвертое переименование этого продукта произошло незадолго до выпуска версии Exchange Server 2010, с выходом которой Microsoft включила этот продукт в состав линейки средств для обеспечения безопасности под общим наименованием Forefront. Он стала называться Forefront Identity Manager (Диспетчер идентификационных данных переднего края), или FIM.

Применение FIM для Exchange Server 2010 особенно выгодно, поскольку позволяет обеспечить синхронизацию информации между лесом AD, в котором содержится Exchange, и другими системами обмена сообщениями, которые также используются в организации.

Что собой представляет FIM

Продукт FIM представляет собой систему, которая управляет и координирует идентификационной информацией из многочисленных существующих в организации источников данных и тем самым позволяет объединять эту информацию в одно логическое представление, отражающее всю идентификационную информацию по тому или иному пользователю или ресурсу.

FIM дает возможность компании синхронизировать идентификационные данные среди множества различных гетерогенных каталогов и хранилищ идентификационной информации и тем самым автоматизировать для клиентов процесс обновления их идентификационных данных среди гетерогенных платформ, сохраняя при этом их целостность и принадлежность по всему предприятию.

Предлагаемые в FIM возможности для управления паролями позволяют конечным пользователям или персоналу службы поддержки легко сбрасывать пароли на множестве систем с помощью одного удобного веб-интерфейса. Благодаря им, конечным пользователям и сотрудникам служб поддержки больше не нужно применять многочисленные средства для того, чтобы менять свои пароли сразу во множестве систем.

Концепции, связанные с FIM

Прежде чем разбираться с тем, как применять FIM для интеграции различных каталогов, важно ознакомиться с ключевыми терминами, которые используются в этом продукте. Следует иметь в виду, что перечисленные ниже термины описывают используемые в FIM понятия, но могут также помочь получить более широкое представление о том, как в целом функционируют метакаталоги. Ниже перечислены основные концепции, которые нужно знать для того, чтобы работать с FIM.

- **Агент управления (Management Agent — MA)**. Агентом управления в FIM называется средство, используемое для взаимодействия с каталогом конкретного типа. Например, агент управления Active Directory позволяет FIM импортировать и экспортировать данные, а также выполнять другие задачи в Active Directory.
- **Подключенный каталог (Connected Directory — CD)**. Подключенным каталогом называется каталог, с которым FIM взаимодействует за счет использования соответствующего сконфигурированного агента управления. Например, в роли подключенного каталога может выступать лес Acitve Directory.
- **Пространство имен соединителя (Connector Namespace — CS)**. Под пространством имен соединителя подразумевается иерархия реплицируемой информации и контейнеров, которая либо извлекается из соответствующего подключенного каталога, либо направляется в него.
- **Пространство имен метастрок (Metaverse Namespace — MV)**. Под пространством имен метастрок подразумеваются авторитетные данные каталога, которые создаются на основе информации, собираемой из пространств имен всех соответствующих соединителей.
- **Метакаталог (Metadirectory)**. В FIM в состав метакаталога входят пространства имен всех соединителей плюс авторитетное пространство имен метастрок.
- **Атрибуты (Attributes)**. Атрибутами называются поля информации, которые экспортируются из записей каталогов или импортируются в них. К числу наиболее распространенных атрибутов записей каталогов относятся имя, псевдоним, адрес электронной почты, номер телефона, табельный номер и т.д.

FIM может применяться для решения многих задач, но чаще всего используется для управления идентификационными данными каталогов. Это предполагает управление учетными записями пользователей за счет синхронизации атрибутов, таких как идентификатор для входа в систему, имя, фамилия, номер телефона, наименование должности и название отдела. Например, если пользователь по имени Jane Doe получает повышение в должности от менеджера до вице-президента, изменение должности может сначала быть занесено в базы данных отдела кадров и бухгалтерии, а затем с помощью агентов управления автоматически реплицировано во все остальные каталоги организации. Это дает уверенность в том, что если кому-то позже понадобится просмотреть атрибут названия должности пользователя Jane Doe, он будет выглядеть одинаково во всех каталогах, которые синхронизируются с помощью FIM. Такой способ применения FIM является наиболее распространенным и называется *управлением идентификацией* (identity management). К числу других распространенных способов использования FIM относятся инициализация учетных записей и управление группами.

НА ЗАМЕТКУ

FIM представляет собой очень многостороннее и мощное средство для синхронизации каталогов, которое может применяться для упрощения и автоматизации некоторых связанных с управлением каталогами задач. Однако из-за своей природы FIM может также быть очень опасным средством в случае предоставления агентам управления полного доступа к подключенным каталогам. Неправильная настройка агентов управления в FIM может приводить к утрате данных, поэтому перед внедрением FIM в производственной среде должно обязательно проводиться тщательное планирование этого процесса и обширное его тестирование в лабораторной среде. Во многих случаях может быть целесообразнее связаться с консультирующими службами в Microsoft и сертифицированными партнерами или поставщиками продуктов Microsoft для выяснения того, подходит ли FIM для реализации в конкретной среде, или даже для проектирования и упрощения процесса внедрения этого продукта.

Инициализация учетных записей с помощью FIM

FIM позволяет администраторам легко производить инициализацию (provisioning) и деинициализацию (deprovisioning), т.е. централизованное добавление и удаление учетных записей и идентификационной информации пользователей, включающей членство в группах рассылки, электронной почты и безопасности, среди множества систем и платформ. В частности, FIM позволяет администраторам быстро создавать новые учетные записи для сотрудников на основе событий или изменений в авторитетных хранилищах, таких как система отдела кадров, а в случае увольнения сотрудников — немедленно удалять использованные ими учетные записи из тех же систем.

Инициализация учетных записей в FIM предоставляет возможность применять усовершенствованные конфигурации агентов управления каталогами вместе со специальными агентами инициализации для автоматизации процесса создания и удаления учетных записей в нескольких каталогах. Например, в случае создания новой учетной записи пользователя в Active Directory агент управления Active Directory (Active Directory MA) может снабдить эту учетную запись специальным дескриптором (tag). При запуске соответствующих агентов управления для других подключенных каталогов аналогичная учтенная запись может генерироваться в них автоматически.

Одно из важных улучшений в FIM по сравнению с предыдущими версиями этого продукта связано с тем, что синхронизация паролей теперь поддерживается для конкретных каталогов, в которых предусмотрено управление паролями. FIM предоставляет для этого

специальный API-интерфейс, доступ к которому можно получить через интерфейс WMI (Windows Management Instrumentation — инструментарий управления Windows). Для подключаемых каталогов, в которых предусмотрено управление паролями, функция управления паролями активизируется при настройке агента управлении в средстве MA Designer (Конструктор агентов управления). Помимо включения функции управления паролями для каждого агента управления, Management Agent Designer с помощью интерфейса WMI возвращает для каждого объекта, представляющего пространство соединителя, атрибут имени системы.

Роль агентов управления в FIM

Агент управления (Management Agent) связывает конкретный подключенный источник данных с метакаталогом. Он, по сути, отвечает, за перемещение данных между подключенным источником данных и метакаталогом. При изменении данных в метакаталоге он может экспортировать данные в подключенный источник данных для поддержания того в синхронизированном с метакаталогом состоянии. Обычно для каждого подключаемого каталога создается как минимум один агент управления. В общем случае в FIM допускается создавать агенты управления для многих источников каталогов, как показано на рис. 8.9.

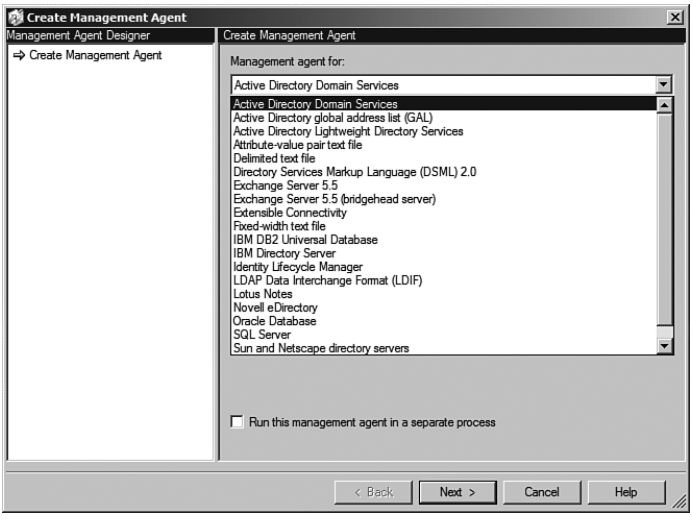

Рис. 8.9. *Потенциальные агенты управления для FIM*

НА ЗАМЕТКУ

Кроме того, в FIM предлагается интегрированная поддержка для обеспечения синхронизации с дополнительными каталогами, такими как SAP, Oracle, IBM и Sun, а также возможность сброса конечными пользователями собственных паролей с помощью специального веб-интерфейса.

В агентах управления содержатся правила, которые указывают, каким образом должны сопоставляться атрибуты объекта, как объекты подключенных каталогов должны отыскиваться в пространстве имен метастрок (metaverse) и когда объекты подключенных каталогов должны создаваться или удаляться.

По сути, эти агенты позволяют настраивать способ, по которому FIM должен связываться и взаимодействовать с подключенными каталогами при запуске этих агентов. Все операции по конфигурированию агента можно выполнять прямо при создании его первого экземпляра. К числу элементов, которые можно конфигурировать, относятся типы объектов каталога, которые должны реплицироваться в пространство имен соединителя, подлежащие репликации атрибуты, правила объединения и проецирования элементов каталогов, правила потока атрибутов между пространством имен соединителя и пространством имен метастрок и т.д. Если при создании агента управления необходимая для него конфигурация неизвестна, необходимые конфигурационные изменения можно внести позже.

Управление группами с помощью FIM

Помимо задач, связанных с управлением идентификационными данными учетных записей, FIM может также применяться для решения задач, связанных с управлением группами. При проектировании группы на пространство имен метастрок атрибут членства в этой группе может реплицироваться в другие подключенные каталоги через их агенты управления. В результате изменение, внесенное в данные о членстве в группах в одном каталоге, автоматически реплицируется в другие каталоги.

Установка FIM с SQL Server 2005/2008

FIM для работы требуется лицензионная версия SQL Server 2005 или SQL Server 2008 и в ходе процесса установки этого продукта будет обязательно запрашиваться местонахождение сервера SQL.

Устанавливать новый экземпляр SQL не обязательно, поскольку может использоваться существующая копия SQL Server. Если сервер SQL Server 2005 или SQL Server 2008 отсутствует, его понадобится установить в той же системе, что и FIM.

Использование мощи и потенциала FIM

FIM является функциональным и мощным средством. В случае правильной настройки и написания нескольких хорошо продуманных сценариев FIM может выполнять огромное количество самых разнообразных задач автоматическим образом. В современных средах используется масса каталогов, что увеличивает объем усилий, которые требуется прикладывать администраторам для создания учетных записей, их удаления и обновления пользовательских данных вручную. FIM может значительно снизить объемы этих усилий и улучшить качество администрирования и степень безопасности. В следующем разделе рассказывается о некоторые наиболее ценных возможностях FIM и том, как их эффективно использовать.

Управление идентификационными данными с помощью FIM

FIM подходит для большинства базовых и простейших конфигураций. Например, FIM может применяться для синхронизации идентификационных данных между учетными записями, находящимися в разных каталогах. В эти идентификационные могут входить имена пользователей, их электронные и почтовые адреса, наименование их должностей, названия отделов, в которых они работают, и т.д. В сущности, идентификационные данные представляют собой такие сведения, которые постоянно встречаются в корпоративных телефонных книгах или внутренних сетях. Ниже перечислены шаги, необходимые для обеспечения управления идентификационными данными между Active Directory и сервером каталогов LDAP с помощью FIM.

1. Установите поставляемый в составе FIM компонент Metadirectory Services (Службы метакаталогов).
2. Создайте для каждого из каталогов отдельный агент управления (management agent — MA), в том числе агент управления Active Directory и агент управления LDAP.
3. Сконфигурируйте агенты управления так, чтобы они предусматривали импорт типов объектов каталогов в пространства имен соответствующих соединителей.
4. Настройте один из агентов управления, например, Active Directory MA, чтобы объекты каталогов из пространства соответствующего ему соединителя и иерархия каталогов проектировались на пространство имен метастрок (Metaverse Namespace — MV).
5. При желании сконфигурируйте внутри каждого из агентов управления функцию потока атрибутов (Attribute Flow) для указания того, какие из атрибутов объектов каталога в каждом каталоге должны проектироваться на соответствующие объекты каталога метастрок. Настройте правила потока атрибутов для каждого агента управления.
6. Сконфигурируйте для объектов каталогов свойства присоединения к учетным записям. Этот шаг является наиболее важным, поскольку именно он будет определять то, как объекты в каждом каталоге будут соотноситься друг с другом внутри пространства имен метастрок. Для конфигурирования этих свойств можно использовать конкретные критерии, вроде идентификатора сотрудника или комбинации и из его имени и фамилии. Главное — подобрать наиболее уникальную комбинацию, чтобы избежать проблем, связанных с обнаружением двух объектов с похожими именами, которые могут появиться, например, из-за существования в Active Directory двух пользователей по имени Tom Jones.
7. Завершив настройку агентов управления (MA) и правил присоединения данных к учетным записям (account joins), сконфигурируйте профили выполнения этих агентов и укажите им в этих профилях, что они должны делать с подключенным каталогом и пространством имен соединителя. Например, можно указать, что они должны импортировать или экспортировать все данные. При первом запуске агента управления всегда производится импорт информации из подключенного каталога для создания первичного пространства имен соединителя.
8. После первого запуска агентов управления они могут быть запущены второй раз для распространения авторитетных данных из пространства имен метастрок по пространствам имен соответствующих соединителей и затем — по подключенным каталогам.

Эти шаги могут применяться для упрощения задач, связанных с обслуживанием учетных записей, если необходимо управление сразу несколькими каталогами одновременно. Помимо управления идентификационными данными учетных записей пользователей FIM может также использоваться и для выполнения задач, связанных с обслуживанием целых групп. При проектировании группы на пространство имен метастрок атрибут членства в группах может реплицироваться в другие подключенные каталоги посредством уже их агентов управления. В результате изменения, внесенные в данные членства в группах в одном каталоге, будут автоматически реплицироваться в остальные каталоги.

Инициализация и деинициализация учетных записей с помощью FIM

Под инициализацией (provisioning) учетных записей в FIM подразумевается расширенная настройка агентов управления каталогами вместе со специальными агентами инициализации (provisioning agents) для автоматизации процесса создания и удаления учетных записей в нескольких каталогах. Например, в случае создания в Active Directory новой учет-

ной записи пользователя агент управления Active Directory может пометить ее каким-то особым образом, а агенты управления других каталогов при запуске автоматически сгенерируют аналогичную учетную запись в других обслуживаемых ими каталогах.

Процесс инициализации и деинициализации учетных записей в FIM является чрезвычайно полезным средством в ситуациях, когда требуется, чтобы создание и удаление пользовательских учетных записей производилось автоматическим образом. Например, создание в базе данных учета кадров Oracle одной учетной записи может автоматически повлечь за собой целую цепочку событий по созданию аналогичных учетных записей в других местах, как показано на рис. 8.10.

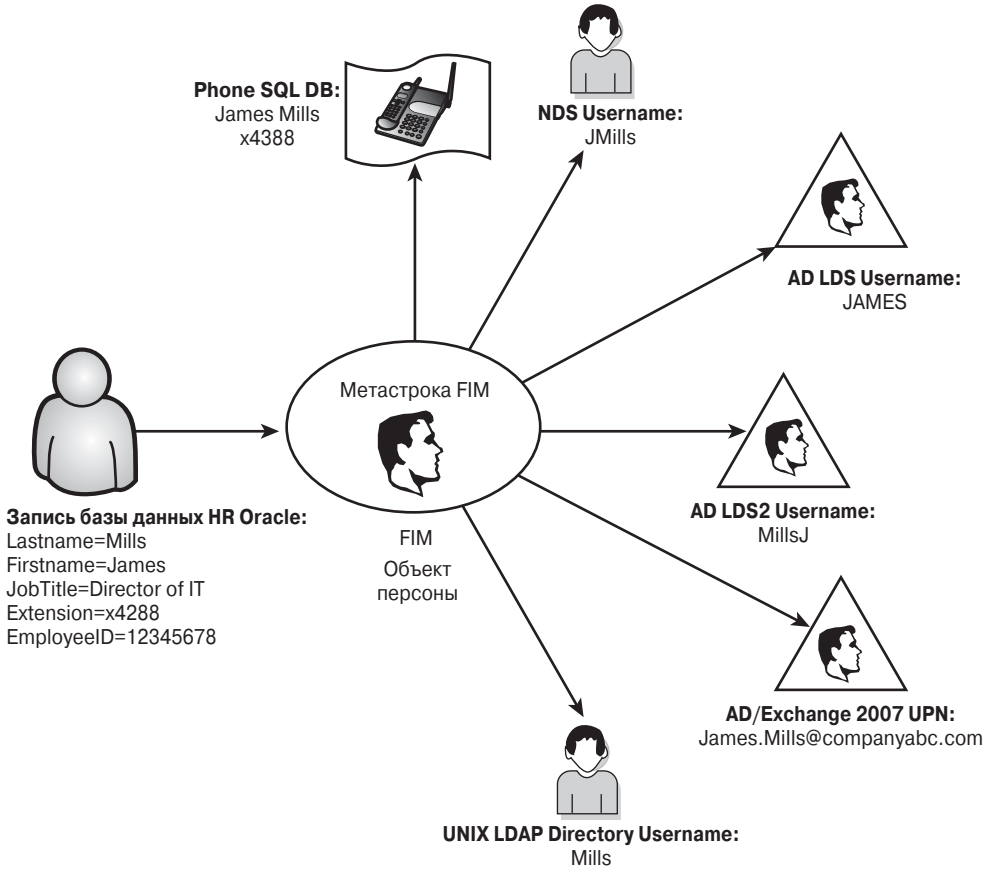

Рис. 8.10. *Инициализация учетных записей с помощью FIM*

Кроме того, связанные учетные записи пользователей могут в FIM не только автоматически создаваться с помощью процесса инициализации, но и автоматически удаляться или отключаться через процесс деинициализации (deprovisioning). Автоматизация процесса удаления связанных учетных записей упрощает администрирование массы учетных записей в организации, а также сводит к минимуму риск случайного оставления действующей учетной записи после увольнения сотрудника.

Ниже приведен общий пример, демонстрирующий, какие шаги необходимо выполнить для настройки простого процесса инициализации учетных записей. В этом примере

предполагается, что к FIM требуется подключить домен AD DS, а также, что для всех создаваемых в этом домене учетных записей пользователей в отдельном лесу ресурсов Active Directory должны автоматически создаваться соответствующие почтовые ящики Exchange. Ниже перечислены шаги, которые потребуется выполнить.

1. Установите FIM.
2. Создайте агент управления для подключаемого домена AD DS.
3. Сконфигурируйте агент управления AD DS так, чтобы атрибуты, необходимые для создания почтовых ящиков ресурсов, поступали в пространство имен метастрок.
4. Настройте поток атрибутов между атрибутами агента управления AD DS и пространством имен метастрок FIM.
5. Создайте дополнительный агент управления для домена AD DS Exchange Resource.
6. Удостоверьтесь в том, что атрибуты агента управления AD DS Exchange Resource (контейнер типов объектов, группа, `inetOrgPerson`, `organizationUnit` и имя пользователя), которые будут необходимы FIM для создания почтовых ящиков, установлены.
7. Создайте с помощью Visual Studio специальную DLL-библиотеку расширения правил (Rules Extension DLL), которая должна будет применяться при автоматическом создании учетных записей с почтовыми ящиками в лесу ресурсов. В данном случае эта DLL-библиотека должна использовать в сценарии класс `MVExtensionExchange`.
8. Установите эту DLL-библиотеку в пространстве имен метастрок.
9. Сконфигурируйте профили выполнения так, чтобы они предусматривали импорт информации и автоматическое создание почтовых ящиков.

Описанный выше пример, хотя и является сложным, очень полезен в ситуациях, когда один и тот же лес Exchange Server используется множеством организаций. Идентификатор безопасности (SID) учетной записи AD DS может импортироваться в пространство имен метастрок и использоваться для создания почтового ящика в лесу ресурсов, имеющем внешнюю учетную запись под названием Associated External Account (Связанная внешняя учетная запись). Централизованная реализация FIM позволяет лесу ресурсов Exchange поддерживать автоматическое создание почтовых ящиков ресурсов для большого количества подключенных доменов.

Резюме

Active Directory как платформа имеет много мощных средств для централизации и хранения информации о пользователях и других объектах в организации. Однако эффективность этих средств существенно снижается, если поддерживается множество платформ каталогов, у каждой из которых имеется свой набор пользователей и атрибутов. Такие средства от Microsoft, как продукт Forefront Identity Manager (FIM), предоставляют администраторам возможность обеспечивать синхронизацию данных между разными каталогами и тем самым поддерживать информацию организации среди множества платформ в стандартизированном виде.

Помимо технологий для синхронизации каталогов вроде FIM, компания Microsoft также предлагает поддержку и для таких продуктов, как AD FS и AD LDS, которые позволяют организациям упрощать процедуры аутентификации идентификационных данных и создавать персональные каталоги для приложений. Правильно используя эти технологии, организации могут получить гораздо больше преимуществ, чем при использовании множества традиционных распределенных технологий.

Полезные советы

Ниже перечислены полезные советы этой главы.

- Используйте продукт FIM для поддержания множества разрозненных каталогов в синхронизированном состоянии.
- Применяйте экземпляры AD LDS для приложений, которые требуют внесения специальных изменений в схему, и поддерживайте информацию в этих экземплярах AD LDS в синхронизированном с центральной платформой AD DS состоянии с помощью FIM.
- Для добавления на сервер ролей AD FS и AD LDS используйте приложение Server Manager (Диспетчер сервера).
- Применяйте технологию AD FS для поддержки возможности единого входа в систему (Single Sign-On) среди множества платформ.
- Для автоматизации процессов инициализации и деинициализации учетных записей пользователей рассмотрите вариант использования продукта FIM. За счет установки строгой политики относительно деинициализации (уничтожения) недействительных учетных записей можно добиться в целом более высокой степени безопасности.
- Для сокращения степени подверженности сервера атакам рассмотрите вариант развертывания AD LDS в рамках Windows Server 2008 R2 Server Core.