Лабораторная работа №1

Изучение возможностей системного программного обеспечения для централизации управления информационной безопасностью.

Цель работы: сформировать у студента теоретические и практические навыки работы со службой каталогов, как инструмента централизованного управления безопасностью в современной организации, на примере службы Active Directory. Получение навыков управления службой через средства PowerShell и графический интерфейс операционной системы.

Краткая теория:

Active Directory («Активный каталог», AD) — LDAP-совместимая реализация службы каталогов корпорации Microsoft для операционных систем семейства Windows NT. Active Directory позволяет администраторам использовать групповые политики для обеспечения единообразия настройки пользовательской рабочей среды, разворачивать программное обеспечение на множестве компьютеров через групповые политики или посредством System Center Configuration Manager (ранее Microsoft Systems Management Server), устанавливать обновления операционной системы, прикладного и серверного программного обеспечения на всех компьютерах в сети, используя Службу обновления Windows Server. Active Directory хранит данные и настройки среды в централизованной базе данных. Сети Active Directory могут быть различного размера: от нескольких десятков до нескольких миллионов объектов.

LDAP (или lightweight directory access protocol) – это протокол, который определяет методы, с помощью которых можно получить доступ к службе каталогов. В более широком смысле LDAP формирует способ отображения данных в службе каталогов для пользователей, определяет требования к компонентам, используемым для создания записей данных, и описывает способ использования разных примитивных элементов для составления записей.

Групповая политика — это набор правил или настроек, в соответствии с которыми производится настройка рабочей среды приёма/передачи (Windows, X-unix и другие операционные системы с поддержкой сети). Групповые политики создаются в домене и реплицируются в рамках домена. Объект групповой политики (Group Policy Object, GPO) состоит из двух физически раздельных составляющих: контейнера групповой политики (англ. Group Policy Container, GPC) и шаблона групповой политики (Group Policy Template, GPT). Эти два компонента содержат в себе все данные о параметрах рабочей среды, которая

включается в состав объекта групповой политики. Продуманное применение объектов GPO к объектам каталога Active Directory позволяет создавать эффективную и легко управляемую компьютерную рабочую среду на базе ОС Windows. Политики применяются сверху вниз по иерархии каталога Active Directory.

Представление Active Directory состоялось в 1999 году, продукт был впервые выпущен с Windows 2000 Server, а затем был модифицирован и улучшен при выпуске Windows Server 2003. Впоследствии Active Directory был улучшен в Windows Server 2003 R2, Windows Server 2008 и Windows Server 2008 R2 и переименован в Active Directory Domain Services. Ранее служба каталогов называлась NT Directory Service (NTDS), это название до сих пор можно встретить в некоторых исполняемых файлах.

В отличие от версий Windows до Windows 2000, которые использовали в основном протокол NetBIOS для сетевого взаимодействия, служба Active Directory интегрирована с DNS и TCP/IP. Для аутентификации по умолчанию используется протокол Kerberos. Если клиент или приложение не поддерживает аутентификацию Kerberos, используется протокол NTLM.

Устройство

Объекты

Active Directory имеет иерархическую структуру, состоящую из объектов. Объекты разделяются на три основные категории: ресурсы (например, принтеры), службы (например, электронная почта) и учётные записи пользователей и компьютеров. Active Directory предоставляет информацию об объектах, позволяет организовывать объекты, управлять доступом к ним, а также устанавливает правила безопасности.

Объекты могут быть хранилищами для других объектов (группы безопасности и распространения). Объект уникально определяется своим именем и имеет набор атрибутов — характеристик и данных, которые он может содержать; последние, в свою очередь, зависят от типа объекта. Атрибуты являются составляющей базой структуры объекта и определяются в схеме. Схема определяет, какие типы объектов могут существовать.

Сама схема состоит из двух типов объектов: объекты классов схемы и объекты атрибутов схемы. Один объект класса схемы определяет один тип объекта Active Directory (например, объект «Пользователь»), а один объект атрибута схемы определяет атрибут, который объект может иметь.

Каждый объект атрибута может быть использован в нескольких разных объектах классов схемы. Эти объекты называются объектами схемы (или метаданными) и позволяют изменять и дополнять схему, когда это необходимо. Однако каждый объект схемы является частью определений объектов Active Directory, поэтому отключение или изменение этих

объектов могут иметь серьёзные последствия, так как в результате этих действий будет изменена структура Active Directory. Изменение объекта схемы автоматически распространяется в Active Directory. Будучи однажды созданным, объект схемы не может быть удалён, он может быть только отключён. Обычно все изменения схемы тщательно планируются.

Контейнер аналогичен объекту в том смысле, что он также имеет атрибуты и принадлежит пространству имён, но, в отличие от объекта, контейнер не обозначает ничего конкретного: он может содержать группу объектов или другие контейнеры.

Структура

Верхним уровнем структуры является лес — совокупность всех объектов, атрибутов и правил (синтаксиса атрибутов) в Active Directory. Лес содержит одно или несколько деревьев, связанных транзитивными отношениями доверия. Дерево содержит один или несколько доменов, также связанных в иерархию транзитивными отношениями доверия. Домены идентифицируются своими структурами имён DNS — пространствами имён.

Объекты в домене могут быть сгруппированы в контейнеры — подразделения. Подразделения позволяют создавать иерархию внутри домена, упрощают его администрирование и позволяют моделировать организационную и/или географическую структуры компании в Active Directory. Подразделения могут содержать другие подразделения. Корпорация Microsoft рекомендует использовать как можно меньше доменов в Active Directory, а для структурирования и политик использовать подразделения. Часто групповые политики применяются именно к подразделениям. Групповые политики сами являются объектами. Подразделение является самым низким уровнем, на котором могут делегироваться административные полномочия.

Другим способом деления Active Directory являются сайты, которые являются способом физической (а не логической) группировки на основе сегментов сети. Сайты подразделяются на имеющие подключения по низкоскоростным каналам (например, по каналам глобальных сетей, с помощью виртуальных частных сетей) и по высокоскоростным каналам (например, через локальную сеть). Сайт может содержать один или несколько доменов, а домен может содержать один или несколько сайтов. При проектировании Active Directory важно учитывать сетевой трафик, создающийся при синхронизации данных между сайтами.

Ключевым решением при проектировании Active Directory является решение о разделении информационной инфраструктуры на иерархические домены и подразделения верхнего уровня. Типичными моделями, используемыми для такого разделения, являются модели разделения по функциональным подразделениям компании, по географическому

положению и по ролям в информационной инфраструктуре компании. Часто используются комбинации этих моделей.

Физическая структура и репликация

Физически информация хранится на одном или нескольких равнозначных контроллерах доменов, заменивших использовавшиеся в Windows NT основной и резервные контроллеры домена, хотя для выполнения некоторых операций сохраняется и так называемый сервер «операций с одним главным сервером», который может эмулировать главный контроллер домена. Каждый контроллер домена хранит копию данных, предназначенную для чтения и записи. Изменения, сделанные на одном контроллере, синхронизируются на все контроллеры домена при репликации. Серверы, на которых сама служба Active Directory не установлена, но которые при этом входят в домен Active Directory, называются рядовыми серверами.

Репликация Active Directory выполняется по запросу. Служба Knowledge Consistency Checker создаёт топологию репликации, которая использует сайты, определённые в системе, для управления трафиком. Внутри сайтовая репликация выполняется часто и автоматически с помощью средства проверки согласованности (уведомлением партнёров по репликации об изменениях). Репликация между сайтами может быть настроена для каждого канала сайта (в зависимости от качества канала) — различная «оценка» (или «стоимость») может быть назначена каждому каналу и трафик репликации будет ограничен, передаваться по расписанию и маршрутизироваться в соответствии с назначенной оценкой канала. Данные репликации могут транзитивно передаваться через несколько сайтов через мосты связи сайтов, если «оценка» низка, хотя AD автоматически назначает более низкую оценку для связей «сайт-сайт», чем для транзитивных соединений. Репликация сайт-сайт выполняется серверами-плацдармами в каждом сайте, которые затем реплицируют изменения на каждый контроллер домена своего сайта. Внутри доменная репликация проходит по протоколу RPC по протоколу IP, междоменная — может использовать также протокол SMTP.

Если структура Active Directory содержит несколько доменов, для решения задачи поиска объектов используется глобальный каталог: контроллер домена, содержащий все объекты леса, но с ограниченным набором атрибутов (неполная реплика). Каталог хранится на указанных серверах глобального каталога и обслуживает меж доменные запросы.

Возможность операций с одним главным компьютером позволяет обрабатывать запросы, когда репликация с несколькими главными компьютерами недопустима. Есть пять типов таких операций: эмуляция главного контроллера домена (PDC-эмулятор), главный компьютер относительного идентификатора (мастер относительных идентификаторов или

RID-мастер), главный компьютер инфраструктуры (мастер инфраструктуры), главный компьютер схемы (мастер схемы) и главный компьютер именования домена (мастер именования доменов). Первые три роли уникальны в рамках домена, последние две — уникальны в рамках всего леса.

Базу Active Directory можно разделить на три логических хранилища или «раздела». Схема является шаблоном для Active Directory и определяет все типы объектов, их классы и атрибуты, синтаксис атрибутов (все деревья находятся в одном лесу, потому что у них одна схема). Конфигурация является структурой леса и деревьев Active Directory. Домен хранит всю информацию об объектах, созданных в этом домене. Первые два хранилища реплицируются на все контроллеры доменов в лесу, третий раздел полностью реплицируется между репликами контроллеров в рамках каждого домена и частично — на сервера глобального каталога.

База данных (хранилище каталогов) в Windows 2000 использует расширяемую подсистему хранения Microsoft Jet Blue (англ.), которая позволяет для каждого контроллера домена иметь базу размером до 16 терабайт и 1 миллиард объектов (теоретическое ограничение, практические тесты выполнялись только с приблизительно 100 миллионами объектов). Файл базы называется NTDS.DIT и имеет две основные таблицы — таблицу данных и таблицу связей. В Windows Server 2003 добавлена ещё одна таблица для обеспечения уникальности экземпляров дескрипторов безопасности.

С выходом Windows Server 2016, служба Active Directory получила три важных новых функции: Access Management, Azure AD Join и Microsoft Passport.

Основная цель Azure AD Join — предоставить преимущества локальной Active Directory среды без сопутствующей сложности владения и управления

Microsoft Passport может предложить повышенную безопасность, по сравнению с обычными паролями, без сложностей таких традиционных решений, как смарт карты. Он спроектирован для использования совместно с Windows Hello (встроенная биометрическая система авторизации в Windows 10 Pro/Enterprise)

Именование

Active Directory поддерживает следующие форматы именования объектов: универсальные имена типа UNC, URL и LDAP URL. Версия LDAP формата именования X.500 используется внутри Active Directory.

Каждый объект имеет различающееся имя (distinguished name, DN). Например, объект принтера с именем HPLaser3 в подразделении «Маркетинг» и в домене foo.org будет иметь следующее различающееся имя: CN=HPLaser3, OU=Маркетинг,DC=foo,DC=org, где CN — это общее имя, OU — раздел, DC — класс объекта домена. Различающиеся имена

могут иметь намного больше частей, чем четыре части в этом примере. У объектов также есть канонические имена. Это различающиеся имена, записанные в обратном порядке, без идентификаторов и с использованием косых черт в качестве разделителей: foo.org/Маркетинг/HPLaser3. Чтобы определить объект внутри его контейнера, используется относительное различающееся имя: CN=HPLaser3. У каждого объекта также есть глобально уникальный идентификатор (GUID) — уникальная и неизменная 128-битная строка, которая используется в Active Directory для поиска и репликации. Определённые объекты также имеют имя участника-пользователя (UPN, в соответствии с RFC 822) в формате объект@домен.

Управление:

Средства управления Microsoft Active Directory включают:

- Active Directory Administrative Center (Introduced with Windows Server 2012 and above),
- Active Directory Users and Computers,
- Active Directory Domains and Trusts,
- Active Directory Sites and Services,
- ADSI Edit,
- Local Users and Groups,
- Active Directory Schema snap-ins for Microsoft Management Console (MMC),

Представленные инструменты не полностью обеспечивают выполнение задач администрирования служб каталогов в больших средах, но позволяют расширить внешние решения по автоматизации, генерации отчетов интеграции.

Интеграция с UNIX

Различные уровни взаимодействия с Active Directory могут быть реализованы в большинстве UNIX-подобных операционных систем посредством соответствующих стандарту LDAP клиентов, но такие системы, как правило, не воспринимают большую часть атрибутов, ассоциированных с компонентами Windows, например групповые политики и поддержку односторонних доверенностей.

Сторонние поставщики предлагают интеграцию Active Directory на платформах UNIX, включая UNIX, Linux, Mac OS X и ряд приложений на базе Java, с пакетом продуктов:

- Centrify DirectControl (Centrify Corporation) — совместимые с Active Directory централизованную аутентификацию и контроль доступа.

- Centrify Express (Centrify Corporation) — набор свободных совместимых с Active Directory сервисов для централизованной аутентификации, мониторинга, разделяемого доступа к файлам и удаленного доступа.
- UNAB (Computer Associates).
- TrustBroker (CyberSafe Limited) — реализация Kerberos.
- PowerBroker Identity Services, ранее Likewise (BeyondTrust) — позволяет клиенту войти в домен Active Directory.
- Authentication Services (Quest Software).
- ADmitMac (Thursby Software Systems).
- Samba — может выполнять роль контроллера домена.

Добавления в схему, поставляемые с Windows Server 2003 R2, включают атрибуты, которые достаточно тесно связаны с RFC 2307, чтобы использоваться в общем случае. Базовые реализации RFC 2307, nss_ldap и pam_ldap, предложенные PADL.com, непосредственно поддерживают эти атрибуты. Стандартная схема для членства в группе соответствует RFC 2307bis (предлагаемому). Windows Server 2003 R2 включает Консоль управления Microsoft для создания и редактирования атрибутов.

Альтернативным вариантом является использование другой службы каталогов, например 389 Directory Server (ранее Fedora Directory Server, FDS), eB2Bcom ViewDS v7.1 XML Enabled Directory или Sun Java System Directory Server от Sun Microsystems, выполняющую двухстороннюю синхронизацию с Active Directory, реализуя таким образом «отраженную» интеграцию, когда клиенты UNIX и Linux аутентифицируются FDS, а клиенты Windows аутентифицируются Active Directory. Другим вариантом является использование OpenLDAP с возможностью полупрозрачного перекрытия, расширяющей элементы удаленного сервера LDAP дополнительными атрибутами, хранимыми в локальной базе данных.

Active Directory автоматизируются с помощью Powershell.

Основные понятия и выводы:

Домен – это основная административная единица в сетевой инфраструктуре предприятия, в которую входят все сетевые объекты, такие как пользователи, компьютеры, принтеры, общие ресурсы и многое другое. Совокупность таких доменов называется лесом.

Службы Active Directory (службы активного каталога) представляют собой распределённую базу данных, которая содержит все объекты домена. Доменная среда Active Directory является единой точкой аутентификации и авторизации пользователей и

приложений в масштабах предприятия. Именно с организации домена и развёртывания служб Active Directory начинается построение ИТ-инфраструктуры предприятия.

База данных Active Directory хранится на выделенных серверах – контроллерах домена. Службы Active Directory являются ролью серверных операционных систем Microsoft Windows Server. Службы Active Directory имеют широкие возможности масштабирования. В лесу Active Directory может быть создано более 2-х миллиардов объектов, что позволяет внедрять службу каталогов в компаниях с сотнями тысяч компьютеров и пользователей. Иерархическая структура доменов позволяет гибко масштабировать ИТ-инфраструктуру на все филиалы и региональные подразделения компаний. Для каждого филиала или подразделения компании может быть создан отдельный домен, со своими политиками, своими пользователями и группами. Для каждого дочернего домена могут быть делегированы административные полномочия местным системным администраторам. При этом всё равно дочерние домены подчиняются родительским.

Кроме того, службы Active Directory позволяют настроить доверительные отношения между доменными лесами. Каждая компания имеет собственный лес доменов, каждый из которых имеет собственные ресурсы. Но иногда бывает нужно предоставить доступ к своим корпоративным ресурсам сотрудникам другой компании – работа с общими документами и приложениями в рамках совместного проекта. Для этого между лесами организаций можно настроить доверительные отношения, что позволит сотрудникам одной организации авторизоваться в домене другой.

Для обеспечения отказоустойчивости служб Active Directory необходимо развернуть два или более контроллера домена в каждом домене. Между контроллерами домена обеспечивается автоматическая репликация всех изменений. В случае выхода из строя одного из контроллеров домена работоспособность сети не нарушается, ведь оставшиеся продолжают работать. Дополнительный уровень отказоустойчивости обеспечивает размещение серверов DNS на контроллерах домена в Active Directory, что позволяет в каждом домене получить несколько серверов DNS, обслуживающих основную зону домена. И в случае отказа одного из DNS серверов, продолжат работать остальные.

Преимущества, которые получает компания, отказываясь от одноранговой сети с использованием рабочих групп.

1. Единая точка аутентификации

В рабочей группе на каждом компьютере или сервере придётся вручную добавлять полный список пользователей, которым требуется сетевой доступ. Если вдруг один из сотрудников захочет сменить свой пароль, то его нужно будет поменять на всех

компьютерах и серверах. При использовании домена Active Directory все учётные записи пользователей хранятся в одной базе данных, и все компьютеры обращаются к ней за авторизацией. Все пользователи домена включаются в соответствующие группы, например, «Бухгалтерия», «Финансовый отдел». Достаточно один раз задать разрешения для тех или иных групп, и все пользователи получат соответствующий доступ к документам и приложениям. Если в компанию приходит новый сотрудник, для него создаётся учётная запись, которая включается в соответствующую группу, – сотрудник получает доступ ко всем ресурсам сети, к которым ему должен быть разрешён доступ. Если сотрудник увольняется, то достаточно заблокировать – и он сразу потеряет доступ ко всем ресурсам (компьютерам, документам, приложениям).

2. Единая точка управления политиками

В рабочей группе все компьютеры равноправны. Ни один из компьютеров не может управлять другим, невозможно проконтролировать соблюдение единых политик, правил безопасности. При использовании единого каталога Active Directory, все пользователи и компьютеры иерархически распределяются по организационным подразделениям, к каждому из которых применяются единые групповые политики. Политики позволяют задать единые настройки и параметры безопасности для группы компьютеров и пользователей. При добавлении в домен нового компьютера или пользователя, он автоматически получает настройки, соответствующие принятым корпоративным стандартам. При помощи политик можно централизованно назначить пользователям сетевые принтеры, установить необходимые приложения, задать параметры безопасности браузера, настроить приложения Microsoft Office.

3. Повышенный уровень информационной безопасности

Использование служб Active Directory значительно повышает уровень безопасности сети. Во-первых – это единое и защищённое хранилище учётных записей. В доменной среде все пароли доменных пользователях хранятся на выделенных серверах контроллерах домена, которые, как правило, защищены от внешнего доступа. Во-вторых, при использовании доменной среды для аутентификации используется протокол Kerberos, который значительно безопаснее, чем NTLM, использующийся в рабочих группах.

4. Интеграция с корпоративными приложениями и оборудованием

Большим преимуществом служб Active Directory является соответствие стандарту LDAP, который поддерживается другими системами, например, почтовыми серверами (Exchange Server), прокси-серверами (ISA Server, TMG). Причем это не обязательно только продукты Microsoft. Преимущество такой интеграции заключается в том, что пользователю не требуется помнить большое количество логинов и паролей для доступа к тому или иному

приложению, во всех приложениях пользователь имеет одни и те же учётные данные – его аутентификация происходит в едином каталоге Active Directory. Windows Server для интеграции с Active Directory предоставляет протокол RADIUS, который поддерживается большим количеством сетевого оборудования. Таким образом, можно, например, обеспечить аутентификацию доменных пользователей при подключении по VPN извне, использование Wi-Fi точек доступа в компании.

5. Единое хранилище конфигурации приложений

Некоторые приложения хранят свою конфигурацию в Active Directory, например, Exchange Server. Развёртывание службы каталогов Active Directory является обязательным условием для работы этих приложений. Хранение конфигурации приложений в службе каталогов является выгодным с точки зрения гибкости и надёжности. Например, в случае полного отказа сервера Exchange, вся его конфигурация останется нетронутой. Для восстановления работоспособности корпоративной почты, достаточно будет переустановить Exchange Server в режиме восстановления.

Службы Active Directory являются сердцем ИТ-инфраструктуры предприятия. В случае отказа вся сеть, все сервера, работа всех пользователей будут парализованы. Никто не сможет войти в компьютер, получить доступ к своим документам и приложениям. Поэтому служба каталогов должна быть тщательно спроектирована и развёрнута, с учётом всех возможных нюансов, например, пропускной способности каналов между филиалами или офисами компании (от этого напрямую зависит скорость входа пользователей в систему, а также обмен данными между контроллерами домена).

Задание.

1. Выбрать и инсталлировать средство виртуализации.
2. Скачать и установить образ серверной операционной системы.
3. Установить роль Active Directory.
4. Настроить роль и повысить сервер до уровня контроллера домена.
5. Выполнить основные задачи администрирования через GUI и через PowerShell.

Список основных задач:

1. Создать и удалить пользователя.
2. Сбросить пароль пользователя
3. Активировать и деактивировать учетные записи

4. Разблокировать учетную запись пользователя
5. Удалить учетную запись
6. Найти пустые группы
7. Добавить пользователей в группу
8. Вывести список членов группы
9. Найти устаревшие учетные записи компьютеров
10. Деактивировать учетную запись компьютера
11. Найти компьютеры по типу

Контрольные вопросы.

1. Что такое служба Active Directory?
2. Что такое служба LDAP
3. Что такое служба Групповая политика?
4. Структура службы каталогов, основные объекты.
5. Схема службы каталогов, атрибуты, типы объектов.
6. Понятия: лес, домен, дерево.
7. Что такое сайты AD?
8. Принципы проектирования Active Directory.
9. Физическая структура и репликация.
10. Именование объектов Active Directory.
11. Средства управления Active Directory.
12. Преимущества внедрения Active Directory?
13. Что такое PowerShell?
14. Командлеты и принцип создания скриптов.