Лекция №6. ACTIVE DIRECTORY WINDOWS SERVER

Учебные вопросы:

1. Эволюция службы каталогов
2. Структура службы ADDS
3. Компоненты ADDS
4. Определение организационных единиц домена
5. Роль DNS и безопасность в ADDS

Вопрос №1. Эволюция службы каталогов

Служба каталогов в той или иной форме существовала с самого начала эпохи компьютеров - для **обычного поиска файлов** и **для аутентификации** в реализациях производственных сетей.

Служба каталогов **предоставляет** подробную информацию о **пользователях** или **объектах сети**, примерно так же, как телефонная книга позволяет найти номер телефона по известной фамилии.

Первые электронные каталоги были созданы вскоре после изобретения цифровых компьютеров и применялись для **аутентификации пользователей** и **управления доступом** к ресурсам.

Примерами ранних каталогов могут служить

MVS PROFS (IBM),

база регистрационных данных Grapevine

WHOIS.

Вскоре появились **специализированные службы каталогов** для специального поиска и ведения контактной информации для **конкретных программных продуктов**. Доступ к таким каталогам был возможен только с помощью специальных методов, а область их применения была ограниченной.

Дальнейшее развитие крупномасштабных служб каталогов для предприятий возглавила компания Novell, выпустив в начале девяностых годов прошлого века **службу каталогов Novell Directory Services** (NDS). Она была принята организациями NetWare, а затем в нее была включена поддержка смешанных сред **NetWare/NT**.

Линейная структура **доменов NT** и отсутствие синхронизации и взаимодействия этих двух сред заставила многие организации перейти **на использование NDS** в качестве реализации службы каталогов. Именно **эти недостатки NT** были основной причиной выпуска службы **ADDS** компанией Microsoft.

Разработка **облегченного протокола доступа к каталогам** (Lightweight Directory Access Protocol - **LDAP**) была вызвана ростом сети Интернета и необходимостью более тесного взаимодействия и строгой стандартизации.

Этот **общепринятый метод доступа** к информации каталогов и ее модификации использовал все возможности протокола TCP/IP, оказался надежным и функциональным, и для его применения были разработаны новые реализации служб каталогов. Сама служба AD DS разрабатывалась так, чтобы соответствовать стандарту LDAP.

Основные характеристики доменной службы Active Directory

Совместимость с TCP/IP. В отличие от ряда специализированных протоколов вроде IPX/SPX и NetBEUI, протокол TCP/IP с самого начала создавался межплатформенным. Последующее принятие TCP/IP в качестве Интернет-стандарта для обмена данными сделало его одним из лидеров в мире протоколов и, по сути, превратило в обязательный протокол для операционных систем уровня предприятия. В AD DS и Windows Server **стек протоколов TCP/IP** используется в качестве **основного метода** для обмена данными.

Основные характеристики доменной службы Active Directory

Поддержка протокола LDAP. Протокол LDAP (Lightweight Directory Access Protocol - облегченный протокол доступа к каталогам) был разработан в качестве стандартного Интернет-протокола для доступа к каталогам. Он применяется для **обновления** и **запросов данных**, хранящихся в каталогах. Служба AD DS непосредственно **поддерживает** LDAP.

Поддержка системы доменных имен. Система доменных имен (Domain Name System - DNS) была создана для преобразования упрощенных имен, понятных людям (таких как www.cco.com), в IP-адреса, понятные компьютерам (вроде 12.222.165.154). В AD DS она **поддерживается** и даже **требуется** для нормальной работы.

Основные характеристики доменной службы Active Directory

Поддержка безопасности. Поддержка безопасности в соответствии со стандартами Интернета чрезвычайно важна для бесперебойного функционирования среды, к которой подключены миллионы компьютеров по всему миру. Отсутствие надежных средств защиты привлекает хакеров, поэтому в Windows Server и AD DS средства безопасности были значительно расширены.

Так, в Windows Server и AD DS была встроена непосредственная **поддержка IPSec**, **Kerberos**, **центров сертификации** и **шифрования** с помощью протокола защищенных сокетов (Secure Sockets Layer - **SSL**).

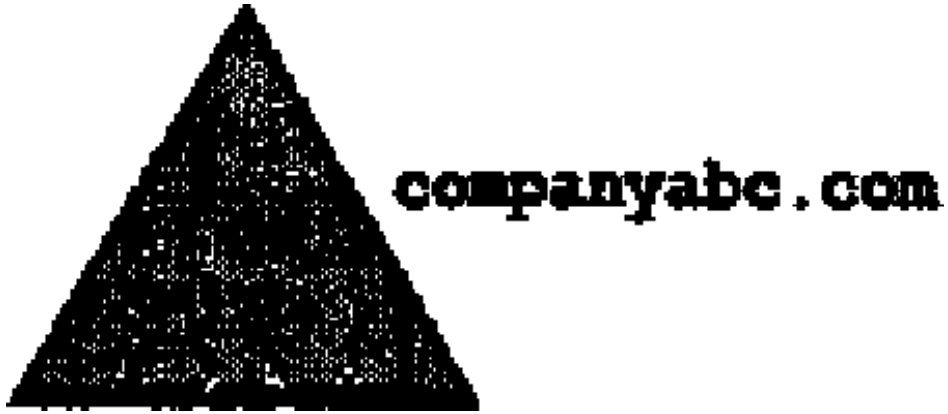
Основные характеристики доменной службы Active Directory

Легкость администрирования. Для улучшения администрирования AD DS в Windows Server добавлены компоненты Active Directory Administration Center (Центр администрирования Active Directory), Active Directory Web Services (Веб-служба Active Directory) и модуль для администрирования Active Directory из оболочки Windows PowerShell.

Вопрос №2. Структура службы ADDS

Домен AD DS

Домен AD DS, традиционно изображаемый в виде треугольника (рис. 1), является главной логической границей AD DS.



Домен AD DS

Информация о пользователях и компьютерах хранится и обрабатывается внутри домена. Домены в AD DS разграничивают административную безопасность для объектов и содержат собственные политики безопасности.

Домены представляют собой логическую организацию объектов и могут охватывать **несколько физических местоположений**. Это реализуется с помощью контроллеров RODC (read-only domain controller).

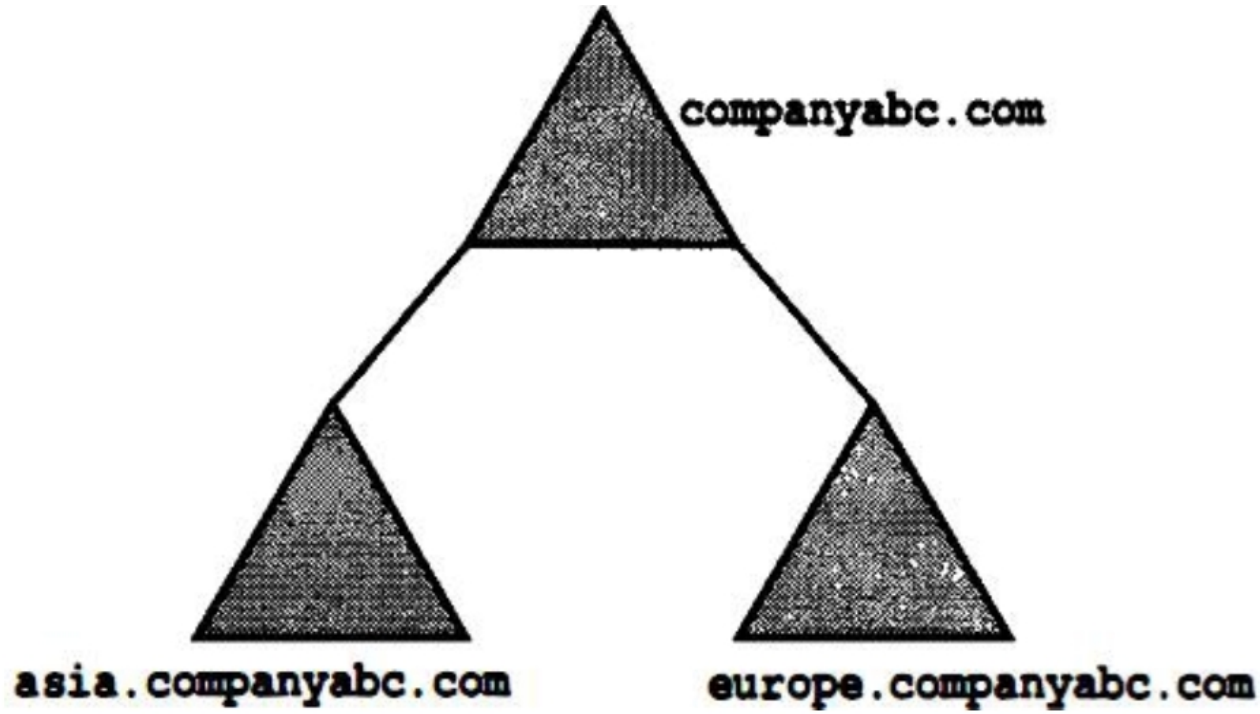
Домен AD DS

Основная задача, которую преследует технологией RODC, возможность **безопасной установки** собственного контролера домена в **удаленных** филиалах и офисах, в которых сложно обеспечить физическую защиту сервера с ролью DC.

Контроллер домена RODC **содержит копию** базы Active Directory, доступную **только на чтение**. Это означает, что никто, даже при получении физического доступа к такому контроллеру домена, не сможет изменить данные в AD (в том числе сбросить пароль администратора домена).

Деревья доменов AD DS

Дерево AD DS состоит из нескольких доменов, соединенных **двунаправленными** транзитивными **отношениями доверия**. Каждый домен в дереве AD DS использует **общую схему** и **глобальный каталог**. *Корневым доменом* дерева ADDS является companyabc.com, а asia.companyabc.com и europe.companyabc.com — его *поддомены* (см. рис. 2).



Деревья доменов AD DS

Транзитивное отношение доверия устанавливается автоматически. Оно означает, что если **домен asia доверяет** корневому домену companyabc, и **домен europe** также **доверяет** домену companyabc, то домен **asia доверяет** и **домену europe**. Доверительные отношения пронизывают всю доменную структуру.

Транзитивность отношений доверия в среде ADDS не означает, что правами доступа могут пользоваться все пользователи или даже администраторы других доменов. Доверительные отношения лишь **обеспечивают путь** от одного домена к другому. По умолчанию **никакие права доступа** от одного транзитивного домена к другому **не передаются**. Чтобы пользователи или администраторы другого домена могли **получать доступ** к ресурсам данного домена, его **администратор должен предоставить** им соответствующие права.

Леса в AD DS

Лесами (forest) в ADDS называются группы **связанных** между собой **деревьев доменов**. Неявные отношения доверия объединяют корни всех деревьев в один общий лес.

Связями, объединяющими все домены и деревья доменов в общий лес, служит наличие **общей схемы** и **общего глобального каталога**. Хотя доменам и деревья доменов в этом лесу вовсе **не обязательно** использовать **общее пространство имен**.

Например, домены microsoft.internal и msnbc.internal теоретически могут являться частями одного и того же леса, но при этом иметь собственные раздельные пространства имен.

Леса служат основной границей **организационной безопасности** в AD DS, и потому предполагают наличие некоторой степени доверия к администраторам всех входящих в их состав доменов.

Режимы аутентификации в AD DS

В Windows NT 4.0 для аутентификации применялась подсистема под названием **NTLM** (NT LAN Manager — диспетчер локальной сети NT). В ней **зашифрованный пароль пересылался по сети** в виде хэша. Ее **недостатком** было то, что любой желающий мог отслеживать в сети передаваемые хеши, собирать их и затем расшифровывать с помощью сторонних средств взлома паролей по словарю или "грубой силой".

Во всех версиях Windows Server после Windows 2000 стала применяться подсистема аутентификации **Kerberos**. **Kerberos не пересылает информацию пароля по сети** и поэтому гораздо безопаснее NTLM.

Обзор функциональных уровней в Windows Server AD DS

В Windows 2000 Server и Windows Server 2003 поддерживались собственные функциональные уровни для обеспечения обратной совместимости с доменами предыдущих версий. Аналогично Windows Server 2016/2019 содержит **функциональные уровни для поддержки совместимости**.

По умолчанию **при выполнении свежей установки** Active Directory на контроллерах домена Windows Server 2016/2019 автоматически создается домен Windows Server 2016/2019 и функциональные уровни леса. Но при установке контроллеров домена Windows Server 2016/2019 **в существующем устаревшем домене** можно **выбрать функциональный уровень**, с которого начнет работать лес. Если лес Active Directory уже существует, его функциональный уровень **можно поднять** до Windows Server 2016/2019

Вопрос №3. Компоненты ADDS

Связь AD DS с моделью X.500

AD DS в основном следует **информационной модели** службы каталогов **X.500**, которая определяет службу каталогов через **распределенный подход**, определенный **информационным деревом каталога** (Directory Information Tree — DIT). Это дерево логически разбивает структуру службы каталогов в уже знакомый формат:

имя_сервера.имя_поддомена.имя_домена.com

В модели X.500 информация каталога хранится в **иерархической структуре**, получившей название **агентов системы каталогов** (Directory System Agent — DSA). Технология ADDS основана на многих базовых принципах определения X.500, но сама **AD DS не совместима** с реализациями X.500, поскольку протокол X.500 основан на модели OSI, которая неэффективно работает с протоколом TCP/IP, используемым AD DS.

Концепция схемы AD DS

Схемой в AD DS называется **набор определений** для всех типов имеющихся в каталоге **объектов** и связанных с ними **атрибутов**. Именно схема **задает способ хранения** и **представления** в AD DS данных обо всех пользователях, компьютерах и других объектах, чтобы они имели стандартный вид по всей структуре AD DS. Она **защищается** с помощью списков управления разграничением доступа (Discretionary Access Control List - **DA CL**) и отвечает за предоставление возможных атрибутов для каждого объекта в AD DS. По сути, схема представляет собой базовое определение самого каталога и является **основой функционирования** среды домена. При делегировании прав на управление схемой избранной группе администраторов следует соблюдать осторожность, поскольку вносимые в схему изменения влияют на всю среду AD DS.

Объекты схемы

Сохраняемые внутри структуры AD DS **элементы**, вроде пользователей, принтеров, компьютеров и сайтов, в рамках схемы называются **объектами**. У каждого такого объекта имеется свой **список атрибутов**, которые определяют его **характеристики** и могут применяться для его поиска.

Например, объект пользователя для работника по имени Иван Петров будет иметь атрибут FirstName (Имя) со значением "Иван" и атрибут LastName (Фамилия) со значением "Петров".

Помимо этих, могут назначаться и **другие атрибуты**: название подразделения, адрес электронной почты и многое другое. Пользователи, которые выполняют поиск информации в AD DS, смогут строить на основе этой информации **свои запросы** и находить, например, всех пользователей, которые работают в отделе сбыта.

Расширение схемы

Одним из главных преимуществ структуры AD DS является возможность напрямую **изменять** и **расширять** схему, включая в нее **произвольные атрибуты**.

Многие сторонние продукты также выполняют свои расширения схемы, которые позволяют отображать различные типы информации из каталога.

Вопрос №4. Определение организационных единиц домена

Организационные единицы (Organizational Unit - OU) представляют собой **контейнеры**, которые позволяют логически хранить информацию каталогов и назначать ей в ADDS адреса с помощью протокола LDAP.

В AD DS организационные единицы являются **основным методом** организации информации о пользователях, компьютерах и других объектах в более удобном для понимания виде.

На рисунке приведена корневая организационная единица, в которую вложены три других организационных единицы - отдел маркетинга, отдел информационных технологий и отдел исследований.

Подобное вложение одних организационных единиц в другие **позволяет** организациям **распределять информацию** о пользователях в несколько контейнеров, что **облегчает просмотр** и **администрирование** сетевых ресурсов.

Однако организационные единицы следует создавать лишь тогда, когда в организации **необходимо делегировать администрирование** другому коллективу администраторов.

Если одно и то же лицо или группа лиц осуществляет административное управление всем доменом, то **нет смысла** усложнять среду, добавляя в нее организационные единицы. Слишком большое количество организационных единиц может **негативно влиять** на групповые политики, входную регистрацию и другие факторы.

Организационные единицы можно структурировать так, чтобы **отдельные подразделения** имели **различные уровни** административного контроля над своими пользователями.

Другое **преимущество** применении организационных единиц состоит в том, что **пользователей** можно легко **перетаскивать** мышью из одной OU в другую.

Дополнительное преимущество - **легкость исправления ошибок**, допущенных при проектировании OU, поскольку изменения можно внести в любой момент

Вопрос №5. Роль DNS и безопасность в ADDS

Когда в Microsoft начали разрабатывать AD DS, главным приоритетом было **обеспечение** ее **полной совместимости** с системой доменных имен (Domain Name System - **DNS**).

В результате ADDS была создана не только полностью совместимой с DNS, но и настолько интегрированной с ней, что **не может без нее существовать**.

Концепции пространств имен DNS

Пространство имен DNS представляет собой ограниченную **логическую область**, образуемую **именем DNS** и его **поддоменами**.

Например, имена europe.companyabc.com, asia.companyabc.com и companyabc.com являются частями одного и того же непрерывного пространства имен DNS.

Пространство имен DNS в ADDS может быть **опубликовано** в Интернете, наподобие microsoft.com или msn.com, или **скрыто** от всех, что зависит стратегии и требований безопасности тех, кто ее реализует.

Концепции пространств имен DNS

Внешние (опубликованные) пространства имен. Имя DNS, распознаваемое из любого места в Интернете, называется опубликованным или внешним пространством имен.

Внутренние (скрытые) пространства имен. Для многих организаций публикация внутренней доменной структуры недопустима с точки зрения безопасности. Такие организации могут определять схемы AD DS с внутренним пространством имен, не доступным для чтения из Интернета. Из практических соображений **для частной адресации** специально зарезервировано пространство имен **.internal**, и во многих случаях оно очень удобно для использования.

Динамическая служба доменных имен

Динамическая служба доменных имен (Dynamic Domain Name System - DDNS) разработана как средство для устранения проблемы, связанной с необходимостью **ручного обновления таблиц DNS** после внесения изменений. В Windows Server она автоматически обновляет таблицы DNS на основе регистраций и может работать **в сочетании с протоколом DHCP**, автоматически обрабатывая изменения при добавлении и удалении клиентов из сетевой инфраструктуры.

DDNS **не обязательна** для корректной работы AD DS, но она **существенно облегчает** администрирование по сравнению со старыми ручными методами.

Аутентификация Kerberos

Механизм Kerberos был разработан в Массачусетском Технологическом институте как **безопасный метод** для аутентификации пользователей **без пересылки их пароля по сети** ни в зашифрованном, ни в незашифрованном виде. Такая возможность передачи пароля значительно уменьшает опасность хищения пароля, т.к. злоумышленники не могут получить копию пароля во время его передачи по сети и расшифровать его с применением приемов " грубой силы".

Дополнительные меры защиты

Безопасность структуры AD DS можно усилить с помощью **дополнительных мер предосторожности**:

- безопасный обмен данными между серверами по протоколу IPSec,
- использование смарт-карт или других технологий шифрования
- пользовательскую среду можно защитить параметрами **групповых политик** для ограничения паролей пользователей, защиты доменов и прав доступа при входной регистрации.