**Лекция №1**

**Планирование апгрейда и миграции сервера**

Рекомендации по апгрейду и миграции. Создание плана апгрейда и миграции сервера. Планирование виртуализации. **Планирование и внедрение инфраструктуры для развертывания серверов**

Выбор подходящей стратегии создания образов сервера. Внедрение стратегии автоматического развертывания

Рассматриваемые вопросы:

1.Апгрейд

2.Виртуализация

3.Развертывания серверов

**Контрольные вопросы:**

**Лекция №2**

**Планирование и развертывание серверов с использованием диспетчера виртуальных машин (VMM)**

Рассматриваемые вопросы:

1.Планирование и развертывание серверов

2.Диспетчер виртуальных машин

Виртуальная машина – это программа, которая эмулирует реальный (физический) компьютер со всеми его компонентами (жёсткий диск, привод,BIOS, сетевые адаптеры и т.д.). На такой виртуальный компьютер можно установить, например, операционную систему, драйверы, программы и т.д. Таким образом, Вы можете запустить на своем реальном компьютере еще несколько виртуальных компьютеров с такой же или другой операционной системой. Вы можете без проблем осуществить обмен данными между вашим реальным и виртуальным компьютером.

Кроме того, виртуальные машины предоставляют удобные возможности по созданию конкретного специфического окружения, необходимого для исследования разрабатываемого ПО. Можно свободно варьировать специфичные региональные настройки и настраивать локализацию пользователей. И при этом исследователь может легко экспериментировать с настройками среды, без влияния на конфигурацию и работоспособность собственной физической машины.

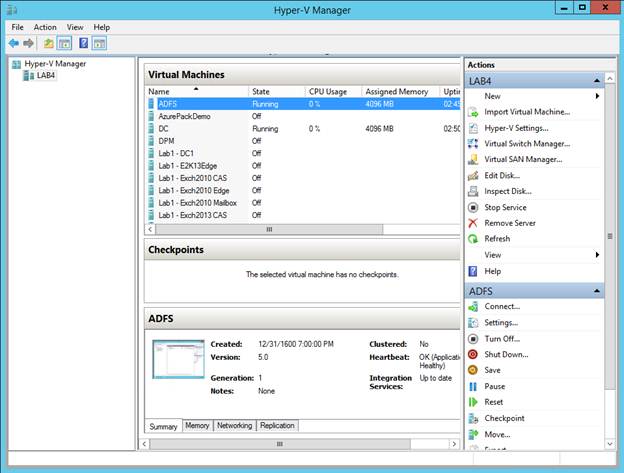
Технологии виртуализации сейчас применяются во многих сферах ИТ как в производственной среде, так и энтузиастами и домашними пользователями для самых разных задач. Несколько одновременно запущенных виртуальных систем на одной физической машине существенно повышают гибкость ИТ-инфраструктуры и увеличивают эффективность использования аппаратных ресурсов. Тестирование программного обеспечения – один из самых распространенных вариантов использования для платформ виртуализации. Неудивительно, ведь виртуальные машины обладают множеством полезных свойств, благодаря которым значительно сокращается время разработки и тестирования и повышается эффективность этих процессов.

Диспетчер Виртуальных Машин) - это инструмент управления, который предназначен для того, чтобы сделать Hyper-V намного проще для управления этими серверами по мере того, как размер развёртывания Hyper-V увеличивается.

Справедливости ради следует отметить, что Диспетчер Виртуальных Машин также предоставляет ряд возможностей Hyper-V, к которым нельзя получить доступ через Диспетчер Hyper-V или через Диспетчер отказоустойчивости Кластеров. О некоторых из этих возможностей будет сказано позже в статье. Сначала поговорим о масштабируемости, потому что Диспетчер Виртуальных Машин изначально был представлен как решение для масштабирования Hyper-V.

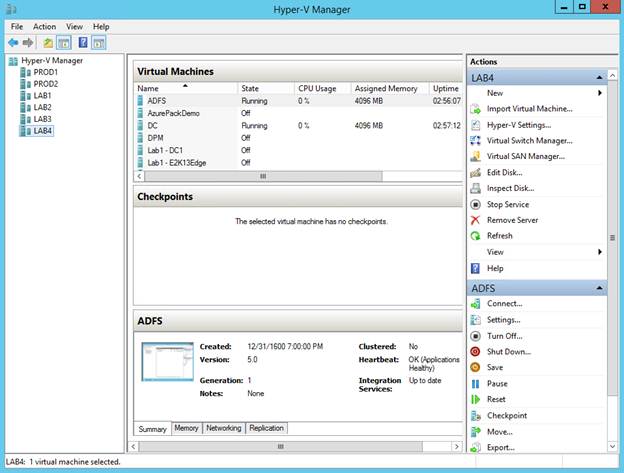
Чтобы по-настоящему оценить возможности, предоставляемые Диспетчером Виртуальных Машин, взглянем на ограничения, которые присутствуют в Диспетчере Hyper-V.

На Рис.1 показан Диспетчер Hyper-V.

****

Как показано на рисунке выше, Диспетчер Hyper-V разделен на три вертикальных столбца. В столбце слева указан хост-сервер. В верхней части среднего столбца перечислены все виртуальные машины, которые запущены на хосте. Хотя такая схема кажется достаточно логичной, она несовершенна с точки зрения масштабируемости. Как уже объяснялось ранее, большинство организаций, использующих Hyper-V в производственной среде, имеют более одного сервера Hyper-V. Тем не менее Диспетчер Hyper-V отображает только локальный сервер и работающие на нём виртуальные машины.

Это не означает, что нет способа ввести в Диспетчер Hyper-V информацию о других хостах Hyper-V. Если желаете, чтобы Диспетчер Hyper-V был в курсе о дополнительных хостах Hyper-V, это можно сделать, нажав правой кнопкой мышки на контейнер Диспетчера Hyper-V (расположенном в верхней левой части консоли) и выбрав команду «Присоединиться к Серверу» из контекстного меню. Таким образом, можно предоставить Диспетчеру Hyper-V имя другого Сервера Hyper-V. Как указано на рисунке ниже, с помощью Диспетчера Hyper-V можно управлять несколькими серверами Hyper-V.



## Компоненты Диспетчера Виртуальных Машин

Первым из этих компонентов является Сервер Управления VMM. Сервер Управления - это компонент, выполняющий всю тяжёлую работу. Он является основным компонентом Сервера Управления Виртуальными Машинами, который отвечает за обработку команд и за запуск основной службы VMM. Сервер Управления также отвечает за координацию связи между всеми различными компонентами.

Следующий компонент, о котором нужно знать, это база данных VMM. База данных VMM - это база данных SQL Server, в которой хранится вся информация о конфигурации, которая используется SCVMM. Эта база данных также хранит такие вещи, как профили и шаблоны служб (подробнее об этом позже статье).

Третий компонент, с которым нужно ознакомиться, это консоль VMM. Консоль VMM - это графический интерфейс пользователя для SCVMM. При работе с SCVMM большая часть времени будет тратиться на работу в этой консоли.

Корпорация Microsoft упорно трудилась в течение последних нескольких лет, чтобы использовать все свои серверные продукты в PowerShell. Таким образом, неудивительно, что Диспетчер Виртуальных машин включает в себя интерфейс PowerShell, известный как Командная Оболочка VMM.

Последний главный компонент - это сервер библиотеки VMM. Как видно из названия, задачей сервера библиотеки является размещение библиотеки VMM. Библиотека является одной из наиболее важных функций Диспетчера Виртуальных Машин. Библиотека действует как набор ресурсов, которые можно использовать для развёртываний виртуальных машин. Эти ресурсы могут включать в себя такие вещи, как виртуальные жёсткие диски и шаблоны. Ресурсы библиотеки обычно основаны на файлах, поэтому задача сервера библиотеки заключается в совместном использовании папок, содержащих ресурсы библиотеки.

## Масштабируемость Диспетчера Виртуальных Машин

В предыдущей статье было объяснено, что одной из задач Диспетчера Виртуальных Машин является улучшение масштабируемости за счёт обеспечения представления ресурсов виртуальной машины на уровне организации, а не ограничивать администратора работой с хостами виртуальных машин от сервера к серверу (как и с Диспетчером Hyper-V). Поскольку обеспечение масштабируемости является такой важной частью работы Диспетчера Виртуальных Машин, уделим некоторое время рассмотрению степени масштабируемости, предоставляемой Диспетчером Виртуальных Машин.

Microsoft предоставляет некоторые цифры, которые показывают, что можно ожидать с точки зрения масштабируемости Диспетчера Виртуальных Машин. Однако важно отметить, что числа, упоминаемые Microsoft, являются теоретическими максимумами. Существует также практический аспект для рассмотрения. Если необходимо развернуть Диспетчер Виртуальных Машин на сервере, который едва соответствует минимальным требованиям к оборудованию, то нереалистично ожидать, что можно будет эффективно управлять крупномасштабными средами.

Стоит также отметить, что со временем числа масштабируемость Microsoft изменились. В System Center 2012 SP1 были внесены значительные улучшения масштабируемости Диспетчера Виртуальных Машин. Этот пакет обновления предоставляет те же числа масштабируемости, что и Диспетчер Виртуальных Машин System Center 2012 R2. Числа, упоминаемые в этой части статьи, основаны на этом пакете обновлений и на Диспетчере Виртуальных Машин System Center 2012 R2.

С учётом этого, Диспетчер Виртуальных Машин может поддерживать до 1000 виртуальных машин. Для сравнения, предыдущий лимит был 400. Можно заметить, что использована фраза «хосты виртуальных машин», а не «хосты Hyper-V». Причина этого в том, что, хотя Диспетчер Виртуальных Машин в первую очередь предназначен для использования с Hyper-V, его также можно использовать для управления хостами Citrix XenServer и VMware ESX. Таким образом, SCVMM может использоваться для управления разнородными гипервизорами через единый интерфейс управления. Существуют некоторые ограничения, которые возникают при управлении гипервизорами не от Microsoft, но сейчас не время, чтобы это обсуждать.

Так же, как Диспетчер Виртуальных Машин ограничивает общее число хостов виртуальных машин, которыми можно управлять, есть ограничение на общее число виртуальных машин, которыми можно управлять. Ограничение составляет 25 000 виртуальных машин.

Существуют также некоторые ограничения, которые вступают в действие с точки зрения управления. Диспетчер Виртуальных Машин поддерживает до 50 одновременных клиентов управления. Другими словами, может быть открыто до 50 копий консоли управления или может быть установлено до 50 сессий Оболочки Управления VMM. Если используется оба инструмента одновременно, общее количество соединений не может превышать 50.

Стоит также отметить, что Сервер Управления VMM обычно не устанавливается непосредственно на хост Hyper-V. Таким образом, Сервер Управления VMM ведёт себя аналогично прокси-серверу. Администратор выдаёт команды управления через консоль управления или через оболочку управления, и эти команды отправляются на Сервер Управления VMM. Сервер Управления VMM получает команды и интерпретирует их. Затем он передаёт необходимые команды хосту целевой виртуальной машины.

Фактические задачи управления не выполняются локально на сервере управления, а выполняются на удалённом хосте виртуальной машины. В этом случае большинство задач управления рассматриваются как задания (в отличие от локальных команд, выполняемых мгновенно). Причина, по которой это упоминается, состоит в том, что существует ограничение на общее количество одновременных заданий, которые можно запустить. Ограничение составляет 250 заданий. Кстати, Записи Истории Заданий Диспетчера Виртуальных Машин могут хранить данные о последних пяти миллионах заданий, которые были выполнены.

Ещё одна вещь, о которой необходимо упомянуть, - это то, что Диспетчер Виртуальных Машин предназначен для предоставления многопользовательских виртуальных серверов. Диспетчер Виртуальных Машин имеет теоретический предел 1000 арендаторов. В действительности, однако, реальное число арендаторов, которые могут поддерживаться, может быть намного ниже. Причина этого заключается в том, что Диспетчер Виртуальных Машин ограничивает количество ролей пользователей, которые могут быть созданы. Это ограничение также равно 1000. Таким образом, единственный способ, которым Диспетчер Виртуальных Машин может поддерживать 1000 арендаторов, заключается в том, что каждый арендатор использует только одну роль пользователя. Роли пользователей и многопользовательская аренда будут подробно рассмотрены далее в этой статье.

Развёртывание одиночного сервера Диспетчера Виртуальных Машин System Center 2012 R2. Развёртывание будет запущено в Windows Server 2012 R2, и на сервере будет установлен SQL Server 2012 локально. Сервер также полностью исправен.

С учётом вышесказанного, можно установить Диспетчер Виртуальных Машин System Center 2012 R2, вставив установочный DVD-диск и запустив Setup.exe. Когда появится экран заставки, нажмите на ссылку «Установить». После этого программа установки скопирует некоторые файлы, а затем запустит Мастер Установки Диспетчера Виртуальных Машин Microsoft System Center 2012 R2.

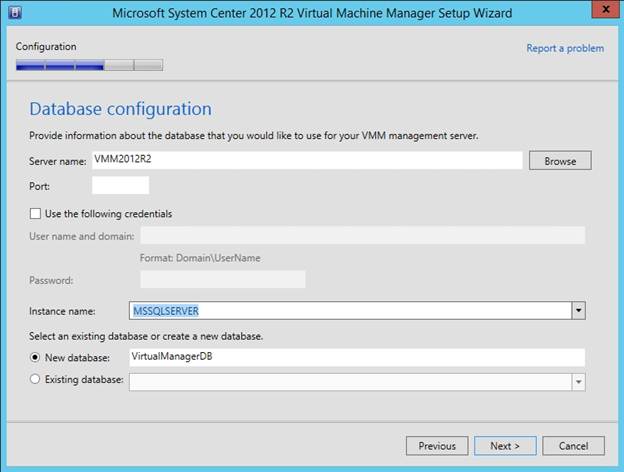
На первом экране мастера установки появится запрос на то, какие компоненты необходимо установить. Для целей этой статьи установим Сервер Управления VMM и консоль VMM на один сервер. В этом случае установите оба флажка, как показано на Рис.3, и нажмите «Далее». Кстати, если выбрана установка Сервера Управления VMM, то консоль VMM будет также установлена.



Следующий экран, который появится, — это экран Информации о Регистрации Продукта. Здесь вводится ключ продукта. После этого нажмите «Далее». Теперь вы должны увидеть экран, который просит вас принять лицензионное соглашение. После этого нажмите «Далее». На следующем экране появится запрос на участие в Программе Улучшения Качества Программного Обеспечения. Сделайте свой выбор и нажмите «Далее».

На этом этапе будет предложено указать желаемый путь установки. Путь установки по умолчанию обычно подходит для большинства развёртываний.

Нажмите «Далее», и программа Установки выполнит быструю предварительную проверку. Как только эта проверка завершится, появится экран Конфигурации Базы Данных. Как минимум, вам нужно будет указать имя сервера базы данных и имя экземпляра SQL Server. Как правило, потребуется создать новую базу данных для Диспетчера Виртуальных Машин. По умолчанию программа установки создаст базу данных с именем VirtualManagerDB, как показано на Рис.4.

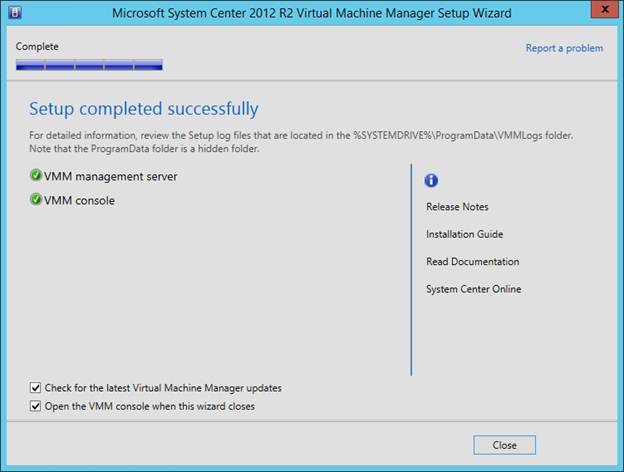
****

На следующем экране будет предложено ввести учётные данные для учётной записи, которую можно будет использовать в качестве учётной записи службы. Что ещё более важно, экран также даёт возможность сохранить ключи шифрования в Active Directory. Необязательно хранить ключи в Active Directory, если Диспетчер Виртуальных Машин не будет высокодоступным. Однако хранение ключей в Active Directory является наилучшей практикой, поскольку это помогает предотвратить потерю ключа.

Нажмите «Далее» и будет предложено выбрать порты, которые необходимо использовать для различных функций Диспетчера Виртуальных Машин. В большинстве случаев номера портов по умолчанию, будут работать нормально. Однако необходимо записать номера портов, потому что может потребоваться открыть порты в брандмауэре.

Нажмите «Далее» и появится запрос, создавать новый общий ресурс библиотеки или использовать существующий общий ресурс библиотеки. Поскольку это совершенно новое развёртывание, перейдите далее и выберите вариант создания нового общего ресурса библиотеки.

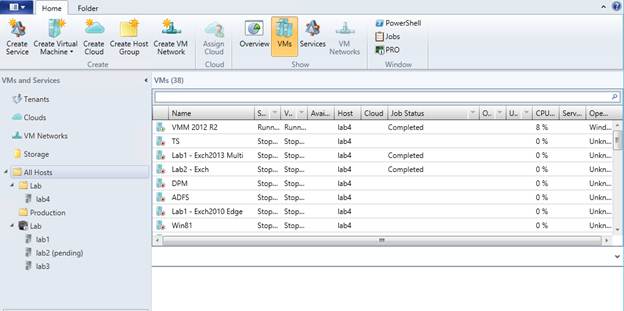
После нажатия кнопки «Далее» отобразится сводка выбранных опций установки. Найдите время, чтобы просмотреть краткое описание установки. Если итоговая информация отображается правильно, нажмите кнопку «Установить». По завершении установки отобразится сообщение, подобное показанному на Рис.5, что свидетельствует об успешной установке.



VMM отличается от Диспетчера Hyper-V тем, что он предназначен для централизованного представления виртуальных машин. Однако было бы технически точнее сказать, что VMM выделяет несколько представлений виртуальных машин.

В предыдущей части было показано, что VMM отображает группы хостов и виртуальные машины из рабочей области «Виртуальные Машины и Службы». Также было сказано, что VMM содержит группу хостов по умолчанию, называемую «All Hosts». Группа «All Hosts» содержит все серверы Hyper-V, которые находятся под управлением VMM.

Таким образом, с учётом вышесказанного, SCVMM выделяет три основных представления виртуальных машин. Первым из этих представлений является «All Hosts». Если выбрать контейнер «All Hosts», то список виртуальных машин будет включать в себя все виртуальные машины со всех хост-серверов, которыми управляет Диспетчер Виртуальных Машин.



Второе представление, которое можно использовать для виртуальных машин, - это представление группы хостов. Например, выбрана группа хостов «Lab». Это заставляет Диспетчер Виртуальных Машин отобразить только виртуальные машины, которые находятся на хостах, которые являются частью выбранной группы хостов. Можно заметить, что количество виртуальных машин в списке падает до 26.

Контрольные вопросы

1. Что такое VMM?
2. Расскажите о развертывании одиночного сервера

**Лекция №3**

Реализация библиотек и профилей диспетчера виртуальных машин. Планирование и развертывание служб VMM

Рассматриваемые вопросы

1.Реализация библиотек и профилей VMM

2.Развертывание служб VMM

Профиль VMM содержит параметры, которые используются при создании виртуальной машины или шаблона виртуальной машины. Профили упрощают развертывание, помогая быстро создавать виртуальные машины с согласованными параметрами. Профили можно использовать для ограничения параметров, доступных для пользователей самообслуживания, которые создают виртуальные машины.

## Создание профиля операционной системы виртуальной машины

1. В консоли VMM щелкните **Библиотека** > **Создать** > **Профили ОС виртуальной машины**.
2. На вкладке **Создать профиль ОС виртуальной машины** > **Общие** введите имя профиля. На странице **Профиль ОС виртуальной машины** задаются параметры ОС.
3. В поле **Общие параметры** > **Операционная система** укажите операционную систему виртуальной машины. В поле **Сведения об удостоверении** укажите фактическое имя виртуальной машины. Возможно, потребуется задать уникальные имена. Чтобы для каждой виртуальной машины создавалось новое имя, можно использовать подстановочный знак. Можно также использовать символы ###, чтобы добавить в имена увеличивающееся числовое значение. Например, если ввести ContosoVM-#, создаются машины с именами ContosoVM-01, ContosoVM-02 и т. д. В поле **Пароль администратора** укажите, требуется ли пароль локальному администратору. Можно использовать предопределенную учетную запись запуска от имени. В поле **Ключ продукта** введите ключ для установки операционной системы. Если в области **Сценарии** добавлен файл ответов, можно выбрать параметр **Ключ продукта, указанный в файле ответов**. В поле **Часовой пояс** укажите часовой пояс, в котором находится виртуальная машина.
4. В разделе **Роли и компоненты** укажите, что необходимо установить на виртуальной машине. Имейте в виду, что этот параметр применяется только для профиля в шаблоне виртуальной машины, который затем используется в шаблоне службы.
5. В разделе **Сетевые подключения** укажите параметры домена для виртуальной машины и учетные данные, которые следует использовать для присоединения к домену.
6. В области **Сценарии** укажите скрипты, которые следует использовать для виртуальной машины. Скрипты должны находиться в общей папке библиотеки. Это может быть, например, установочный файл ответов. Параметр **GUIRunOnce** позволяет выполнять скрипт при первом входе пользователя в виртуальную машину.
7. Завершив создание профиля ОС виртуальной машины, вы можете щелкнуть его правой кнопкой мыши, чтобы настроить дополнительные свойства. На вкладке **Зависимости** приводятся все зависимости профиля. Это могут быть, например, учетные записи запуска от имени. На вкладке **Доступ** приводятся роли или пользователи, имеющие разрешения на использование этого профиля.
8. Создав профиль ОС виртуальной машины, вы можете использовать его при настройке виртуальной машины или шаблона виртуальной машины.

## Создание профиля приложения

1. В консоли VMM щелкните **Библиотека** > **Создать** > **Профили приложений**.
2. На вкладке **Создание профиля приложения** > **Общие** введите имя профиля. На вкладке **Конфигурация приложения** можно задать параметры приложения.
3. В разделе **Конфигурация приложения** > **Совместимость ОС** укажите операционные системы виртуальных машин, совместимые с профилем приложения.
4. Нажмите кнопку **Добавить**, а затем выберите тип приложения или скрипта, который требуется применить к профилю. Для развертывания приложения любого типа выберите **Общий**. Для развертывания пакетов приложений уровня данных SQL Server или скриптов выберите **Узел приложений SQL Server**, чтобы в профиль можно было добавлять пакеты и скрипты. Для развертывания веб-приложений выберите **Узел веб-приложений**, чтобы в профиль можно было добавлять пакеты веб-развертывания и скрипты.
5. Если выбран вариант **Общий**, в профиль можно добавить несколько приложений или скриптов.
6. Для приложений можно задать такие параметры, как сертификат, порты и папки.Можно также указать, что развертыванием приложения должен управлять скрипт.Вы можете указать имя скрипта и то, когда он должен выполняться.
7. Выберите **Сценарии**, чтобы добавить неограниченное количество скриптов и свойств, например параметров безопасности. Например, можно настроить скрипт так, чтобы он создавал гостевой кластер на основе нескольких виртуальных машин, развернутых службой VMM. Например, можно указать, что один сценарий будет выполняться при выборе параметра "Создание: первая виртуальная машина" (для формирования кластера на первой виртуальной машине), а другой сценарий будет выполняться при выборе параметра "Создание: виртуальные машины после первой (для добавления дополнительных виртуальных машин в кластер).
8. По завершении можно проверить, создан ли профиль, на странице **Библиотека** > **Профили** > **Профили приложений**.
9. Профили приложений используются в шаблонах служб. Например, можно создать несколько шаблонов виртуальных машин с профилями оборудования и ОС. Затем можно создать шаблон службы, включающий эти шаблоны виртуальных машин, и профили приложений с целью создания набора виртуальных машин, настраиваемых и развертываемых как единое целое.

## Создание профиля SQL Server

1. В консоли VMM щелкните **Библиотека** > **Создать** > **Профили SQL Server**.
2. На вкладке **Создание профиля SQL Server** > **Общие** введите имя профиля. На вкладке **Конфигурация SQL Server** можно задать параметры приложения.
3. Выберите **Конфигурация приложения** > **Добавить** > **Развертывание SQL Server**. Развертывание SQL Server соответствует отдельному экземпляру SQL Server.Если на одной виртуальной машине должно быть несколько экземпляров SQL Server, необходимо создать несколько развертываний.
4. В разделе **Развертывание SQL Server** щелкните **Развертывание 1** и укажите имя развертывания, а также сведения об экземпляре SQL Server. Учетная запись запуска от имени является необязательной. Если ее не указать, используется учетная запись службы VMM.
5. В разделе **Конфигурация** введите путь к установочному файлу SQL Server (setup.exe) и укажите администраторов SQL Server.
6. В разделе **Учетная запись службы** укажите учетные записи, которые следует использовать.

## Создание профиля возможностей

Точные параметры профиля возможностей зависят от используемого профиля. В качестве примера давайте настроим профиль возможностей Hyper-V, чтобы задать высокую доступность для ресурсов, используемых в частном облаке VMM.

1. В консоли VMM щелкните **Библиотека** > **Создать** > **Профили возможностей**.
2. На вкладке **Создание профиля возможностей** > **Общие** введите имя профиля. На странице **Возможности** задаются параметры профиля.
3. В разделе **Возможности** > **Совместимость с библиотекой Fabric** выберите **Узел виртуализации Hyper-V**. Также можно настроить пользовательский профиль возможностей.
4. Настройте параметры конфигурации оборудования для профиля. Эти параметры аналогичны используемым в [профиле оборудования](https://docs.microsoft.com/ru-ru/system-center/vmm/library-profiles?view=sc-vmm-1711#create-a-hardware-profile). Однако в профилях возможностей они представляют ограничения, а не точные значения.
5. В разделе **Дополнительно** > **Доступность** выберите **Режим высокой надежности VM** > **Использовать значение по умолчанию** > **Требуется**.
6. Завершите работу мастера. Создав профиль, вы можете выбрать и включить его на странице **Виртуальные машины (VM) и службы** > имя облака > **Свойства** > **Профили возможностей**.
7. Помните, что все остальные профили и шаблоны, используемые для виртуальных машин в облаке, должны соответствовать требованиям профиля возможностей и параметру высокого уровня доступности.

## Создание профиля физического компьютера

С помощью службы VMM можно подготавливать физические компьютеры на узлах Hyper-V или на масштабируемом файловом сервере. При подготовке физических компьютеров можно использовать профиль физического компьютера для задания параметров компьютера. Чтобы создать профиль физического компьютера, выполните указанные ниже действия.

1. В консоли VMM щелкните **Библиотека** > **Создать** > **Профиль физического компьютера**.
2. В разделе **Создание профиля физического компьютера** > **Определение профиля** введите имя и описание профиля.
3. В разделе **Образ ОС** выберите виртуальный жесткий диск из общей папки библиотеки. На нем должна быть установлена ОС Windows Server 2012 R2 или более поздней версии. Для создания жесткого диска можно создать виртуальную машину, установить на ней операционную систему, а затем запустить средство Sysprep с параметрами **/generalize** и **/oobe**. Если диск является динамическим, VMM преобразует его в фиксированный во время развертывания. Рекомендуется использовать фиксированный диск, чтобы повысить производительность и защитить данные пользователей.
4. В разделе **Конфигурация оборудования** настройте сетевые адаптеры, диски и разделы, а также все драйверы.
5. Чтобы присвоить адаптеру имя в соответствии с правилами согласованного именования устройств (CDN), в разделе **Сетевые адаптеры** щелкните **Свойства подключений**. Укажите, следует ли выделять IP-адрес с помощью DHCP или из статического пула. В случае с физическим сетевым адаптером, подключенным к логическому коммутатору, этот параметр недоступен.
6. В разделе **Диск** укажите схему секционирования для первого диска. Выберите вариант "Основная загрузочная запись (MBR)" для BIOS или "Таблица разделов GPT" для EFI. Укажите метку тома, размер свободного дискового пространства, который следует использовать, и загрузочный раздел. VMM копирует VHD- или VHDX-файл в загрузочный раздел и автоматически создает системный раздел на том же диске.
7. В разделе "Фильтр драйвера" укажите файлы драйверов, которые будут применяться к операционной системе во время развертывания. Драйверы можно фильтровать по идентификаторам Plug and Play или по определенным тегам. Для использования тегов необходимо добавить файлы драйверов в библиотеку и присвоить соответствующие теги общей папке библиотеки перед развертыванием.
8. В разделе **Конфигурация ОС** настройте домен, пароль локального администратора, имя и организацию, группу по продукту, часовой пояс и файл ответов с дополнительными параметрами установки. В разделе "GUIRunOnce" можно указать команды или скрипты, которые должны выполняться при первом входе пользователя в компьютер.
9. Проверьте параметры на странице **Сводка** и нажмите кнопку **Готово**. Чтобы проверить, создан ли профиль физического компьютера, выберите **Библиотека** > **Профили** > **Профили физических компьютеров**.

Контрольные вопросы

1. Что значит конфигурации ОС?
2. Что значит профиль приложения?

**Лекция №4**

**Проектирование и внедрение инфраструктуры лесов и доменов Active Directory Domain Services** Проектирование леса AD DS

Рассматриваемые вопросы:

1.Проектирование и внедрение инфраструктуры и доменов ADDS

2. Проектирование леса AD DS

Проектирование структуры Леса

Проектирование Active Directory начинается с проектирования основной структуры Леса (forest). Лес Active Directory выступает границами безопасности для создаваемой инфраструктуры идентификации. Когда вы развёртываете свой самый первый контроллер домена в вашей инфраструктуре, он создаёт также и некий Лес. Всякая инфраструктура Active Directory обладает по крайней мере одним Лесом.

Существует две разновидности реализации Леса:

Отдельный Лес

Множество Лесов

Развёртывание с отдельным Лесом является установленным по умолчанию режимом. Большинство моделей ведения дел укладываются в модель с отдельным лесом. Для этой модели сложность и стоимость реализации минимальны. Один из основных моментов, который вам требуется рассматривать для данного режима это репликации. Домены используются для деления на разделы основного каталога и управления необходимыми репликациями. Однако данные для всего Леса, такие как схемы, всё ещё требуется реплицировать между всеми доменами. Когда в репликации вовлечены офисы филиалов, вам требуется гарантировать надлежащую обработку репликаций по всему Лесу.

Модель со множеством Лесов является сложным процессом реализации. Общая стоимость реализации также выше, ибо требует дополнительных ресурсов (аппаратных, программных и сопровождения). Имеется ряд причин зачем вам может потребоваться модель со множеством лесов:

* **Изолированность бизнес операций**: Ваши бизнесы могут иметь группы компаний или подразделений, которым требуется работать независимо. Их зависимость от прочих поразделений и партнёрских компаний может быть минимальной. В подобной ситуации будет лучше создавать для них обособленные леса.
* **Быстрые изменения в службах каталога**: Бизнес может иметь некие подразделения или бизнес единицы, которые вовлечены в быстрые изменения каталога. Например, среды R&D, проверок DevOps и подразделения разработки программного обеспечения могут требовать измеения схемы, игтеграции с Active Directory и изменения Групповых политик для проверок или разработки своих пролуктов и служб. Будет лучше оставлять их в обособленном Лесу чтобы минимизировать их воздействие на всю инфраструктруру идентификации.
* **Режим работы ИТ**: Некоторые организации имеют децентрализованную работу ИТ. Примером этого могут служить группы компаний. Каждая компания может иметь свой собственный персонал ИТ, причём требуется его независимая работа. Некий обособленный Лес задаст границы безопасности и действий для каждой из таких компаний.
* **Изоляция ресурсов**: Это является идеальным решением для поставщиков служб или организаций со множеством обособленных Лесов, которые желают совместно использовать свои ресурсы. Например, Rebeladmin Corp. обладает некой группой компаний с обособленными Лесами AD. Каждая из компаний имеет своё собственное подразделение ИТ. Однако их материнская компания всё ещё желает совместно использвать некие общие системы для всех своих компаний, например, платёжные ведомости, электронную почту и CMS (компьютеризованной производственной системой). Создание некого отдельного Леса для таких ресурсов позволит данной организации управлять ими действенным и безопасным способом. Прочие Леса могут иметь домерительные отношения леса с таким Лесом ресурсов и пользоваться размещёнными там службами. Кроме того, поставщики служб могут создавать Леса ресурсов для изоляции своих продуктов и служб.
* **Требования наследования**: Дела ограничены государстенными правилами и регулированием. Вы можете также иметь бизнес- соглашения с партнёрами и объединёнными компаниями. На основании этого может потребоваться создение некого отдельного леса для изоляции данных, служб и идентификации.
* **Приобретения или отчуждения бизнеса**: Приобретения или отчуждения бизнеса требуют расширения границ безопасности или изоляции ресурсов и идентичности. Наилучшим способом осуществления этого будет использование модели со множеством лесов. Когда требуется разделение данных или ресурсов между Лесами, могут устанавливаться доверительные отношения между Лесами.

После принятия решения относительно режима Леса наш следующий этап состоит в создании необходимой структуры Леса. Для этого нам требуется принять решение собираемся ли мы достигать автономии и изоляции.

**Автономность**

Автономия предоставляет вам независимый контроль ресурсов. Та среда Active Directory, которая осредоточена на автономности, поможет администраторам независимо управлять их ресурсами, однако будут иметься и более привилегированные администраторы, которые смогут управлять этими ресурсами и привилегиями прочих администраторов.

Существует два вида автономии:

* **Автономность служб**: Она предосавляет полномочия персонам или группам администраторов контролировать целиком или частично уровень служб AD DS. Например, она позволит администраторам добавлять или удалять контроллеры домена, изменять установленную схему Active Directory и изменять DNS без владельца данного Леса.
* **Автономность данных**: Предоставляет полномочия персонам или группам администраторов для контроля данных, хранимых в Active Directory или присоединённых к домену контроллеров. Это также позволит вам выполнять любые относящиеся к данным административные задачи без поддтверждения на то некого привилегированного пользователя. Такая автономность не препятствует администраторам служб Леса в доступе к данным.

**Изоляция**

Изоляция даёт независимый и привилегированный контроль над имеющимися ресурсами. Администраторы способны независимо контролировать ресурсы, причём никакие иные учётные записи не способны получать контроль.

Существует два вида изоляции:

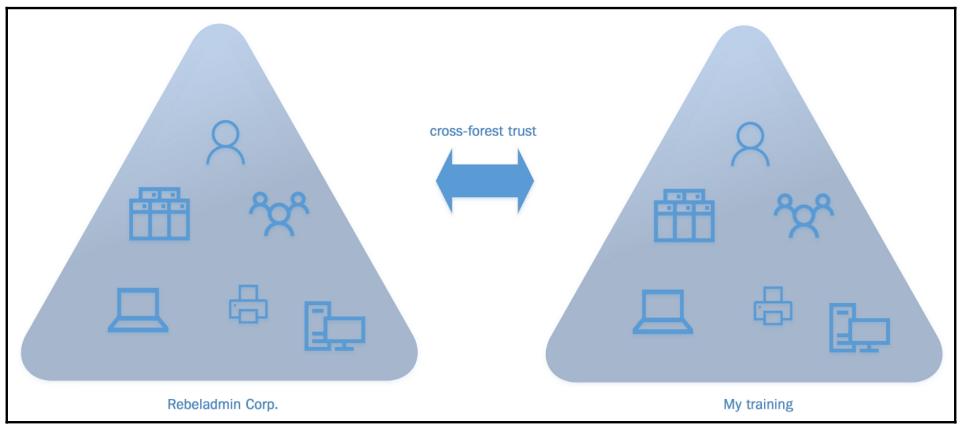
* **Изоляция служб**: Она предотвращает всякий прочий контроль или взаимодействие с AD DS, отличными от тех, для которых определены эти администраторы. Иными словами, она предоставляет полный контроль над данной инфраструктурой идентификации. В основном изолирование службы происходит по причине рабочих или юридических требований. Например, Rebeladmin Corp. имеет три различных службы, которые построены локально. Каждая из служб обладает своей собственной базой потребителей. Работа с одним продуктом не должна оказывать воздействия на работу с прочими. Изоляция службы позволит данной организации изолировать действия для каждой службы.
* **Изоляция данных**: Предоставит обладание теми данными, которые хранятся в Active Directory или подключённых к домену компьютерах для персон или групп администраторов. Однако Администраторы данных не смогут предотвращать доступ имеющихся администраторов служб для контроля ими своих ресурсов. Для полной изоляции некого подмножества данных им понадобится создать некий обособленный Лес.

Общее число требуемых для некой инфраструктуры Лесов зависит от требований автономности и изолированности.

Когда принято решение по необходимой модели Леса и общем числе Лесов, нашим следующим шагом является выбор моделей проектирования Леса. Существует три модели проектирования Леса: организации, ресурсов и ограничений.

**Модель Леса организации**

При модели Леса, соответствующей организации, ресурсы, данные и идентификация будут оставаться в отдельных лесах и будут продолжать управляться независимо. Эту модель можно применять для предоставления автономности служб, изоляции служб или изоляции данных:



В нашем предыдущем примере, Rebeladmin Corp. и My training являются двумя компаниями под одной и той же материнской компанией. Согласно операционным требованиям им необходима изоляция служб. Для её осуществления инженеры создали два отдельных Леса. Каждая из компаний обладает своим собственным подразделением ИТ и независимо управляет идентичностями. Если ресурсам требуется совместное использование между двумя Лесами, это может быть выполнено через доверительные отношения между Лесами.

Модель Леса ресурса

При модели Леса, соответствующей ресурсу, для ресурсов используется некий отдельный Лес. Лес ресурса не содержит никаких учётных записей пользователя; вместо этого он содержит учётные записи служб и учётные записи администрации ресурса Леса. Для того чтобы некий Лес организации получал доступ к данному Лесу ресурсов без дополнительной аутентификации, между Лесами создаётся доверительное отношение. Модели Леса ресурсов предоставляют изоляцию служб:

Модель Леса ограничения доступа

При модели Леса, соответствующей ограничению доступа, для изоляции идентичностей создаётся некий отдельный Лес, а данные должны быть обособлены от прочих данных идентичностей организации. Между такими двумя Лесами не создаётся доверия, поэтому идентичности из одного Леса не будут иметь возможности доступа к ресурсам в другом. Для доступа к ресурсам в каждом из Лесов нам требуется иметь отдельные учётные записи пользователей. Данная модель Леса ограничения доступа предоставляет изоляцию данных:

В нашем предыдущем примере Rebeladmin Corp. вовлечена в некий процесс лишения прав корпорации. Для неких активов здесь требуется полная изоляция данных и идентичностей. Для осуществления этого компания вводит Лес ограничения доступа.

Раз необходимая структура Леса, общее число Лесов и их модели проектирования были завершены, нашим следующим этапом будет проектирование необходимой струтктуры доменов.

Проектирование конкретной структуры домена

Всякий AD DS Лес имеет по крайней мере одним доменом. Когда вы устанавливаете свой первый Лес доменов, это также установит и некий домен по умолчанию. Имеется несколько причин почему вам может потребоваться рассмотреть возможность множества доменов в одном лесу:

Меньшие административные границы: Active Directory способна управлять примерно 2 миллиардами объектов. Наличие большого каталога создаёт ночные кошмары администратора. Представьте себе выпас большого стада овец. По мере роста этого стада, пастуху требуется всё больше и больше усилий по присмотру за ним. Хищники также могут извлекать из этого выгоду, и, порой, пастухи могут не замечать пропажи овцы, поскольку они слишком заняты погонкой всего гурта. Вместо совместного выпаса большого числа овец, не лучше ли будет каждому пастуху пасти стадо меньшего размера? Домены помогут установить административные границы меньшего размера и меньшие цели управления. Это способствует более действенному управлению ресурсами организации.

Репликация: Каждый домен в своём Лесу Active Directory совместно использует одну и ту же схему. Требуется её репликация во все контроллеры домена. Однако каждый домен имеет свой собственный раздел, который требуется реплицировать только в контроллеры домена внутри этого домена. Это делает для вас возможным управление необходимыми репликациями внутри общего Леса Active Directory. Rebeladmin Corp. имеет филиалы в различных странах. Эти филиалы соединены между собой выделенными линиями связи. Каждый такой филиал также обладает установленным контроллером домена. Таким образом, когда имеется некая установка единственного- леса- единственного- домена, абсолютно все контроллеры домена будут реплицироваться друг в друга. Выделенные линии между странами не дешёвы, и это не всегда высокоскоростные соединения. Когда мы создаём различные домены для представления каждого из филиальных офисов, это исключит необходимость репликаций, поскольку разделам домена требуется лишь реплицироваться в пределах границ самого домена.

Безопасность: В своём предыдущем разделе мы обсуждали изоляцию данных и служб на основании Лесов. Она обусловлена операционными или юридическими требованиями в самом бизнесе. Домены способствуют изоляции ресурсов и объектов на основе требований безопасности в рамках своего Леса. My-Learning Inc. является некой ИТ компанией. Она в целом имеет два вида обучающихся. Некоторые являются академическими студентами, изучающими соответствующую программу HND (высших национальных дипломов, UK), а прочие - это студенты, сдающие свои профессиональные экзамены. Обе группы имеют различные лабораторные занятия, программное обеспечение и доступ к ресурсам. Обе группы обладают различными данными, ресурсами и требованиями идентификации безопасности. Некоторые из таких требований доступны лишь через установки безопасности для всего домена. Тем самым, наличие двух отдельных доменов позволяет им применять различные стандарты безопаснсоти без пересечений.

Существуют две модели, которые мы можем применять при проектировании такой структуры домена: модель с отдельным доменом и модель региональных доменов

Модель единственного домена

Модель с единственным доменом содержит структуру единственного- домена- единственного- леса. Она проще для администрирования и имеет меньшую стоимость реализации. Когда мы впервые настраиваем инфраструктуру Active Directory, это будет именно данная модель по умолчанию. Этот домен становится доменом корня в данной модели по умолчанию с единственным доменом. Наш домен станет по умолчанию корневым доменом для своего леса и в нём будут храниться все объекты

В данном режиме все данные каталога будет необходимо реплицировать во все доступные имеющиеся доступнми контроллеры домена. Не имеет значения что они могут быть расположены в различных географических местоположениях. Сам пользователь может пользоваться для аутентификации в любой системе или ресурсах любым доступным контроллером домена. Все контроллеры домена могут действовать в этом домена в качестве серверов глобального каталога. Изнанкой этой модели будут административные накладные расходы и менее контроллируемый обмен репликациями.

Модель регионального домена

В модели регионального домена Лес AD DS содержит корневой домен Леса и множество доменов, которые подключаются через WAN (wide area networks). В основном это приемлемо для офисов филиалов и продчинённых компаний, которые расположены в различных географических местоположениях

Данная модель сложнее чем модель с единственным доменом и будет требовать добполнительного оборудования и ресурсов. В этой модели данные раздела домена будут реплицироваться в контроллеры домена внутри такого домена и это позволит вам снизить поток обмена репликациями в WAN подключениях. Эта модель также поможет вам с изоляцией требований безопасности. Обратите внимание, что она не предоставляет изолированности данных или служб. Если они необходимы, их следует выполнять на уровне соответствующего Леса.

После принятия решения по модели структуры необходимого домена, наш следующий этап состоит в выявлении общего числа требуемых доменов. Общее число доменов зависит от общего числа подлежащих управлению объектов, имеющегося числа географических местоположений, административных требований и значения полос пропускания подключений.

Домен корня леса

Самым первым настраиваемым в вашем Лесу доменом является корневой домен Леса. Такой корневой домен содержит две важные привилегированные группы, которыми выступают Администраторы компании и Администраторы схемы (Enterprise Admins и Schema Admins). Участники этих групп безопасности способны добавлять/ удалять домены и изменять имеющуюся схему Active Directory.

В модели со множеством доменов имеются два типа, которыми вы можете задать необходимый корневой домен Леса:

Выделенный корневой домен Леса: Некий обособленный домен для для работы в качестве корневого домена Леса. Он не будет содержать каких- бы то ни было учётных записей обычных пользователей, объектов или ресурсов. Он будет содержать лишь учётные записи Администраторов. Все прочие домены в этом Лесу будут дочерними доменами для такого корневого домена. В среде с единственным доменом Администраторы домена могут сами себя добавлять в группы Администраторов компании и схемы. Однако когда вы имеете отдельный корневой домен, Администраторы дочерних доменов не будут способны добавлять себя в эти привилегированные группы без осуществления этого с уровня корневого домена Леса. Такой выделенный корневой домен Леса не должен разделять каких бы то ни было географических наименований, причём он обязан устанавливать некое отдельное название для всех прочих своих дочерних доменов. Например, rebeladmin.com может быть именем корневого домена вместо Europe.rebeladmin.com.

Региональный корневой домен Леса: Когда вы не собираетесь использовать некий выделенный домен Леса, ваш региональный домен также может быть выбран в качестве корневого домена всего Леса. Он будет родительским доменом для всех прочих региональных контроллеров домена. Например, HQ.rebeladmin.com может быть нашим региональным корневым доменом. Этот домен может содержать и обычные учётные записи пользователей, группы и ресурсы.

Теперь у нас имеются все необходимые сведения для проектирования общей струткуры доменов. Наш следующий этап будет состоять в определении уровней функциональности домена и Леса.

Лес Active Directory определяет набор одного или нескольких доменов, использующих одни и те же схему, конфигурацию и глобальный каталог. Кроме этого, все домены участвуют в двусторонних транзитивных отношениях доверия. Обратим внимание на термины, которые используются в определении леса.

Домен — домен предоставляет способ организации и защиты объектов, например, пользователей и компьютеров, которые являются частью одного пространства имен. Например, windata.ru и ebay.com являются доменами. Компьютеры в каждом домене используют одинаковую конфигурацию домена и могут являться объектом применения политик и ограничений, устанавливаемых администратором домена. Использование доменов позволяет упростить обеспечение безопасности в масштабе предприятия.

Схема Active Directory используется совместно всеми доменами в пределах леса. Схема это конфигурационная информация, которая управляет структурой и содержимым каталога.

Конфигурация — конфигурация определяет логическую структуру леса, например, число и конфигурацию сайтов в пределах леса.

Глобальный каталог — глобальный каталог можно воспринимать в виде справочника для леса. Глобальный каталог содержит информацию о всех объектах леса включая информацию о расположении объектов. Кроме этого, глобальный каталог содержит информацию о членстве в универсальных группах.

Доверие — доверие предоставляет различным доменам возможность работать вместе. Без доверия домены работают как отдельные сущности, то есть пользователи из домена A не смогут получать доступ к ресурсам в домене B. Если отношение доверия устанавливается между доменами таким образом, что домен B доверяет домену A, то пользователи домена A смогут получать доступ к ресурсам домена B, если у них есть соответствующие разрешения.

Существует три основных типа отношений доверия.

Транзитивные — транзитивные отношения доверия создаются автоматически между доменами одного леса. Они позволяют пользователям любого домена потенциально получать доступ к ресурсам любого другого домена этого леса, если у пользователей есть соответствующие права доступа.

Shortcut — это отношение доверия между доменами одного леса, которые уже имеют транзитивное отношение доверия. Такое отношение доверия предоставляет более быструю аутентификацию и проверку доступа к ресурсам между несоседними доменами леса.

Внешние — внешние отношения доверия позволяют доменам из различных лесов совместно использовать ресурсы. Такие отношения доверия не являются транзитивными, то есть они относятся только к тем доменам, для которых они создавались.

Выяснив значение базовых терминов, рассмотрим пример леса. Далее представлен единый лес, который содержит два дерева доменов.

Контрольные вопросы

1.Что такое транзитивные отношения?

2. Как используется схема Active Directory

**Лекция№5**

Проектирование и реализация доверительных отношений между лесами. Проектирование интеграции ADDS с WindowsAzureActiveDirectory.

Рассматриваемые вопросы

1. Доверительные отношения

2. Интеграции ADDS

Транзитивные отношения доверия между лесами

Транзитивные отношения доверия между лесами - это двусторонние транзитивные

отношения доверия между двумя различными лесами AD DS. Установка явных доверительных отношений между отдельными доменами в различных лесах была возможна еще в Windows 2000 Server, а во всех версиях, начиная с Windows Server 2003, можно устанавливать двусторонние доверительные отношения между лесами.

Azure Active Directory (AAD)

(Служба каталогов Microsoft Cloud)

Несмотря на то, что его название звучит аналогично традиционному Active Directory, это другая служба, размещенная в Microsoft и являющаяся объектом верхнего уровня в Microsoft Cloud (O365, D365 и Azure).Содержит объекты пользователя, группы и контакта.

Windows 10 и более новые компьютеры могут присоединяться к AAD, в то время как старые компьютеры с операционной системой не могут.Может быть синхронизирован с Windows Server AD с помощью инструмента ADConnect, поэтому для обоих можно использовать одно и то же имя пользователя и пароль.Поддерживает службы федерации Active Directory (ADFS), где запросы проверки подлинности в облаке Microsoft перенаправляются в AD для проверки, а затем перенаправляются обратно в облако для доступа к ресурсам.

Доменные службы Azure Active Directory (AAD DS)

(Microsoft альтернатива Windows Server AD в Azure)

На хосте Azure Microsoft управляет AD.

Большинство из тех же возможностей, что и традиционные локальные Windows Server AD, с некоторыми ограничениями из-за отсутствия административного доступа к фактическим контроллерам домена (этим управляет Microsoft).

Синхронизируется с AAD (который синхронизируется с локальной службой Windows Server AD) и позволяет виртуальным машинам, работающим в Azure, присоединяться к ней независимо от типа ОС Windows (например, Windows 10/8/7 или Server 2008/2012/2016/2019 ).

Клиенты с облачной средой

Azure AD (AAD) должен использовать любую из служб Microsoft Cloud (например, Office 365, Виртуальный рабочий стол Windows (WVD), Dynamics 365 и т. Д.). Вся аутентификация пользователей при доступе к этим облачным службам начинается в Azure AD.

Для организаций с «облачным» развертыванием пользовательская информация (например, имя пользователя, пароль, членство в группе и т. Д.) Находится только в AAD и не синхронизируется с каким-либо другим каталогом. Если у клиента нет локальных серверов бизнес-приложений и он не хочет внедрять виртуальные рабочие столы в Azure, этот сценарий только для AAD может быть достаточным и довольно простым.

Контрольные вопросы

1.Что означает клиенты с облачной средой?

2. Что значит ADD?

**Лекция №6**

Проектирование и создание доменов AD DS. Проектирование пространств имен DNS в среде AD DS. Проектирование доверительных отношений AD DS.

Рассматриваеиые вопросы:

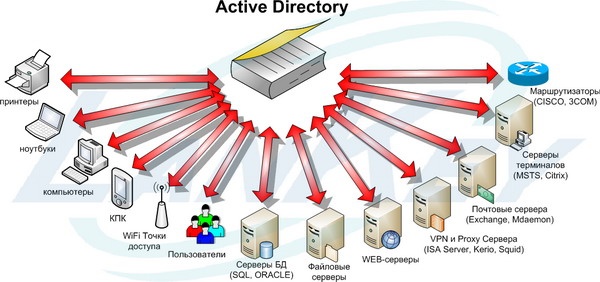
1. Создание доменов в AD DS

2. Пространство имен DNS

Домен – это основная административная единица в сетевой инфраструктуре предприятия, в которую входят все сетевые объекты, такие как пользователи, компьютеры, принтеры, общие ресурсы и т.д. Совокупность (иерархия) доменов называется лесом. У каждой компании может быть внешний и внутренний домен.

Например lankey.ru – внешний домен в сети Интернет, который был приобретён у регистратора имён. В данном домене размещён наш WEB-сайт и почтовый сервер. lankey.local –внутренний домен службы каталогов Active Directory, в котором размещаются учётные записи пользователей, компьютеров, принтеров, серверов и корпоративных приложений. Иногда внешние и внутренние доменные имена делают одинаковыми.

ctive Directory (Служба каталогов) представляет 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 Active Directory начинается построение ИТ-инфраструктуры предприятия. База данных Active Directory хранится на выделенных серверах – контроллерах домена. Служба Active Directory является ролью серверных операционных систем Microsoft Windows Server



Логическая структура AD D S позволяет выбрать ее размер и для небольтих офисов, и

для крупных международных организаций. Встроенная возможность детализации обязанностей,связанных с администрированием, позволяет делегировать управление группам пользователей или отдельным пользователям. Предоставление прав на администрирование по принципу "все или ничего" осталось в прошлом.

AD DS в основном следует модели каталогов Х.500, но обладает и рядом собственных

характеристик. Многие уже привыкли к лесам и деревьям AD DS, а некоторые ограниче

ния, которые имелись в предыдущих версиях AD DS, теперь устранены.

Чтобы понять AD DS, сначала нужно разобраться в ее основных структурных компонентах.



Пример домена в AD DS

Домен AD DS, традиционно изображаемый в виде треугольника является главной лоmческой границей AD DS.

В некотором смысле структура домена AD DS во мноrом схожа с более ранней структу­

рой доменов Windows NT 4.0, которую он заменил. Информация о пользователях и компьютерах хранится и обрабатывается внутри домена. Однако появилось несколько серьезных изменений в структуре домена и в способе ero взаимодействия с другими доменами в структуре AD DS.

Домены в AD DS разграничивают административную безопасность для объектов и со­

держат собственные политики безопасности. Важно помнить, что домены представляют

собой логическую организацию объектов и моrут охватывать несколько физических место­

положений. Значит, уже не нужно создавать множество доменов для различных удаленных

офисов или вычислительных центров, поскольку вопросы репликации и безопасности те­

перь rораздо удобнее решать с помощью сайтов AD DS или контроллеров RODC.

Пространство имен DNS представляет собой логически ограниченную область, об­разуемую именем DNS и его поддоменами. Например, именаcompanyabc.com, asia. companyabc. com и companyabc. com являются частями одного и того же непрерыв­ного пространства имен DNS. Пространство имен DNS в Active Directory может как публи­коваться в Интернете, например, в виде microsoft. com или msn. com, так и скрываться от всех, что зависит стратегии и потребностей в безопасности тех, кто ее реализует.Внешние (опубликованные) пространства имен. Имя DNS, которое может быть доступным из любого места в Интернете, называется опубликованным или внешним пространством имен. Пространства имен такого типа раньше часто применялись в тех организациях, которые для полного удобства хотели, чтобы их обычно исполь­зуемое в Интернете имя домена представляло структуру AD DS. Однако в настоящее время появились практические приемы, которые делают такую модель менее при­влекательной.

* Внутренние (скрытые) пространства имен. Для многих организаций публикация внутренней доменной структуры является слишком рискованной с точки зрения безопасности. Такие организации могут создавать схемы AD DS с внутренним про-странством имен, не доступным для чтения из Интернета. Например, компания может иметь внешнее пространство имен DNS company.com но решить, что структура AD DS должна соответствовать сompany.internal или какому-то другому пространству имен.
* В Active Directory существует два различных вида доверительных отношений: «однонаправленные» и «двунаправленные». В первом случае один домен доверяет другому, но не наоборот. Пользователи Домена 1 могут получить доступ к ресурсам Домена 2, однако у пользователей Домена 2 нет доступа к ресурсам Домена 1. Естественно, возможен и обратный случай. Другие варианты доверительных отношений: «исходящие» и «входящие». При исходящих доверительных отношениях Домен 1 доверяет Домену 2, т. е. пользователи Домена 2 могут обращаться к ресурсам Домена 1.
* При таком процессе домен, от которого доверительные отношения исходят, является доверяющим доменом (Trusting Domain). Домен с входящими доверительными отношениями — доверенный домен (Trusted Domain), в нем создаются учетные записи пользователей, обладающих правами в доверяющем домене.

**Лекция №7**

**Проектирование и реализация инфраструктуры подразделений (OU) и разрешений AD DS**

Планирование делегирования административных задач. Проектирование структуры подразделений OU.

Рассматриваемые вопросы

1.Инфраструктура подразделений OU

2. Разрешения AD DS

Организационное подразделение (Organizational Unit — OU) представляет собой контейнер в домене Active Directory, который может содержать различные объекты из того же самого домена AD: другие контейнеры, группы, аккаунты пользователей и компьютеров. OU представляет собой единицу административного управления внутри домена, на который администратор может назначить объекты групповых политик и назначить разрешения другим пользователем.

Таким образом, выделим две основные задачи использования OU кроме хранения объектов Active Directory

Делегирование управления и административных задач внутри домена другим администраторам и обычным пользователям без предоставления им прав администратора домена;

Назначение групповых политик на все объекты (пользователей и компьютеры), которые находятся в данном подразделении (OU).

Структура OU в Active Directory

В небольших инфраструктурах AD (20-50 пользователей) необязательно создавать новые OU, можно все складывать в дефолтные контейнеры в корне (Users и Computer). В большой инфраструктуре желательно разделить все объекты на разные контейнеры. В основном используется иерархический дизайн Organizational Unit в AD, по географическому или функциональному принципу.

К примеру, у вашей организация имеются подразделения в разный странах и городах. Было бы логично на верхнем уровне домена создать отдельные контейнеры для каждой страны, а внутри страны отдельные контейнеры для города / региона / области. Внутри последних можно создать отдельные контейнеры для администраторов, групп, компьютеров, серверов и пользователей (см скриншот). При необходимости вы можете добавить дополнительные уровни иерархии (здания, отделы и т.д.). С такой иерархией вы сможете гибко делегировать полномочия в AD и назначать групповые политики.

Как делегировать полномочия на OU

При делегировании полномочия на OU другим пользователям желательно предоставлять права не непосредственно учетным записям пользователям, а административным группам. Таким образом, чтобы предоставить права на OU новому пользователю достаточно добавить его в предварительно созданную доменную группу.

Чтобы настроить разрешения Active Directory для учетной записи соединителя AD DS, можно использовать следующие командлеты PowerShell. Их можно использовать для каждой функции, какую вы включаете в Azure AD Connect. Чтобы избежать проблем, следует заранее подготовлять разрешения Active Directory каждый раз, когда вы хотите установить Azure AD Connect, используя личный домен для подключения к вашему лесу. Модуль ADSyncConfig также можно использовать для настройки разрешений после развертывания Azure AD Connect.

Одно из важнейших достоинств Active Directory (AD) состоит в том, что в этом каталоге администраторы могут делегировать разрешения другим пользователям с желаемой степенью детализации. Реализованная в AD модель делегирования разрешений в сфере безопасности позволяет предоставлять разрешения на выполнение рутинных задач — таких, как изменение пароля, разблокирование учетной записи или даже создание объектов и управление ими — обычным пользователям, которых по такому случаю необязательно наделять правами администратора каталога. В состав оснастки Active Directory Users and Computers (ADUC) консоли управления Microsoft Management Console (MMC) входит мастер, облегчающий решение ряда.

Подобно разрешениям в файловой системе, разрешения в каталоге AD наследуются объектами-потомками, если пользователь не дает каталогу инструкцию отменить такое наследование. Благодаря этому обстоятельству процедура предоставления администратору разрешений на выполнение той или иной операции (скажем, изменения пароля) во всех объектах заданной организационной единицы organizational unit (OU) или в иерархии OU выполняется очень легко. Если бы такой функции не было, нам приходилось бы предоставлять разрешения каждому пользователю в индивидуальном порядке.

Для применения унаследованных разрешений к дочерним объектам в AD используется внутренний фоновый процесс, именуемый распространителем дескрипторов безопасности Security Descriptor Propagator (SDProp). В очень больших сетях унаследованные разрешения обычно применяются с некоторой задержкой. Кстати, если в AD вам попадался атрибут dSCorePropagationData и вы задавались вопросом, для чего он нужен, имейте в виду, что данный атрибут используется с целью хранения информации о состоянии процесса SDProp.

После определения структуры домена организации и планирования доменного пространства имен необходимо разработать структуру организационных единиц (OU или подразделений — ОП). По информации, собранной о компании и ее персонале, необходимо определить, как лучше всего делегировать административные полномочия в доменах. Можно создать иерархию ОП в домене: в отдельном домене разместить пользователей и ресурсы, повторив структуру компании в конкретном подразделении. Таким образом, можно создать логичную и осмысленную модель организации и делегировать административные полномочия на любой уровень иерархии.  
  
В каждом домене разрешается внедрять собственную иерархию ОП. Если организация имеет несколько доменов, то можно создать структуры ОП внутри каждого домена независимо от структуры в других доменах.  
  
Организационное подразделение позволяет [4]:

* отразить структуру компании и организации внутри домена. Без ОП все пользователи поддерживаются и отображаются в одном списке независимо от подразделения, местоположения и роли пользователя;
* делегировать управление сетевыми ресурсами, но сохранить способность управлять ими, то есть присваивать административные полномочия пользователям или группам на уровне ОП;
* изменять организационную структуру компании;
* группировать объекты так, чтобы администраторы легко отыскивали сетевые ресурсы.
* Не следует создавать структуру OU исключительно ради того, чтобы просто иметь какую-то структуру: OU используются в определенных целях. К этим целям относятся   
  *Делегирование административного управления объектами****.*** Правильно разработанная структура OU позволяет администраторам эффективно делегировать полномочия. Каждое OU по умолчанию наследует разрешения, заданные для родительского OU. Аналогично объекты, содержащиеся в OU, наследуют разрешения, заданные для этого OU (и для каждого из его родителей). Наследование — эффективный способ предоставить или делегировать разрешения на доступ к объектам. Преимущество наследования в том, что администратор может управлять разрешениями на доступ ко всем объектам в OU, задавая разрешения для самого OU, а не конфигурируя все дочерние объекты по отдельности;
* ***ограничение видимости объектов.*** В некоторых организациях определенные объекты должны быть скрыты от определенных администраторов или пользователей. Даже если запретить изменение атрибутов объекта, пользователи, имеющие доступ к контейнеру с таким объектом, все равно смогут видеть, существует ли этот объект. Однако можно скрыть объекты, поместив их в OU и ограничив круг пользователей, которые имеют разрешение на список содержимого (List Contents) для этой OU. Тогда объекты, помещенные в контейнер, будут невидимы пользователям, не имеющим этого разрешения;
* ***управление применением групповой политики.*** Групповая политика позволяет применять одни и те же параметры конфигурации сразу к нескольким объектам. С ее помощью можно определять параметры пользователей (например, ограничения, налагаемые на пароли) или компьютеров. При использовании групповой политики создается объект групповой политики (Group Policy Object, GPO) — объект, связанный с доменом, сайтом или OU и содержащий параметры конфигурации, которые требуется применить.

Возможности ОП облегчат обеспечение безопасности и выполнение любых административных задач.  
  
Первый этап проектирования административной структуры защиты — планирование использования организационных единиц (OU) в каждом домене. Следующий этап проектирования этой структуры — выработка стратегии управления учетными записями пользователей, компьютеров и групп. После этого необходимо разработать эффективную реализацию групповой политики.  
  
OU служит контейнером, в который можно поместить ресурсы и учетные записи домена. Затем можно назначить OU административные разрешения и позволить содержащимся в нем объектам наследовать эти разрешения. OU могут содержать любые объекты следующих типов [3]: пользователи; компьютеры; группы; принтеры; приложения; политики безопасности; общие папки; другие OU.

### Планирование иерархии OU

При планировании иерархии ОП важно соблюсти следующие правила [4]:  
  
Хотя глубина иерархии ОП не ограничена, производительность мелкой иерархии выше, чем глубокой.  
ОП должны отражать неизменные структурные единицы организации.  
  
Существует много способов структурирования ОП в организации. На этапе планирования развертывания Active Directory важно определить, какая модель ляжет в основу иерархии ОП. Например, существуют следующие модели классификации ОП в иерархии ОП [4]:

* ***Модель деления на ОП согласно выполняемым задачам.***ОП можно создавать, учитывая функции, которые необходимо выполнять внутри организации. Верхний уровень ОП может соответствовать бизнес-подразделениям компании, при этом следующие уровни ОП — это функциональные подразделения внутри бизнес-подразделений.
* ***Географическая модель деления на ОП.***Иногда при создании ОП учитывается местоположение филиалов компании. Верхний уровень ОП соответствует региональным подразделениям организации, а второй уровень представляет физическое местоположение офисов компании.
* ***Модель деления на ОП согласно выполняемым задачам и географическому местоположению.*** В некоторых случаях две описанные выше модели создания ОП совмещают. Верхний уровень ОП учитывает, где географически расположены офисы компании. Второй уровень ОП построен на основе функциональных особенностей каждого подразделения внутри организации.
* Следует уделять особое внимание верхнему уровню структуры OU, который всегда должен отражать относительно неизменную часть структуры предприятия, чтобы его не приходилось изменять в случае реорганизации. Так, следующие типы структуры верхнего уровня основаны на постоянных характеристиках предприятия, изменение которых маловероятно [3]:
* ***Физические участки.*** В филиалах, физически расположенных в разных местах (особенно, когда компания действует на обширной территории, например в нескольких странах), часто имеются свои ИТ-отделы, поэтому у филиалов разные требования к администрированию. Создание отдельного OU верхнего уровня для каждого филиала — один из вариантов архитектуры, основанной на задачах; в зависимости от местонахождения определяются разные административные задачи.
* ***Типы административных задач.***Структура верхнего уровня, основанная на административных задачах, относительно постоянна. Какие бы реорганизации не происходили в компании, основные типы административных задач вряд ли сильно изменятся.
* ***Типы объектов.*** Как и структура, основанная на задачах, структура, в которой OU верхнего уровня соответствуют типам объектов, обеспечивает устойчивость архитектуры к изменениям.  
  При планировании структуры OU верхнего уровня для среды с несколькими доменами есть смысл подумать о создании структуры верхнего уровня, которая будет одной и той же для каждого домена сети. Создание структуры OU, одинаковой для различных доменов, позволяет реализовать единый подход к администрированию и поддержке сети.  
    
  OU нижних уровней, создаваемые в OU верхнего уровня, должны использоваться для более тонкого управления административными полномочиями или в других целях, например для применения групповой политики. При этом надо учитывать, что по умолчанию OU нижних уровней наследуют разрешения от родительских OU. Поэтому при планировании архитектуры OU необходимо определить, когда наследуются разрешения и когда они не наследуются. Архитектура OU нижних уровней должна быть как можно проще: если создать слишком глубоко вложенную структуру OU, то можно столкнуться и со снижением производительности.  
  ^

### Стандартные модели структуры OU

Наряду с перечисленными выше моделями классификации ОП в иерархии ОП можно использовать следующую терминологию для стандартных моделей

* Модель структуры OU на основе местоположения.
* Модель структуры OU на основе структуры организации.
* Модель структуры OU на основе функций.
* Смешанная модель структуры OU — сначала по местоположению, затем по структуре организации.
* Смешанная модель структуры OU — сначала по структуре, затем по местоположению.

Контрольные вопросы:

1.Что такое разрешение AD DS?

2.Поясните суть подразделения OU

**Лекция №8**

Проектирование и внедрение стратегии

групп AD DS.

**Проектирование и внедрение стратегии групповых политик .**Сбор требуемой информации для проектирования групповых политик. Проектирование и внедрение групповых политик.

Рассматриваемые вопросы:

1.Групповые политики

2.Внедрение групповых политик

Инфраструктура групповых политик Microsoft -сложная система, которая задействует

несколько средств и служб, включенных в состав серверной и клиентской операционных

систем Windows и IР-сетей, к которым подключены эти системы.

Если говорить совсем просто, груnnовые nолитики - это набор указаний для централизованной настройки и развертывания конфигураций компьютеров и IЮльзователей.

Групповая политика уже изначально содержит обширный набор параметров и может быть

расширена с помощью сторонних поставщиков и собственной разработки параметров политик опытными администраторами групповых политик. В качестве примера можно создать политику для автоматической установки сетевого принтера на всех компьютерах,

которые находятся в конкретном офисе. Еще один пример - групповая политика, определяющая профиль брандмауэра, который несколько менее ограничивает работу в корпоративной сети и обеспечивает мощную защиту при подключении рабочей станции к общедоступной беспроводной сети.

Групповые политики появились в Windows 2000 Server Active Directory. До этого отдельные

элементы групповых политик вазывались системными политиками, но их применение

было довольно ограниченным. Версия групповых политик в Windows 2000 Server оказалась

очень удобной для настройки безопасности и базовых параметров пользователей,

но в ней не хватало многих возможностей, а когда появились мобильные устройства, она

оказалась не очень состоятельной. В Microsoft Windows Server 2003 и Windows ХР инфраструктура групповых политик Windows 2000 Server была улучшена добавлением некоторых новых возможностей обнаружения сетей и новых параметров настройки компьютеров и пользователей, включая и развертывание принтеров. Но полного расцвета групповые политики достигли лишь в Windows Vista и Windows Server 2008.

Начиная с Windows Vista и Windows Server 2008, разработчики Microsoft определили два

различных типа групповых политик: локальные и доменные. Локальные групповые политики

в Windows Vista и Windows Server 2008 были, по сути, лишь отражениями параметров,

доступных для компьютеров и пользователей в групповых политиках доменов. Одна

эта возможность расширила применимасть групповых политик за пределы сред Active

Directory и сделала их гораздо более полезными для организаций, где используются рабочие

станции Windows в конфигурациях рабочих групп, или для сетевой аутентификации и

других служб в сетях, которые не обязательно основаны на Microsoft Active Directory.

Еще одним заметным изменением в групповых политиках стало введение предпочтений

групповых политик (Group Policy Pгeferences - GPP ) . К ним относятся предпочтения для

компьютеров и пользователей, и хотя они настраиваются с помощью групповых политик,

по их названию понятно, что они реализуют предпочтительные параметры конфигурации,

и большинство из них пользователь может изменить после применеимя политик. В GPP

присутствуют многие функции, которых раньше не хватало администраторам групповых

политик и которые им приходилось выполнять с помощью сценариев запуска или входа

пользователей для развертывания специальных конфигураций профилей настольных компьютеров, параметров реестра и т.д. GPP действительно изменили административный пейзаж,персместив значительную часть дополнительных настроек из сложных сценариев в

администрирование через графический интерфейс, который позволяет легко просматривать

и корректировать конфигурации.

Как уже было сказано, многие новые возможности групповых политик из инфраструктуры

Windows Vista и Windows Server 2008 были еще более усовершенствованы и расширены,

чтобы повысить изначальную функциональность. Групповые политики делятся на четыре крупных раздела: политики компьютеров, предпочтения компьютеров, политики

пользователей и предпочтения пользователей. Чтобы было понятнее, можно представить

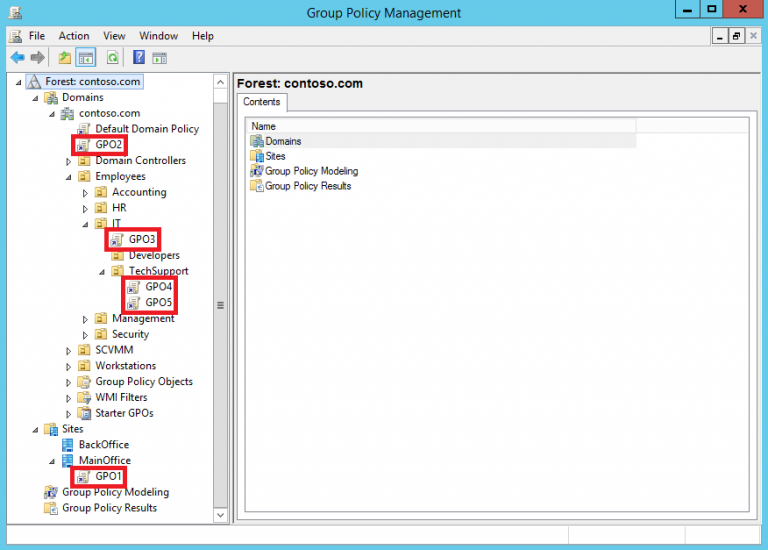
разделы политик как обязательные, а разделы предпочтений как первоначальные конфигурации, которые затем можно изменить по своему желанию.

В данной главе рассматривается администрирование и управление GPO для клиентской

ОС Windows 8 и для серверной ОС Windows Server 2012 .

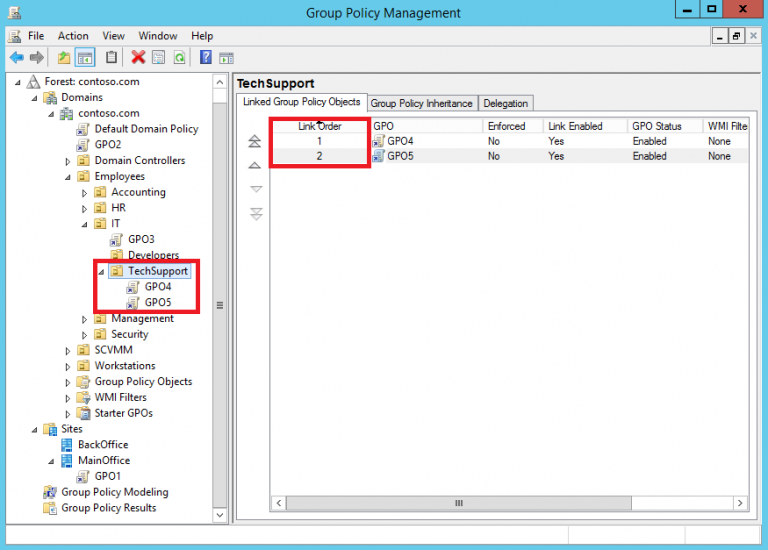
Порядок применения групповых политик напрямую зависит от их области действия. Первыми применяются локальные политики, затем политики, назначенные на сайт, затем отрабатывают доменные политики и затем политики, назначенные на OU.

Так в нашем примере (на рисунке ниже) сначала отработает локальная политика (условно назовем ее GPO0), затем политика сайта GPO1, затем политика домена GPO2, ну а затем применятся политики, назначенные на OU. При этом политики применяются в соответствии с иерархией — сначала политика GPO3, назначенная на вышестоящее OU, затем нижестоящие политики GPO4 и GPO5.



Если на одну OU назначено несколько GPO, то они обрабатываются в том порядке, в котором были назначены. Например, к подразделению TechSupport относятся GPO4 и GPO5, которые обрабатываются согласно порядку назначения (Link Order).

Политики обрабатываются в обратном порядке (снизу вверх), т.е. политика с номером 1 отработает последней. При необходимости этот порядок можно изменить, выделив политику и передвинув ее вверх или вниз с помощью соответствующих стрелок.



Контродьные вопросы

1.Поясните внедрение групповых политик

**Лекция №9**

Проектирование обработки групповых политик. Планирование управления групповыми политиками

Рассматриваемые вопросы

1.Обработка групповых политик

2.Управление групповыми политиками

Когда мы выполняем оценку требований Групповой политики для некой организации, мы можем указывать некие настройки, которые являются общими для объектов во всём домене целиком. Однако в то же самое время, некоторые установки являются уникальными для особых подразделений или групп. Все Групповые политики, которые применяются на уровне самого корня, по умолчанию будут наследоваться прочими OU. Таким образом организационные элементы способны наследовать Групповые политики, а также напрямую связываться с Групповыми политиками.

В каком порядке будут обрабатываться Групповые политики, когда к некому организационному элементу применяется множество Групповых политик? Не прекратит ли обработку какая- то из Групповых политик? Если одни и те же настройки применяются к различным политикам, какие именно будут применены? Для ответа на все эти вопросы важно понимать как работает обработка Групповых политик.

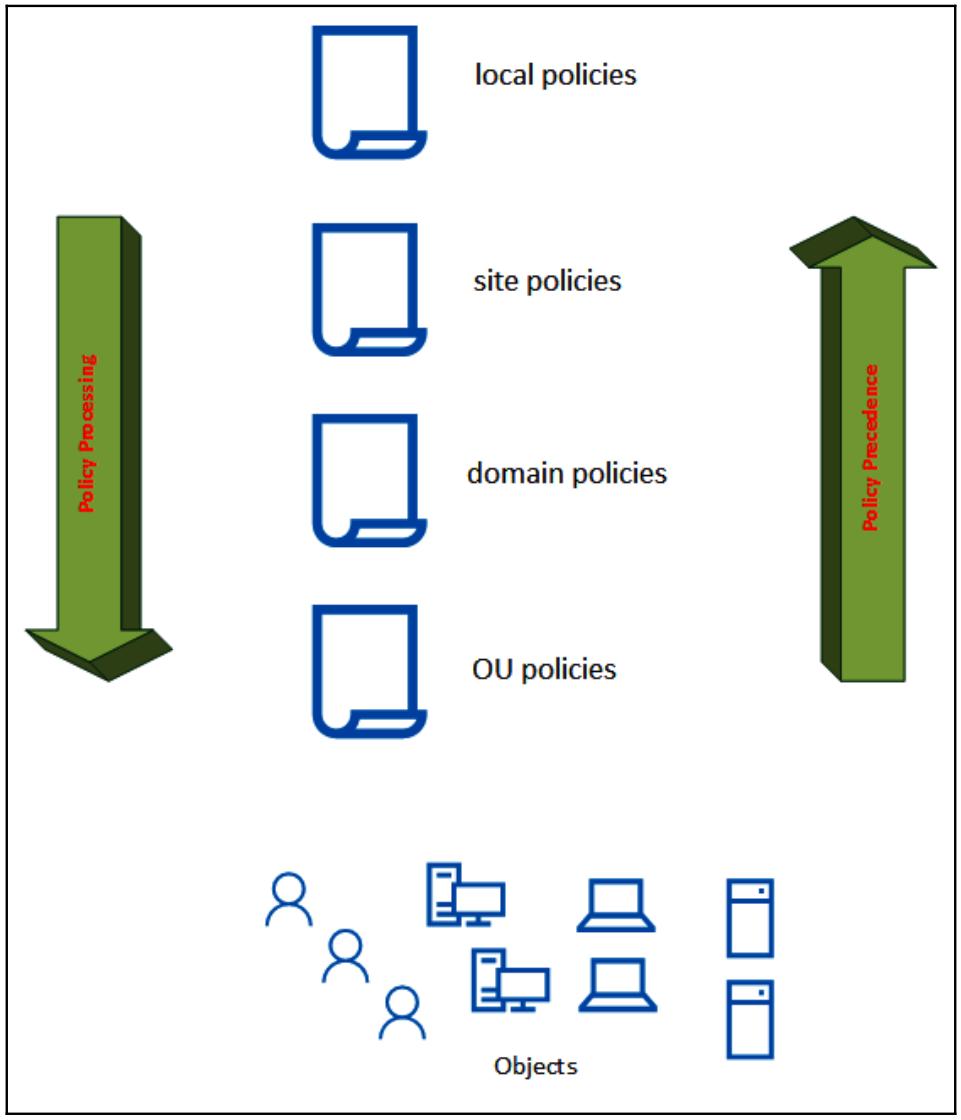
В установленной среде AD имеются два основных вида политик:

* **Локальные политики**: Сиситемы Windows поодерживвают установку локальных политик безопасности. Эти политики отличаются от GPO домена и они содержат ограниченную функциональность, которая в основном сосредоточена на установках безопасности. Они применяются к любому пользователю, который входит в данную систему (регистрируется в ней).
* **Нелокальные политики**: Данные политики являются основанными на политиках AD, которые и будут обсуждаться далее на протяжении этой главы. Эти политики применяются только к подключаемых к домену компьютерам и пользователям AD. По сравнению с локальными политиками эти политики имеют более богатые функциональные возможности.

Групповые политики могут применяться на трёх уровнях имеющейся среды AD:

* **Площадка** (Site): Групповая политика может быть привязана к некой площадке AD. Любая Групповая политика уровня площадки бкдет применяться ко всем доменам на этой площадке.
* **Домен**: Все Групповые политики, которые применяются на данном уровне домена будут применяться ко всем объектам AD пользователей и компьютеров в этом домене. По умолчанию, сама система создаёт некую политику с названием **Default Domain Policy** на уровне своего домена. В большинстве случаев политики уровня домена будут применяться для публикации настроек безопасности, которые применяются ко всей инфраструктуре целиком.
* **OU** (**Organization units**): Групповые политики уровня Организационного элемента применяются ко всем объектам пользователей или компьютеров внутри них. По умолчанию сама система создаёт некую Групповую политику уровня OU с названием **Default Domain Controllers Policy**, которая применяется к OU рассматриваемого контроллера домена. Применяемые на таком уровне OU установки Групповой политики более конкретны, так как их целевая аудитория меньше по сравнению с площадкой или доменом.

Приводимая ниже схема иллюстрирует имеющиеся в AD уровни политик:



В конкретной среде AD групповые политики будут обрабатываться в следующем порядке:

Локальные политики (Local policies

Политики площадки (Site policies)

Политики домена (Domain policies)

Политики OU (OU policies)

Обычно такой порядок именуется как LSDOU. Самой первой для обработки политикой выступает локальная политика, а самой полседней является политика OU. Это вовсе не означает, что наиболее предпочтительной политикой является локальная. Из всех четырёх политик, именно той политикой, которая удерживает самое низкое значение следования будет выигравшим GPO, которым и выступает политика OU. Данный порядок следования политик важен в случае, когда политики обладают конфликтующими значениями, потому как выигрывающей политикой является именно та политика, которая ближе всего к данному объекту. Именно политика уровня OU будет ближайшей политикой к конкретному объекту. Как я уже говорил ранее, установки политики уровня OU являются более конкретными в соответствии с организационными требованиями. Тем самым, они содержат наиболее точные настройки политики для своих целевых объектов. Данный порядок является уствановленным по умолчанию, но при наличии требований существует возможность изменения такого порядка следования.

В целом Групповые политики обрабатываются в двух различных режимах. По умолчанию, установки Групповых политик компьютера начинают обрабатываться в процессе запуска, прежде чем блок регистрации пользователя выдаст приглашение на ввод данных. Данный режим предварительного выполнения именуется обработкой с высоким приоритетом (foreground processing). На протяжении этой обработки с высоким приоритетом некоторые политики завершают выполнение, а некоторые нет. Они будут продолжены в фоновом режиме (background) после входа в систему и инициализации сетевого подключения. Кроме того, после того как пользователь вошёл в систему, по умолчанию имеющиеся групповые политики будут запускаться в фоновом режиме каждые 90 минут. Именно это и является вторым режимом обработки Групповой политики

Обработка в фоновом режиме может быть и далее разделена на два подчинённых режима. Вплоть до введения Windows XP, все те установки, которые запускались в фоновом режиме прежде чем его пользователь увидит свой рабочий стол после процесса входа в систему. Он имеет название синхронного режима. Однако после Windows XP устанавливаемым по умолчанию режимом обработки стал асинхронный, что означает, что операционная система не дожидается пока завершится процесс применения Групповых политик или до того как данный пользователь начнёт применять свой компьютер. Когда определённый компьютер представляется со своим окном регистрации в системе, в своём фоновом режиме, настройки этого компьютера, которые являются частью всех групповых политик, всё ещё будут применяться. После того как его пользователь вошёл в систему, эта система начнёт применение настроек данного пользователя как часть всех политик. Ко времени загрузки первоначального домашнего экрана, имеющиеся групповые политики могут всё ещё применяться в фоновом режиме. Существует четыре определённых Microsoft настройки политик, которые всегда применяются в синхронном режиме. Если какая- то политика имеет включённым перенаправление папки, установку программного обеспечения, квотирование диска и установку дискового соотвествия, они будут применяться в синхронном режиме. Кроме того, все сценарии запуска также будут обрабатываться синхронно в приоритетном режиме.

**Лекция № 10**

**Проектирование и реализация физической топологии AD DS.**Проектирование и реализация сайтов Active Directory.

Рассматриваемые вопросы

1.Физическая топология AD DS

2.Реализация сайтов AD

Физическая структура Active Directory служит для связи между логической структурой AD и *топологией* корпоративной сети.

Основные элементы физической структуры Active Directory — *контроллеры домена* и *сайты*.

Контроллеры домена были подробно описаны в предыдущем разделе.

**Сайт** — группа IP-сетей, соединенных быстрыми и надежными коммуникациями. Назначение сайтов — управление процессом репликации между контроллерами доменов и процессом аутентификации пользователей. Понятие "быстрые коммуникации" очень относительное, оно зависит не только от качества линий связи, но и от объема данных, передаваемых по этим линиям. Считается, что быстрый канал — это не менее 128 Кбит/с (хотя Microsoft рекомендует считать быстрыми каналы с пропускной способностью не менее 512 Кбит/с).

Структура сайтов никак не зависит от структуры доменов. Один домен может быть размещен в нескольких сайтах, и в одном сайте могут находиться несколько доменов

Поскольку сайты соединяются друг с другом медленными линиями связи, механизмы репликации изменений в AD внутри сайта и между сайтами различные. Внутри сайта контроллеры домена соединены линиями с высокой пропускной способностью. Поэтому репликация между контроллерами производится каждые 5 минут, данные при передаче не сжимаются, для взаимодействия между серверами используется технология вызова удаленных процедур (RPC). Для репликации между сайтами кроме RPC может использоваться также протокол SMTP, данные при передаче сжимаются (в результате сетевой трафик составляет от 10 до 40% от первоначального значения), передача изменений происходит по определенному расписанию. Если имеется несколько маршрутов передачи данных, то система выбирает маршрут с наименьшей стоимостью.

Кроме управления репликацией, сайты используются при аутентификации пользователей в домене. Процесс аутентификации может вызвать заметный трафик, особенно если в сети имеется большое количество пользователей (особенно в начале рабочего дня, когда пользователи включают компьютеры и регистрируются в домене). При входе пользователя в сеть его аутентификация осуществляется *ближайшим контроллером домена*. В процессе поиска "ближайшего" контроллера в первую очередь используется информация о сайте, к которому принадлежит компьютер, на котором регистрируется пользователь. Ближайшим считается контроллер, расположенный в том же сайте, что и регистрирующийся пользователь. Поэтому рекомендуется в каждом сайте установить как минимум один контроллер домена.

В процессе аутентификации большую роль играет также сервер глобального каталога (при использовании универсальных групп). Поэтому в каждом сайте необходимо также размещать как минимум один сервер глобального каталога (или на одном из контроллеров домена в каждом сайте настроить кэширование членства в универсальных группах). Пользователи сети (в том числе компьютеры и сетевые службы) используют серверы глобального каталога для поиска объектов. В случае, если доступ к серверу глобального каталога осуществляется через линии связи с низкой пропускной способностью, многие операции службы каталога будут выполняться медленно. Это обстоятельство также стимулирует установку сервера глобального каталога в каждом сайте (более подробно осерверах глобального каталога будет рассказано ниже).

В самом начале создания леса автоматически создается сайт по умолчанию с именем Default-First-site-Name. В дальнейшем сетевой администратор должен сам планировать и создавать новые сайты и определять входящие в них подсети, а также перемещать в сайты соответствующие контроллеры доменов. При созданиянового контроллера на основании выделенного ему IP-адреса служба каталога автоматически отнесет его к соответствующему сайту.

Репликация, управление топологией репликации

Рассмотрим сам процесс репликации изменений в AD как внутри сайта, так и между сайтами.

Разбивать большую корпоративную сеть на отдельные сайты необходимо по следующим причинам: отдельные подсети корпоративной сети, расположенные в удаленных офисах, могут быть подключены друг к другу медленными каналами связи, которые сильно загружены в течение рабочего дня; поэтому возникает необходимость осуществления репликации в те часы, когда сетевой трафик минимален, и передавать данные репликации со сжатием.

Вернемся к сетевой структуре, изображенной и обсудим понятия и термины, играющие важную роль в управлении репликацией между сайтами.

В этой конфигурации топология репликации также строится системной компонентой KCC. KCC выбирает контроллеры, которые осуществляют репликацию между сайтами, проверяет их работоспособность и, в случае недоступности какого-либо сервера, назначает для репликации другой доступный сервер.

Для репликации между сайтами используется тот или иной межсайтовый транспорт — это либо IP ( RPC ), либо SMTP. Для каждого вида межсайтового транспорта определяется " соединение сайтов " ( site link ), с помощью которого строится управление репликацией между двумя и более сайтами. Именно для соединения ("линка") задаются такие параметры как " Расписание репликации " и " Стоимость ". Соединение Link-1 связывает в единую цепочку сайты Сайт-1,Сайт-3, Сайт-4 и Сайт-2, соединение Link-2 связывает два сайта — Сайт-1 и Сайт-2. В данном примере репликация между сайтами Сайт-1 и Сайт-2 будет проходить либо по соединению Link-1, либо по соединению Link-2 — в зависимости от расписания, стоимости соединения и его доступности (при доступности обоих соединений преимущество будет иметь соединение с более низкой стоимостью). На рис. 6.37 изображено созданное автоматически соединение для транспорта IP (RPC ) — DEFAULTIPSITELINK. Если открыть Свойства этого соединения можно управлять списком сайтов, относящихся к этому соединению, назначать стоимость соединения (значение по умолчанию — 100), интервал репликации (по умолчанию — каждые 3 часа), а если нажать кнопку " Изменить расписание ", то можно более тонко определить дни и часы, в которые будет производиться репликация.

Контейнер Subnets консоли " Active Directory - сайты и службы " служит для описания подсетей, входящих в тот или иной сайт.

Контрольные вопросы:

1.Расскажите о процессе репликации

**Лекция №11**

Проектирование репликации Active Directory.

Проектирование размещения контроллеров домена. Виртуализация контроллеров домена

Рассматриваемые вопросы

1.Контроллер домена

2.Виртуализация контроллеров домена

Объект Connection — это Active Directory объект, представляющий подключение репликации с исходного контроллера домена к целевому контроллеру домена.Контроллер домена является членом одного сайта и представлен на сайте объектом сервера в службах домен Active Directory Services (AD DS). Каждый объект сервера имеет дочерний объект параметров NTDS, представляющий реплицируемый контроллер домена на сайте.

Объект Connection является дочерним по отношению к объекту параметров NTDS на целевом сервере. Чтобы репликация выполнялась между двумя контроллерами домена, объект сервера одного из них должен иметь объект Connection, представляющий входящую репликацию из другого. Все подключения репликации для контроллера домена хранятся в объекте параметров NTDS в виде объектов соединения. Объект Connection определяет исходный сервер репликации, содержит расписание репликации и указывает транспорт репликации.

Средство проверки согласованности знаний (KCC) автоматически создает объекты подключения, но их также можно создать вручную. Объекты подключения, созданные КСС, отображаются в оснастке "сайты и службы" Active Directory "как и" при нормальных условиях работы. Объекты соединения, созданные администратором, создаются вручную.Объект подключения, созданный вручную, определяется по имени, назначенному администратором при его создании. При изменении объекта соединения он преобразуется в административно измененный объект подключения, а объект отображается в виде идентификатора GUID. KCC не вносит изменения в ручные или измененные объекты подключения.

KCC — это встроенный процесс, который выполняется на всех контроллерах домена и создает топологию репликации для Active Directory леса. KCC создает отдельные топологии репликации в зависимости от того, выполняется ли репликация на сайте (внутрисайтовая) или между сайтами (межсайтовой). KCC также динамически корректирует топологию, чтобы она соответствовала добавлению новых контроллеров домена, удалению существующих контроллеров домена, перемещению контроллеров домена на сайты, изменяющимся затратам и расписаниям, а также к контроллерам домена, которые временно недоступны или находятся в состоянии ошибки.

В пределах сайта подключения между контроллерами домена с возможностью записи всегда упорядочиваются по двунаправленному кругу с дополнительными подключениями для уменьшения задержки на больших сайтах. С другой стороны, межсайтовая топология является слоем распределения деревьев. Это означает, что между двумя сайтами каждого раздела каталога существует одно межсайтическое соединение, которое обычно не содержит ярлыки. Дополнительные сведения о охвате деревьев и Active Directory топологии репликации см. в статье Технический справочник по топологии репликации Active Directory ( <https://go.microsoft.com/fwlink/?LinkID=93578> ).

На каждом контроллере домена KCC создает маршруты репликации, создавая односторонние объекты входящих подключений, которые определяют подключения других контроллеров домена. Для контроллеров домена на одном сайте KCC автоматически создает объекты подключения без вмешательства администратора. При наличии нескольких сайтов вы настраиваете связи сайтов между сайтами, а единое средство проверки согласованности знаний на каждом сайте автоматически создает подключения между сайтами.

**Лекция №12**

**Планирование и реализация хранилищ данных**

Планирование и внедрение iSCSI SAN. Планирование и внедрение Storage Spaces. Оптимизация файловых служб для филиалов. **Планирование и реализация защиты сетей** Обзор проектирования безопасности сетей.

Рассматриваемые вопросы

1.Внедрение iSCSI SAN

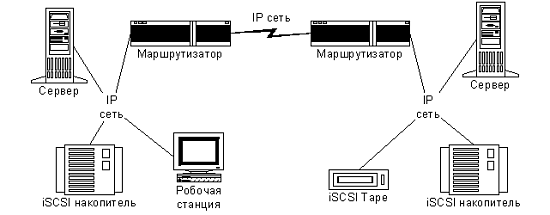
2.Внедрение Storage Spaces

3.Обзор проектирования безопасности сетей

iSCSI (Internet Small Computer System Interface) — это протокол, который базируется на TCP/IP и разработан для установления взаимодействия и управления системами хранения данных, серверами и клиентами

iSCSI описывает:

* Транспортный протокол для SCSI, который работает поверх TCP
* Новый механизм инкапсуляции SCSI команд в IP сети
* Протокол для новой генерации систем хранения данных, которые будут использовать «родной» TCP/IP



IP сеть с использованием iSCSI устройств

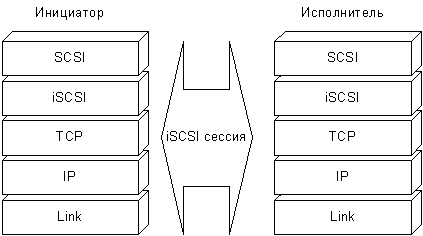
В примере, изображенном на рисунке 1, каждый сервер, рабочая станция и накопитель поддерживают Ethernet интерфейс и стек протокола iSCSI. Для организации сетевых соединений используются IP маршрутизаторы и Ethernet коммутаторы.

С внедрением SAN мы получили возможность использовать SCSI протокол в сетевых инфраструктурах, обеспечивая высокоскоростную передачу данных на уровне блоков между множественными элементами сети хранения данных.

Internet Small Computer System Interface тоже обеспечивает блочный доступ к данным, но не самостоятельно, а поверх сетей TCP/IP.

Архитектура обычного SCSI базируется на «клиент»/«серверной» модели. «Клиент», например сервер, или рабочая станция, инициирует запросы на считывание или запись данных с исполнителя — «сервера», например системы хранения данных. Команды, которые выдает «клиент» и обрабатывает «сервер» помещаются в Command Descriptor Block (CDB). «Сервер» выполняет команду, а окончание ее выполнения обозначается специальным сигналом. Инкапсуляция и надежная доставка CDB транзакций между инициаторами и исполнителями через TCP/IP сеть и есть главная задача iSCSI, причем ее приходится осуществлять в нетрадиционной для SCSI, потенциально ненадежной среде IP сетей.

Перед вами модель уровней протокола iSCSI, которая дает возможность понять порядок инкапсуляции SCSI команд для передачи их через физический носитель.



Модель нижних уровней протокола iSCSI

iSCSI протокол осуществляет контроль передачи блоков данных и обеспечивает подтверждение достоверности завершения операции ввода/вывода. Что, в свою очередь, обеспечивается через одно или несколько TCP соединений.

іSCSI имеет четыре составляющие:

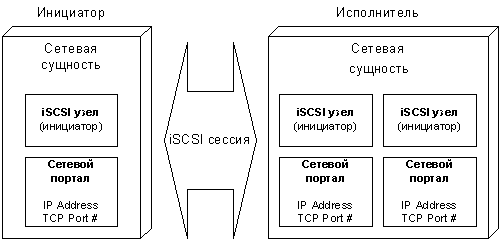
Управление именами и адресами (iSCSI Address and Naming Conventions).

Управление сеансом (iSCSI Session Management).

Обработка ошибок (iSCSI Error Handling).

Безопасность (iSCSI Security).

Так как iSCSI устройства являются участниками IP сети, они имеют индивидуальные Сетевые Сущности (Network Entity). Сетевая Сущность может содержать одних или несколько iSCSI Узлов.

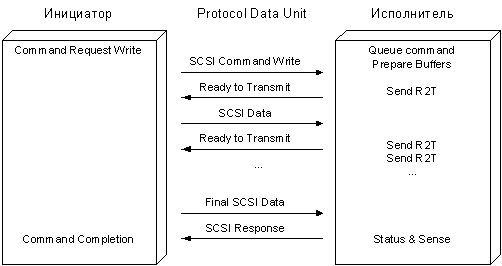


Модель сетевых сущностей

SCSI узел является идентификатором SCSI устройств (в Сетевой Сущности), доступных через сеть. Каждый iSCSI узел имеет уникальное iSCSI имя (длиной до 255 байт), которое формируется по правилам, принятым для обозначения узлов в Internet. Например: «fqn.com.ustar.storage.itdepartment.161». Такое название имеет удобную для восприятия человеком форму и может обрабатываться Сервером Доменных Имен (DNS). Таким образом, iSCSI имя обеспечивает корректную идентификацию iSCSI устройства вне зависимости от его физического местонахождения. В то же время, в процессе контроля и передачи данных между устройствами удобнее пользоваться комбинацией IP адреса и TCP порта, которые обеспечиваются Сетевым порталом (Network Portal). iSCSI протокол дополнительно к iSCSI именам обеспечивает поддержку псевдонимов, которые, как правило, отображаются в системах администрирования для удобства идентификации и управления администраторами сисiSCSI сессия состоит из фаз аутентификации (Login Phase) и фазы обмена (Full Feature Phase), которая звершается специальной командой.

Фаза аутентификации iSCSI аналогична процессу Fibre Channel Port Login (PLOGI). Она используется для того, чтобы согласовать разнообразные параметры между двумя Сетевыми Сущностями и подтвердить право доступа инициатора. Если фаза аутентификации iSCSI завершается успешно, исполнитель подтверждает login инициатору, иначе логин не подтверждается, а TCP соединение закрывается.

Как только login подтвердится, iSCSI сессия переходит к фазе обмена. Если было установлено более одного соединения TCP, iSCSI требует, чтобы каждая пара команда/ответ проходила через одно TCP соединение. Такая процедура гарантирует, что каждая отдельная команда считывания или записи будет осуществляться без необходимости дополнительно отслеживать каждый запрос по поводу его прохождения по разным потокам. Однако разные транзакции могут одновременно передаваться через разные TCP соединения в рамках одной сессии.



Пример iSCSI Write

В завершение транзакции инициатор передает/принимает последние данные, а исполнитель отправляет ответ, который подтверждает успешную передачу данных

В случае необходимости закрыть сессию, используется команда iSCSI logout, которая передает информацию о причинах завершения сессии. Она также может передать информацию о том, какое соединение следует закрыть в случае возникновения ошибки соединения, чтобы закрыть проблемные TCP связи.

Storage Spaces или Дисковые пространства — новая технология хранения данных, призванная предотвратить потерю данных и обеспечить удобство хранения больших объемов информации. Технология серверная и принцип ее работы подобен принципу работы RAID-массивов, однако есть существенные отличия, позволяющие использовать ее в клиентских операционных системах.

Суть работы Storage Spaces состоит в следующем: жесткие диски, подключенные к компьютеру, можно объединить в один или несколько пулов хранения. Каждым пулом можно управлять как единым объектом, хотя он и состоит из нескольких дисков. И в отличие от технологии RAID (где все диски должны быть строго идентичны) Storage Spaces позволяет объединять в пулы диски разных объемов и типов, причем как внутренние (SATA), так и внешние (напр. USB). Диски можно смешивать в разных сочетаниях, а для расширения пула хранения достаточно подключить новый диск и добавить его к пулу.

На основе пула создаются виртуальные области — дисковые пространства,  с помощью которых и происходит доступ к пулу из файловой системы. В одном пуле можно создать несколько дисковых пространств. Если сравнивать Storage Spaces с привычными вещами, то пул хранения — это физический диск, на котором можно создать одну или несколько логических областей, или дисковых пространств. Дисковые пространства интегрируются с Windows Explorer и отображаются в нем как обычные диски, так что доступ к ним можно получить как и к любому диску в системе, с обычной буквой диска.

Для сохранности данных Storage Spaces использует зеркалирование, гарантируя создание как минимум двух копий данных, каждая на отдельном диске, чтобы предотвратить потерю данных в случае поломки жесткого диска. При желании эту функцию можно настроить и так, чтобы хранить данные на трех разных физических дисках. Storage Spaces также поддерживает контроль четности (аналог RAID-5), позволяя создать две разных копии данных; при этом требуется наличие трех физических дисков — два для данных и третий для хранения контрольных сумм

Эффективность компьютерной сети во многом зависит от степени защищенности обрабатываемой и передаваемой информации. Степень защищенности информации от различного вида угроз при ее получении, обработке, хранении, передаче и использовании называют безопасностью информации.

Актуальность проблеме сетевой безопасности придает широкое использование компьютерных технологий во всех сферах жизни современного общества, а также переход от использования выделенных каналов к публичным сетям (Internet, Frame Relay), который наблюдается при построении корпоративных сетей.

Безопасная сеть (или безопасная связь) обладает свойствами:

■ конфиденциальности (Confidentiality), т.е. защищает данные от несанкционированного доступа, предоставляя доступ к секретным данным только авторизованным пользователям, которым этот доступ разрешен;

■ доступности (Availability), что означает обеспечение постоянного доступа к данным авторизованным пользователям. Безопасная связь характеризуется свойством аутентичности, т.е. способностью отправителя и получателя подтвердить свою личность: отправитель и получатель должны быть уверены в том, что каждый из них является тем, за кого он себя выдает;

■ целостности (Integrity), гарантирующей сохранность данных, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные.

Политика безопасности, включающая в себя совокупность норм и правил, регламентирующих процесс обработки информации, формируется на этапе развертывания сети с учетом таких основополагающих принципов, как:

■ комплексный подход к обеспечению безопасности, начиная с организационно-административных запретов и заканчивая встроенными средствами сетевой защиты;

■ предоставление каждому сотруднику предприятия (пользователю компьютеров, информационной системы, сети) того минимального уровня привилегий на доступ к данным, который необходим ему для выполнения своих должностных обязанностей;

■ принцип баланса возможного ущерба от реализации угрозы и за¬трат на ее предотвращение. Например, в некоторых случаях можно отказаться от дорогостоящих аппаратных средств защиты, ужесточив административные меры.

Основная задача политики безопасности состоит в защите от несанкционированного доступа к ресурсам информационной системы. Политика безопасности является эффективным средством, заставляющим всех пользователей корпоративной сети следовать раз и навсегда установленным правилам безопасности. Ее реализация начинается с выявления уязвимых компонентов и угроз и принятия соответствующих контрмер.

Уязвимым является такой компонент, некорректное использование или сбой которого может поставить под угрозу безопасность всей сети. К уязвимым компонентам относят пользователей сети, которые могут нанести вред сознательно, случайно или в силу отсутствия опыта.

Если информация нерегулярно резервируется, перед всей корпоративной сетью возникает вполне реальная угроза потери данных в результате умышленного или случайного повреждения основного накопителя.

Угроза — это потенциальная попытка использования недостатков уязвимого компонента для нанесения вреда. При¬мерами угроз могут служить взломщики, вирусы, пожары, природные катаклизмы.

После оценки возможных угроз (рисков) переходят к выработке контрмер. Под контрмерой понимают действие, позволяющее минимизировать риск от определенного уязвимого компонента или некоторой угрозы. Одной из самых эффективных контрмер минимизации риска потери данных является создание надежной системы резервного копирования.

Результаты оценки рисков и выработанные контрмеры используются для создания плана безопасности, который должен в мельчайших подробностях описывать системные стратегии организации, имеющие непосредственное и отдаленное отношение к вопросам безопасности.

**Планирование безопасности сети и данных.**

Высокая степень безопасности может быть достигнута путем использования плана, предусматривающего применение различных мер и средств обеспечения безопасности.

Оценка требований к безопасности сетевых данных является первым этапом разработки плана по принятию мер их защиты. При этом должны быть учтены характер деятельности организации и хранящихся в сети данных, стратегия и стиль управления организацией, которые должен знать сетевой администратор и реализовать его в подведомственной ему сети.

Высокий уровень безопасности данных должен поддерживаться в организациях, располагающих данными, которые являются строго конфиденциальными по своей природе. Примером могут служить коммерческие организации, предоставляющие услуги или выпускающие продукцию в областях с высоким уровнем конкуренции. Некоторые виды данных должны быть защищены независимо от характера деятельности организации. К ним относятся бухгалтерская документация, налоговая информация, промышленные секреты (планы деятельности организаций и коммерческие планы, рецепты, технологии изготовления, тексты программ и т.д.).

Для принятия мер по защите данных в сети нужно выявить главные источники угроз их безопасности.

Существуют следующие виды угроз:

■ непреднамеренные, к которым относятся ошибочные действия лояльных сотрудников, стихийные бедствия, ненадежность работы программно-аппаратных средств и др.;

■ преднамеренные, которые явно направлены на причинение ущерба информационной безопасности;

■ внешние, которые проявляются в таких формах, как несанкционированное использование паролей и ключей; атаки DoS (Denial of Service — отказ в обслуживании), направленные на разрыв сетевого соединения или приведение его в неработоспособное состояние; подмена адреса; компьютерные вирусы и черви;

■ внутренние, к которым можно отнести промышленный шпионаж, интриги и недовольство служащих, случайные нарушения и т.п.

В плане безопасности должны быть самым детальным образом перечислить процедуры, выполнение которых предписывается политикой безопасности. Каждый сотрудник, отвечающий за выполнение конкретной процедуры, должен быть предупрежден о возможных последствиях в случае отступления от предписанного способа выполнения процедуры. Рекомендуется взять с сотрудника письменное подтверждение того, что он понимает смысл стратегии безопасности, согласен с ней и обязуется ей следовать, а так¬же регулярно обновлять план, т.е. пересматривать аспекты безопасности, пытаясь определить новые потенциально уязвимые компоненты, угрозы и контрмеры для борьбы с ними, и отражать изменения в плане.

Для безопасности сети используется широкий набор различных средств и технологий. Рассмотрим некоторые из них.

Базовые технологии безопасности.

В разных программных и аппаратных продуктах, предназначенных для защиты данных, часто используются одинаковые подходы, приемы и технические решения, которые в совокупности образуют технологию безопасности.

Криптозащита. Разработкой методов преобразования информации в целях ее защиты занимается криптография.

 Преобразование общедоступных (понятных для всех) данных к виду, затрудняющему их распознавание, называется шифрованием (Encryption), а обратное преобразование — дешифрованием (Decryption). Шифрование является доступным средством для администраторов и пользователей и одним из эффективных средств обеспечения конфиденциальности информации. Следует выделить два основных способа шифрования данных: перестановку (Transposition), когда в исходных данных изменяют последовательность символов, и замену (Substitution), при которой с помощью некоторого шаблона производят замену всех символов используемого алфавита, например буквы заменяют цифрами.

Операции шифрования и дешифрования данных (информации) осуществляются с помощью ключей, которые создаются с привлечением математических формул.

Метод, при котором для обеих операций используется один ключ, называется симметричной криптографией (Symmetric Cryptography). При асимметричной криптографии (Asymmetric Cryptography) каждый пользователь сети должен располагать двумя ключами: общим (Public key) и частным (Private key). Оба ключа связаны друг с другом с помощью некоторой математической функции. Общий ключ известен каждому пользователю. Зашифрованное с помощью общего ключа сообщение может быть прочитано только с помощью частного ключа. Поскольку предполагается, что пользователь, которому адресуется сообщение, не разглашает свой ключ, он является единственным человеком, который может прочитать сообщение.

Популярны два алгоритма шифрования: симметричный DES (Data Encryption Standard — стандарт шифрования данных, который является официальным стандартом правительства США) и не¬симметричный RSA, разработанный учеными Rivest, Shamir, Adle- man и названный по начальным буквам их фамилий.

Для шифрования, аутентификации и проверки целостности передаваемых по сети пакетов разработан протокол IPSec (IP Securi¬ty), включающий в себя протокол АН (Authentication Header), позволяющий проверять идентичность отправителя, и протокол ESP (Encapsulating Security Payloads), обеспечивающий конфиденциальность самих данных. Протокол IPSec поддерживают маршрутизаторы компании Cisco Systems и ОС Windows 2000/ХР.

Для передачи через Internet зашифрованных, аутентифицированных сообщений используется протокол SSL (Secure Sockets Layer — уровень защищенных сокетов, или гнезд). В этом протоколе криптографическая система с открытым ключом комбинируется с блочным шифрованием данных.

Аутентификация (Authentication).

Это процедура установления подлинности пользователя при запросе доступа к ресурсам системы (компьютеру или сети). Аутентификация предотвращает доступ нежелательных лиц и разрешает доступ всем легальным пользователям. В процедуре аутентификации участвуют две стороны, одна из которых доказывает свое право на доступ (аутентичность), предъявляя некоторые аргументы, другая — проверяет эти аргументы и принимает решение. Для доказательства аутентичности может использоваться некоторое известное для обеих сторон слово (пароль) или уникальный физический предмет (ключ), а также собственные биохарактеристики (отпечатки пальцев или рисунок радужной оболочки глаза).

Наиболее часто при аутентификации используют вводимые с клавиатуры пароли.

Пароль представляет собой зашифрованную последовательность символов, которая держится в секрете и предъявляется при обращении к информационной системе.

Объектами аутентификации могут быть не только пользователи, но и различные устройства, приложения, текстовая и другая информация.

Идентификация субъектов и объектов доступа.

Идентификация предусматривает закрепление за каждым субъектом доступа уникального имени в виде номера, шифра или кода, например, персональный идентификационный номер (Personal Identification Number — PIN), социальный безопасный номер (So¬cial Security Number — SSN) и т. п. Идентификаторы пользователей должны быть зарегистрированы в информационной системе администратором службы безопасности.

При регистрации в базу данных системы защиты для каждого пользователя заносятся такие данные, как фамилия, имя, отчество и уникальный идентификатор пользователя, имя процедуры для установления подлинности и пароль пользователя, полномочия пользователя по доступу к системным ресурсам и др. Идентификацию следует отличать от аутентификации. Идентификация заключается в сообщении пользователем системе своего идентификатора, в то время как аутентификация является процедурой доказательства пользователем того, что именно ему принадлежит введенный им идентификатор.

**Авторизация (Authorization).**

Это процедура предоставления каждому из пользователей тех прав доступа к каталогам, фай¬лам и принтерам, которыми его наделил администратор. Кроме того, система авторизации может контролировать возможность выполнения пользователями различных системных функций, таких как установка системного времени, создание резервных копий данных, локальный доступ к серверу, выключение сервера и т. п.

Система авторизации наделяет пользователя сети правами выполнять определенные действия над определенными ресурсами. Для этого могут быть использованы два подхода к определению прав доступа:

■ избирательный, при котором отдельным пользователям (или группам), явно указанным своими идентификаторами, разрешаются или запрещаются определенные операции над определенным ресурсом;

■ мандатный, при котором вся информация в зависимости от степени секретности делится на уровни, а все пользователи сети — на группы, образующие иерархию в соответствии с уровнем допуска к этой информации.

Процедуры авторизации реализуются программными средства¬ми по централизованной схеме, в соответствии с которой пользователь один раз логически входит в сеть и получает на все время работы некоторый набор разрешений по доступу к ресурсам сети, и децентрализованной схеме, когда доступ к каждому приложению должен контролироваться средствами безопасности самого приложения или средствами той операционной среды, в которой оно работает.

Поскольку системы аутентификации и авторизации совместно выполняют одну задачу, необходимо предъявлять к ним одинаковый уровень требований. Ненадежность одной системы не может быть компенсирована высоким качеством другой.

Аудит (Auditing). Это фиксация в системном журнале событий, связанных с доступом к защищаемым системным ресурсам. Аудит используется для обнаружения неудачных попыток взлома системы. При попытке выполнить противоправные действия си¬стема аудита идентифицирует нарушителя и пишет сообщение в журнал регистрации. Анализ накопившейся и хранящейся в журнале информации может оказаться действенной мерой защиты от несанкционированного доступа.

Процедура рукопожатий. Для установления подлинности пользователей широко используется процедура рукопожатий (Handshaking — согласованный обмен, квитирование), построенная по принципу вопрос-ответ. Она предполагает, что правильные ответы на вопросы дают только те пользователи, для которых эти вопросы предназначены. Для подтверждения подлинности пользователя система последовательно задает ему ряд случайно вы¬бранных вопросов, на которые он должен дать ответ. Опознание считается положительным, если пользователь правильно ответил на все вопросы.

Технологии защищенного канала широко используются в виртуальных частных сетях, которые требуют принятия дополнительных мер по защите передаваемой информации. Требование конфиденциальности особенно важно, потому что пакеты, передаваемые по публичной сети, уязвимы для перехвата при их прохождении через каждый из узлов (серверов) на пути от источника к получателю. Технология защищенного канала включает в себя:

■ взаимную аутентификацию абонентов при установлении со¬единения;

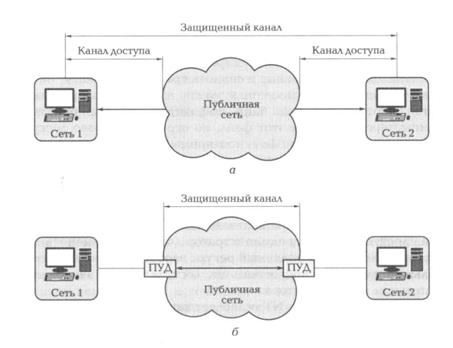
■ защиту передаваемых по каналу сообщений от несанкционированного доступа;

■ подтверждение целостности поступающих по каналу сообщений.

В зависимости от места расположения программного обеспечения защищенного канала различают две схемы его образования.

1. Схема с конечными узлами (рис.1, а). В этой схеме защищенный канал образуется программными средствами, установленными на двух удаленных компьютерах. Компьютеры принадлежат двум разным АС одной организации и связаны между собой через публичную сеть.

2. Схема с оборудованием поставщика услуг публичной сети, расположенным на границе между частной и публичной сетями (рис. 1, б). В этой схеме защищенный канал прокладывается только внутри публичной сети с коммутацией пакетов. Средствами защиты являются пограничные устройства доступа (ПУД).



Средства безопасности, предоставляемые операционными системами.

Современные ОС способны обеспечить доступ к одному компьютеру и сетевым ресурсам многим пользователям. Для этого используются отдельные учетные записи, которым присвоены разные пароли. После правильного ввода регистрационной информации пользователь может получить доступ к ОС и сети; читать, изменять ресурсы и выполнять любые другие действия, которые соответствуют правам его учетной записи, создавать желаемую конфигурацию пользовательского интерфейса (рабочую среду) и т.д.

Выбор (или назначение) паролей подчинен стратегии обеспечения сетевой безопасности. Пароли должны удовлетворять определенным требованиям. Многие сетевые ОС позволяют администратору задавать длину и время жизни пароля; проверять пароль на наличие заданного пароля в словаре и, если он есть, предотвращать использование пароля; следить, чтобы пароль пользователя не повторялся. Кроме того, администратору предоставляются широкие возможности контроля за доступом к ресурсам. Например, одной и той же учетной записи он может одновременно разрешить просматривать содержимое файла  filel. doc, но запретить вносить в него изменения; предоставить право читать, изменять, удалять файл  file2. doc и даже устанавливать права доступа к нему других пользователей, а к файлу file3.doc отменить все права доступа.

В файловых системах с высоким уровнем безопасности права доступа можно устанавливать как на разделение ресурсов по сети, так и на использование этих ресурсов на одном и том же локальном компьютере. Локальные и сетевые права доступа могут не со¬впадать. Например, пользователю можно предоставить право пол¬ного контроля над файлом file4 . doc, когда он регистрируется на компьютере, хранящем этот файл, но ограничить право доступа того же пользователя к file4. doc при попытке получить к нему доступ с другого компьютера сети.

Администратор должен знать и учитывать, какими правами до¬ступа наделена данная ОС по умолчанию (сразу после загрузки). Так, по умолчанию разделяемый ресурс в серверах Windows NT/ ХР доступен для любого пользователя сети. Для ограничения прав доступа к ресурсу администратор должен их изменить, а в серверах NetWare разделяемый ресурс недоступен ни для одного пользователя. Здесь предоставление доступа требует явного вмешательства администратора.

Сетевая ОС Windows NT позволяет каждому пользователю назначать четыре вида (или привилегии) доступа к совместно используемому ресурсу: отсутствие доступа (No Access); полный доступ (Full Control); чтение (Read), предоставляющее право просматривать перечень файлов, открывать файлы, изучать их содержимое и копировать файлы на свои носители; редактирование (Change), предоставляющее дополнительную (к Read) возможность изменять содержимое существующих файлов и каталогов. Windows NT позволяет также управлять доступом к локальным файлам. Для этого файлы или каталоги должны быть расположены в логическом разделе жесткого диска, размеченном файловой системой NTFS. Помимо указанных выше привилегий система NTFS позволяет просматривать файлы каталога (привилегия List), добавлять файлы в каталог без изменения их содержимого (Add), просматривать существующие и добавлять новые файлы (Add & Read).

Администратор должен понимать способы назначения привилегий и взаимоотношения между назначенными привилегиями доступа к локальным и совместно используемым ресурсам и при¬менять наиболее эффективный способ назначения привилегий пользователям. При этом пользователи должны быть лишены возможности обращения к не нужным для работы ресурсам.

Система безопасности Windows NT предоставляет возможность регистрации всех происходящих событий. Однако ведение отчетности требует постоянно запущенных приложений, что снижает производительность сети, поэтому к протоколированию событий, которое также отнимает время, администратор и пользователи сети должны походить избирательно и активизировать средства регистрации событий только на тех рабочих станциях, которые этого требуют. Журнал регистрации событий может оказаться полезным источником информации при администрировании сети.

**Аппаратные средства защиты.**

Основой надежной защиты данных от многих неисправностей аппаратных средств является избыточность. При выходе из строя некоторого сетевого устройства начинает функционировать его резервный дублер. Потерю данных при выходе из строя винчестера можно восполнить файлами, хранящимися в системе резервного копирования.

Некоторые сер¬веры поддерживают возможность установки избыточных устройств, автоматически передающих полномочия отказавшего компонента исправному. Такая избыточность применима к охлаждающим вентиляторам, источникам питания, сетевым адаптерам, жестким дискам и центральным процессорам.

При резервировании электропитания используют избыточные источники электро¬энергии — устройство бесперебойного питания наряду с электро¬сетью. Резервное копирование данных предполагает создание избыточных копий ценных файлов на дополнительных (резервных) носителях. В системах отказоустойчивых дисков данные записываются на избыточных дисках. Высшей степенью избыточности является кластеризация, когда несколько серверов объединяются в группу. В сети кластер серверов виден пользователям как один сервер. Если один из серверов кластера выходит из строя, его обязанности выполняет другой сервер. Пользователи не замечают этого перехода. Средства поддержки кластеризации встроены в такие ОС, как, например Windows NT.

Резервное копирование данных. Оно осуществляется с помощью специальных программ и является действенной мерой защиты от возможной их потери при регулярном выполнении этой процедуры. Наличие резервной копии позволяет быстро восстановить утерянные данные.

Используются следующие способы резервного копирования:

• полное, при котором копируются все данные заданных дисков независимо от того, когда их копирование выполнялось последний раз и вносились ли с тех пор изменения;

• дифференциальное, когда копируются все файлы, которые из¬менялись со времени последнего полного копирования. Дифференциальное копирование выполняется в промежутках между полным копированием, благодаря этому экономится время. Для обновления данных нужно восстанавливать две последних копии — полную и дифференциальную;

• инкрементное. При этом способе копируются все файлы, которые изменялись со времени любого последнего копирования (а не последнего полного копирования). Это наиболее быстрый способ, однако он сложнее и занимает много времени на восстановление данных, так как необходимо восстанавливать последнюю полную копию и все инкрементные копии, созданные со времени последнего полного копирования.

**Отказоустойчивая система дисков.**

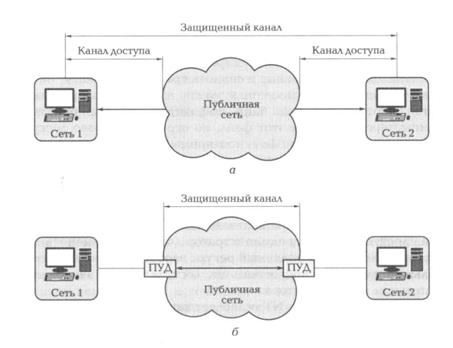
Под отказоустойчивостью понимают способность системы к восстановлению после аварии. Объединение (конфигурация) нескольких физических жестких дисков в отказоустойчивый набор называется системой RAID (Redundant Array of Independent Disks — избыточный набор независимых дисков). Он может быть реализован в не¬скольких различных формах. В зависимости от уровня (0 — 5 и 7) предоставляются различные способы объединения дисков: RAID О, RAID 1, RAID 2, RAID 3, RAID 4, RAID 5.

Брандмауэры позволяют организовать защиту по всему периметру АС, создавая барьер между внутренней АС и соединениями с внешним миром (Internet). Такая защищенная область может быть установлена также в подсети.

Брандмауэр может быть реализован как аппаратным, так и программным способом.

Фактически он является средством фильтрации входящих и исходящих пакетов.

 На основе правил безопасности, установленных сетевым администратором, брандмауэр определяет, следует ли пропустить поступивший пакет. Обычно брандмауэры располагают на шлюзах сети, являющихся точками ее соединения с другой сетью.



**Лекция №13**

Проектирование и внедрение использования Windows Firewall. Проектирование и внедрение инфраструктуры NAP

Рассматриваемые вопросы

1.Windows Firewall

2.Инфраструктура NAP

Брандмауэр (Firewall) служит для повышения защищенности Вашего компьютера путем фильтрации входящего или исходящего трафика. С помощью него можно ограничить доступ в интернет всем кроме конкретных программ или разрешить соединяться с компьютером на котором он установлен только из внешней сети или только из внутренней сети, только по определенному порту, с определенных ip-адресов и т.д.

В windows firewall представляет собой набор правил. Правило это описание разрешения или запрета соединения. Могут быть входящими и исходящими, регулирующими соответственно доступ к этому компьютеру или с этого компьютера в сеть.

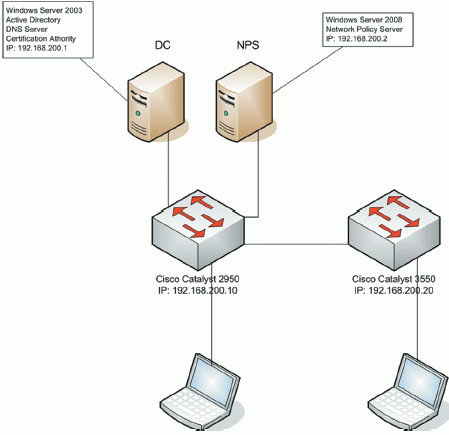
Технология NAP предлагает различные варианты реализации: выдача IP-адресов из различных диапазонов для «хороших» и «плохих» компьютеров; установление соединения IPSec с «хорошими» компьютерами, в то время как «плохим» компьютерам в соединении будет отказано. И самый интересный и наиболее правильный для использования в локальной сети вариант — авторизация сетевых устройств по протоколу IEEE 802.1x на коммутаторах локальной сети. Далее я расскажу, как настроить роль Network Policy Server в Windows Server 2012, а также сетевые коммутаторы для реализации NAP в сети.

Network Access Protection (защита доступа к сети) – это новый инструмент для контроля доступа к сети, входящий в состав операционной системы Windows Server 2012. Network Access Protection, или сокращенно NAP, позволяет вам контролировать, какие компьютеры могут взаимодействовать в вашей сети. Возможность взаимодействия с сетью определяется тем фактором, удовлетворяет ли клиентский компьютер NAP требованиям безопасности, которые заданы вашими политиками NAP.

NAP имеет несколько 'движущих частей', из-за которых его сложно настраивать. Дополнительно проблемой также является тип усиления, который вы хотите подключить. Например, есть несколько клиентов NAP Enforcement Clients, которые контролируют доступ к сети на основании информации об IP адресе, или, основываясь на том, имеет ли клиент сертификат, который позволяет ему подключиться к сети.

Технология NAP предлагает различные варианты реализации: выдача IP-адресов из различных диапазонов для «хороших» и «плохих» компьютеров; установление соединения IPSec с «хорошими» компьютерами, в то время как «плохим» компьютерам в соединении будет отказано. И самый интересный и наиболее правильный для использования в локальной сети вариант — авторизация сетевых устройств по протоколу IEEE 802.1x на коммутаторах локальной сети. Далее я расскажу, как настроить роль Network Policy Server в  Windows Server 2012, а также сетевые коммутаторы для реализации NAP в сети.

Для изучения и демонстрации технологии NAP был собран стенд «Поликом Про», состав оборудования которого был максимально приближен к реальным условиям. В нашей лабораторной сети установлен L3-коммутатор Cisco Catalyst 3550 и L2-коммутаторы Cisco Catalyst 2950. Данные модели наиболее распространены в сетях российских предприятий. Схема собранного стенда показана на рисунке.



Как мы видим, в качестве контроллера домена используется компьютер под управлением Windows Server 2012, центр сертификации также развернут на компьютере под управлением Windows Server 2012. На компьютере под Windows Server 2008 развернута только одна роль — Network Policy Server, которая необходима для реализации технологии NAP. Такая конфигурация стенда была выбрана специально, чтобы показать, что для использования технологии NAP администраторам не придется перестраивать всю существующую инфраструктуру, а при желании достаточно лишь добавить один сервер под управлением Windows Server 2012, и можно использовать новые технологии, реализованные в новой серверной операционной системе. В качестве клиентов использовались компьютеры под управлением Windows Vista и Windows XP SP2 плюс специальный программный модуль или Windows XP SP3.

**Контрольные вопросы**

1.Назовите базовые технологии безопасности

2.Расскажите об использовании Wirewall

**Лекция №14**

**Проектирование и реализация защиты служб доступа к сети** Планирование и внедрение DirectAccess. Планирование и внедрение VPN. Планирование и внедрение Web Application Proxy. Планирование сложной инфраструктуры удаленного доступа. Принципы программного кодирования. Современные методы кодирования

Рассматриваемые вопросы

1.Внедрение Direct Access

2.Внедрение VPN

3.Внедрение Web Application Proxy

4.Инфраструктура удаленного доступа

5.Программное кодирование

6.Современные методы кодирования

Компонент DirectAccess впервые была представлена Micrisoft в Windows Server 2008 R2 и предназначался для организации прозрачного доступа удаленных компьютеров ко внутренним ресурсам сети компании. При подключении через DA пользователь может полноценно пользоваться корпоративными и доменными сервисами, а сотрудники ИТ-поддержки управлять таким компьютеров и поддерживать его актуальном с точки зрения безопасности состоянии. По своей сути DirectAccess во многом напоминает традиционное [VPN](https://winitpro.ru/index.php/2014/01/16/nastrojka-vpn-servera-na-baze-windows-server-2012-r2/) подключение к корпоративной сети. **Рассмотрим** **основные отличия DirectAccess от VPN**:

Для установки соединения с помощью  DirectAccess пользователю не нужно запускать [VPN клиент](https://winitpro.ru/index.php/2012/04/17/nastrojka-vpn-podklyucheniya-v-windows-8/) – подключение осуществляется автоматически при наличия доступа в Интернет

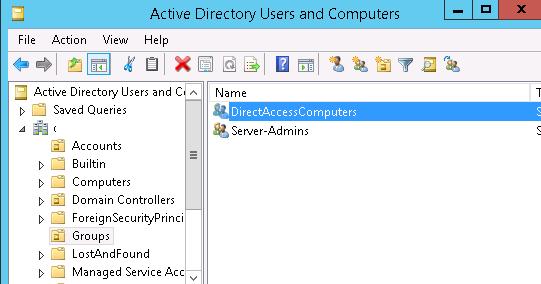
* Для организации соединения между клиентом DA и сервером нужно открыть только 443 порт
* Компьютер пользователя обязательно должен находится в домене AD, а это значит что на него действуют все доменные групповые политики (конечно есть трюки, позволяющие [запускать VPN до входа в Windows](https://winitpro.ru/index.php/2013/06/16/zapusk-vpn-soedineniya-do-vxoda-v-sistemu-windows/), но это обычно практически не практикуется)
* Канал связи между удаленным ПК и корпоративным шлюзом шифруется стойкими алгоритмами с использованием IPsec
* Возможно организовать двухфакторную аутентификацию с использованием системы одноразовых паролей

**В чем же основные отличия версии DirectAccess в Windows Server 2012 / 2012 R2 от версии Windows 2008 R2.**Основное отличие – снижение требований к смежной инфраструктуре. Так, например:

* Сервер DirectAccess теперь не обязательно должен быть пограничным, теперь он может находиться за NAT.
* В том случае, если в качестве удаленных клиентов  используется Windows 8 Enterprise, разворачивать внутреннюю инфраструктуру PKI не обязательно (за аутентификацию клиентов будет отвечать Kerberos-прокси, расположенный на сервере DA)
* Не обязательно стало наличие IPv6 во внутренней сети организации
* Поддержка OTP (One Time Password) и NAP (Network Access Protection) без необходимости развёртывания UAG

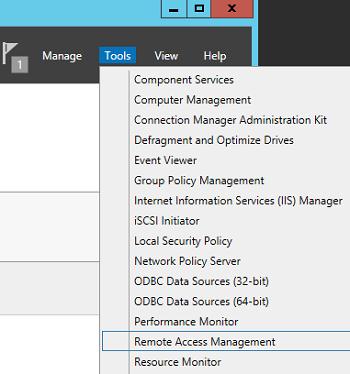
**Требования и инфраструктура, необходимы для развертывания DirectAccess на базе Windows Server 2012 R2**

* Домен Active Directory и права администратора домена
* Выделенный (рекомендуется) сервер DA под управлением Windows Server 2012 R2, [включенный в домен Windows](https://winitpro.ru/index.php/2012/12/06/vvod-windows-8-domen/). Сервер имеет 2 сетевые карты: одна находится во внутренней корпоративной сети, другая – в DMZ сети
* Выделенная DMZ подсеть
* Внешнее DNS имя (реальное или через DynDNS) или IP адрес, доступный из интернета, к которому будут подключатся клиенты DirectAccess
* Настроить перенаправление трафика с порта TCP 443 на адрес сервера DA
* Развернутая инфраструктура PKI для выпуска сертификатов. В certificate authority нужно опубликовать шаблон сертификата **Web Server** и разрешено его автоматическое получение (auto-enrollmen) (Если в качестве клиентов будут использоваться только Windows 8 — PKI не обязателен).
* В качестве клиентов могут выступать компьютеры с Windows 7 и Windows 8.x редакций Professional / Enterprise
* Группа AD, в которой будут состоять компьютеры, которым разрешено подключаться к сети через Direct Access (допустим, эта группа будет называться **DirectAccessComputers**)



**Настройка службы Direct Access в Windows Server 2012 R2**

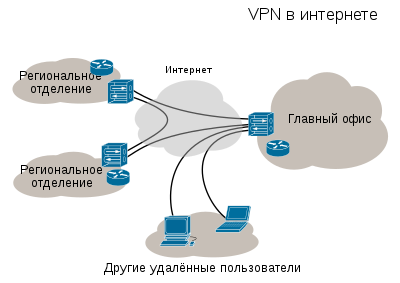
После окончания установки службы Remote Access, откройте оснастку Tools -> Remote Access Management.



Разворачиваем полноценный DirectAccess сервер с возможностью доступа клиентов и их удаленного управления Deploy full DirectAccess for client access and remote management.

VPN (англ. Virtual Private Network «виртуальная частная сеть») — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим или неизвестным уровнем доверия (например по публичным сетям) уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений передаваемых по логической сети сообщений).

В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть.

****

Обычно VPN развёртывают на уровнях не выше сетевого, так как применение криптографии на этих уровнях позволяет использовать в неизменном виде транспортные протоколы (такие как TCP, UDP).

Пользователи Microsoft Windows обозначают термином VPN одну из реализаций виртуальной сети — PPTP, причём используемую зачастую не для создания частных сетей.

Чаще всего для создания виртуальной сети используется инкапсуляция протокола PPP в какой-нибудь другой протокол — IP (такой способ использует реализация PPTP — Point-to-Point Tunneling Protocol) или Ethernet (PPPoE) (хотя и они имеют различия)

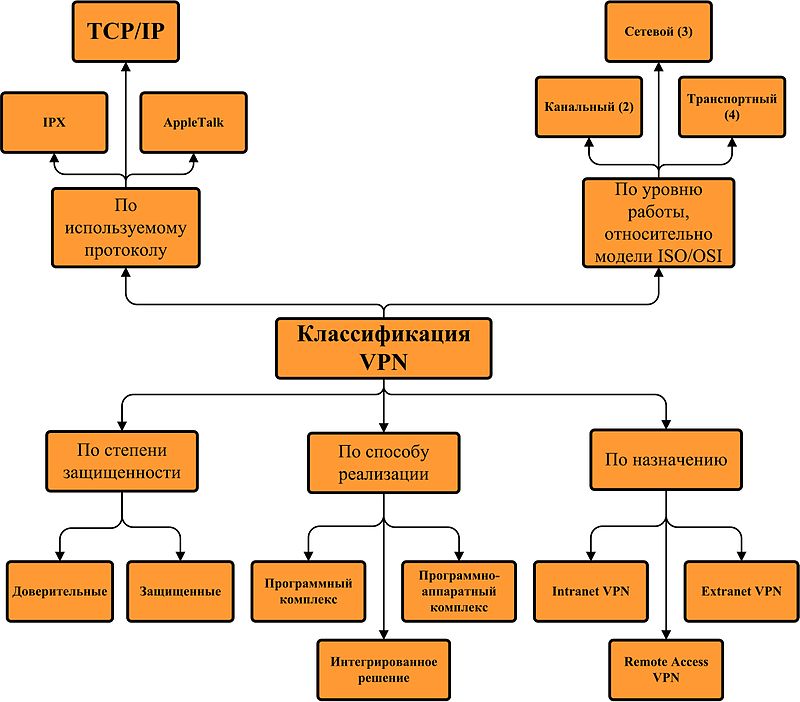
Технология VPN в последнее время используется не только для создания собственно частных сетей, но и некоторыми провайдерами «последней мили» на постсоветском пространстве для предоставления выхода в Интернет.

При должном уровне реализации и использовании специального программного обеспечения сеть VPN может обеспечить высокий уровень шифрования передаваемой информации.

VPN состоит из двух частей: «внутренняя» (подконтрольная) сеть, которых может быть несколько, и «внешняя» сеть, по которой проходит инкапсулированное соединение (обычно используется Интернет).

Возможно также подключение к виртуальной сети отдельного компьютера.

Подключение удалённого пользователя к VPN производится посредством сервера доступа, который подключён как к внутренней, так и к внешней (общедоступной) сети. При подключении удалённого пользователя (либо при установке соединения с другой защищённой сетью) сервер доступа требует прохождения процесса идентификации, а затем процесса аутентификации. После успешного прохождения обоих процессов удалённый пользователь (удаленная сеть) наделяется полномочиями для работы в сети, то есть происходит процесс авторизации.



Реализация сети VPN осуществляется при помощи специального комплекса программно-аппаратных средств. Такая реализация обеспечивает высокую производительность и, как правило, высокую степень защищённости.

Web Application Proxy предоставляет такие же возможности публикации приложений, как и Forefront Unified Access Gateway (UAG), однако данная служба также позволяет взаимодействовать с другими серверами и сервисами, обеспечивая тем самым более гибкую и рациональную конфигурацию.

Web Application Proxy по сути выполняет функцию обратного прокси сервера (HTTP reverse proxy), организуя ретрансляцию запросов клиентов из внешней сети на внутренний сервер, и является межсетевым экраном на прикладном уровне.

Сервер со службой Web Application Proxy получает внешний HTTP/HTTPS трафик и терминирует его, после чего от своего имени инициирует новое подключение ко внутреннему приложению (веб-серверу). Т.е. внешние пользователи прямого доступа к внутреннему приложению реально не получают. Любой другой трафик, получаемый Web Application Proxy, отклоняется (в том числе отклоняются HTTP/HTTPS запросы, которые могут быть использованы при DoS, SSL и 0-day атаках).

Требования к организации Web Application Proxy и ключевые особенности:

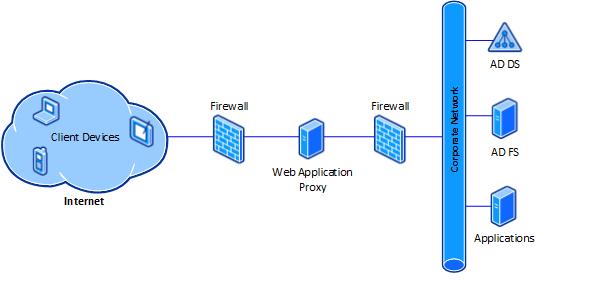
Систему можно развернуть на серверах с ОС Windows Server 2012 R2, включенных в домен Active Directory, с ролями AD FS и Web Application Proxy. Эти роли должны быть установлены на разных серверах.

Необходимо обновить схему Active Directory до Windows Server 2012 R2 (обновлять контроллеры домена до Windows Server 2012 R2 не нужно)

В качестве клиентских устройств поддерживаются устройства с ОС Windows, IOS (iPad и iPhone). Работы над клиентами для Android и Windows Phone пока еще не окончены

Аутентификация клиентов осуществляется службой Active Directory Federation Services (ADFS), которая также выполняет функции ADFS – проксирования.

Типовая схема размещения сервера с ролью Web Application Proxy представлена на рисунке. Данный сервер располагается в выделенной DMZ зоне и отделен от внешней (Интернет) и внутренней сети (Интранет) межсетевыми экранами. В этой конфигурации для работы Web Application Proxy требует наличия двух интерфейсов – внутреннего (Intranet) и внешнего (DMZ)

****

Для обеспечения дополнительной безопасности преаутентифкация внешних клиентов выполняется на сервере ADFS, в противном случае используется pass-through аутентификация на конечном сервере приложения (что менее секьюрно). Поэтому первый шаг при настройке Web Application Proxy – установка на отдельном сервере роли Active Directory Federation Services.

Служба Web Application Proxy в Windows Server 2012 R2 является частью роли “Remote Access”. Установите службу Web Application Proxy и запустите мастер ее настройки.

Удаленный доступ – это система, в которой пользователь может удаленно подключиться и управлять определенным компьютером так, как если бы он находился прямо перед ним. Самый распространенный пример – вы подключаетесь к компьютеру в офисе через домашний ноутбук, что позволяет вам управлять файлами, пользоваться ресурсами рабочего компьютера и делать все, что угодно, как если бы вы находились в непосредственной близости от него.

Тысячи компаний по всему миру пользуются системами удаленного доступа и полагаются на них как на ключевую функцию их отделов IT. Удаленный доступ применим в бесчисленных отраслях, начиная с транснациональных коммерческих корпораций и заканчивая образовательными учреждениями, обеспечивающими удаленное обучение студентов.

И как это часто бывает в IT-системах, у систем удаленного доступа есть как преимущества, так и недостатки. Давайте рассмотрим положительные и негативные стороны введения этой технологии в ваш бизнес. Преимущества:

* Безопасность – вся ваша важная информация, в том числе файлы и документы, будет храниться в самых безопасных для этого местах – дата-центрах, где практически нулевая вероятность их кражи или утери. Соединение с удаленным сервером устанавливается со сложными системами шифрования, которые нивелируют риск атаки и других возможностей утери данных, распространенных в стандартных компьютерных сетях.
* Гибкость – главная задача систем удаленного доступа – возможность работникам исполнять свои функции буквально откуда угодно в любое время. Все, что нужно – это компьютер и безопасное интернет-соединение.
* Экономия – часто использование системы удаленного доступа позволяет отказаться от трат на многочисленные копии одинакового программного обеспечения, поскольку это ПО можно использовать на единственном компьютере. Кроме того, компьютеры, используемые для получения доступа к целевой машине, не обязательно должны быть самыми мощными, и, следовательно, дорогими.

Недостатки:

* Простой – если ваш дата-центр не может обеспечить идеальную бесперебойную работу соединения, то велик риск простоя. А поскольку речь идет о перебоях системы удаленного доступа, вся ваша система будет недоступна, пока не будет восстановлена работоспособность соединения.
* Зависимость от сетевого соединения – подобно предыдущему пункту, здесь система будет работать отлично, пока удаленные компьютеры обладают стабильным и быстрым интернет-соединением. При его потере система становится недоступна для этих компьютеров.
* Снижение производительности – в зависимости от мощности целевого компьютера и количества подключенных компьютеров возможно снижение производительности и взаимные помехи.
* Знания – администратор системы удаленного доступа должен обладать хорошим знанием темы и быть на связи на случай, если появятся проблемы в течение обычного рабочего дня. Без необходимой помощи в случае отказа системы последствия могут быть удручающими.

Как же организовать систему удаленного доступа? Обычно удаленный доступ требует установки программы на целевом компьютере (хосте), к которому нужно осуществить подключение. Когда это происходит, то другой компьютер или устройство с необходимыми полномочиями (клиент) может подключиться к хосту и контролировать его.

**TeamViewer**

TeamViewer – одно из лучших решений среди систем удаленного доступа. Присутствует масса возможностей, а сама программа очень легко устанавливается. Не требуется никаких настроек роутера или фаерволла.

Помимо видео- и голосовых звонков и чата, TeamViewer поддерживает передачу файлов, технологию WOL (wake-on-LAN), и через нее можно даже запустить ПК в безопасном режиме, после чего автоматически переподключиться.

**Хост**

Компьютер, к которому осуществляется подключение через TeamViewer, может работать в любой ОС – Windows, Mac или Linux.

Первый вариант – полная инсталлируемая версия TeamViewer, он подходит в том случае, если вы не знаете наверняка, что вам нужно сделать. Второй – портативная версия TeamViewer QuickSupport, отличный выбор в случае, если удаленный сервер нужно настроить один раз, или если установка невозможна. Третий, TeamViewer Host – лучший вариант, если удаленный сервер должен иметь постоянную возможность подключения к нему.

**Клиент**

TeamViewer предоставляет множество возможностей для подключения к удаленному компьютеру для стороны клиента. Существуют инсталлируемые и портативные версии для Windows, Mac, Linux, а также мобильные приложения для iOS, BlackBerry, Android и Windows Phone. Это означает, что вы можете подключиться и управлять удаленным компьютером с помощью смартфона или планшета. Кроме того, есть возможность воспользоваться браузерным интерфейсом.

Помимо того включен ряд других функций, например, возможность открыть доступ к отдельному окну приложения (вместо целого рабочего стола), а также печать файлов с удаленного компьютера на локальном принтере.

**2. Ammyy Admin**

Ammyy Admin – полностью портативная программа удаленного доступа, которую очень легко настроить. Она работает путем подключения одного компьютера к другому через идентификатор, генерируемый программой.

Хост

Запустите Ammyy Admin на компьютере, к которому нужно получить доступ. Для работы не требуется инсталляция, а файл приложения весит менее 1 Мб.

Через меню Ammyy выберите Service и запустите службу Ammyy Admin, чтобы вы могли получать доступ к компьютеру без необходимости вручную запускать программу. Также вы можете просто запустить программу и записать номер идентификатора, к которому будет подключаться клиент.

Клиент

Чтобы подключиться к хосту с Ammyy Admin, просто запустите программу на стороне клиента и введите идентификатор другого компьютера. Нужный идентификатор отображается в Ammyy Admin на компьютере со стороны хоста. После этого вы можете пользоваться буфером обмена, голосовым чатом и функцией передачи файлов в обе стороны.

К наиболее эффективным методам обеспечения высокого качества цифровой передачи в условиях высокого уровня шума канала связи относятся весьма мощные алгоритмы формирования корректирующих кодов, в разработке которых теория помехоустойчивого кодирования имеет значительные успехи.

За годы развития в технику связи успешно внедрены пороговые декодеры, алгоритм Витерби, коды Рида-Соломона, каскадные схемы кодирования, а также разработки последнего времени – алгоритмы для турбо кодов, многопороговые декодеры и каскадные методы кодирования и декодирования.

Однако требования к алгоритмам коррекции ошибок в каналах связи с помехами, в частности в спутниковых каналах, непрерывно растут и главная проблема – декодирование с эффективностью, близкой к оптимальной по энергетике канала, но при максимально простой реализации.

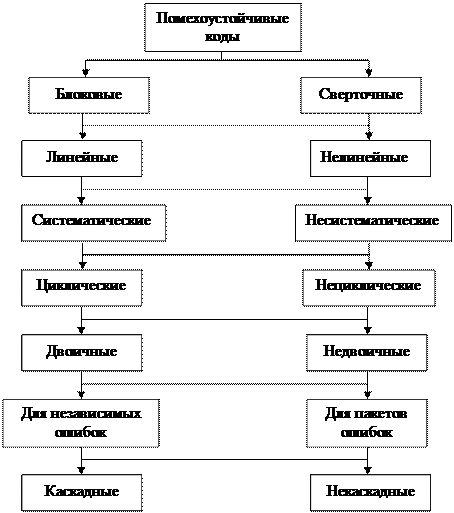
Основными характеристиками методов коррекции ошибок являются:

- средняя вероятность ошибки в информационном бите или последовательности бит;

- энергетический выигрыш кодирования (ЭВК), показывающий величину снижения энергии, необходимой для передачи одного бита данных при некоторой выбранной средней вероятности ошибки;

- сложность реализации алгоритма как программной так и аппаратной. Данная характеристика имеет большое значение, так как применяя очень сложные методы кодирования, получают высокий ЭВК, но эти методы практического применения не находят.

На сегодняшний день известно множество различных классов помехоустойчивых кодов, отличающихся друг от друга структурой, функциональным назначением, энергетической эффективностью, алгоритмами кодирования и декодирования и многими другими параметрами. На рис представлена классификация помехоустойчивых кодов.



К основным наиболее распространенным кодам можно отнести:

1) блоковые коды, в которых кодирование и декодирование производится в пределах кодовой комбинации или блока. К ним относят коды Боуза-Чоудхури-Хоквингема, коды Рида-Соломона, мажоритарно декодируемые коды

2) сверточные коды, в которых обработка символов производится непрерывно, без разделения на блоки;

3) линейные коды, образующие векторное пространство и обладающие важным свойством: два кодовых сообщения можно сложить, используя подходящее определение суммы, и получить третье кодовое слово. Данное свойство упрощает процедуру кодирования и декодирования. Важный подкласс линейных кодов составляют циклические коды или *CRC* коды (*Cyclic Redundancy Codes* – Циклические Избыточные Коды);

4) каскадные схемы кодирования, в основе построения которых лежит идея совместного использования нескольких составляющих кодов. Данный подход позволил существенно повысить эффективность применения кодирования по сравнению с базовыми некаскадными методами. Примером могут служить каскадные коды, построенные с использованием кода Хемминга и его модификации, особое место среди кодовых схем занимают каскадирование с кодами контроля по четности, а также каскадные схемы с методами параллельного кодирования, образуя турбо коды, которые формируются при параллельном каскадировании двух или более составляющих кодов.

Контрольные вопросы:

1.Что такое VPN?

2.Классификация кодов

**Лекция №15**

**Обзор управления Центром Обработки Данных предприятия Обзор ЦОД предприятия**.

Рассматриваемые вопросы:

1.Центр обработки данных

Разбираемся, как устроен центр обработки данных (ЦОД), в чем суть его работы и какую роль он играет в облачных вычислениях.

Центр обработки данных, или, как его еще называют, дата-центр, представляет собой отдельное здание, предназначенное для размещения и эксплуатации производительного вычислительного оборудования. ЦОД создает благоприятные условия для вашего «железа» и персонала, который его обслуживает.

Помещение ЦОД чаще всего размещают рядом с магистральной точкой обмена трафиком, так как доступ к вычислительному оборудованию дата-центра чаще всего осуществляется через интернет. И оснащают его современными эффективными инженерными системами — это залог стабильного функционирования.

В ЦОДе используются разные схемы резервирования инженерных систем, уровень которых подтверждается сертификатом, а качество и объем предоставляемых услуг могут быть очень р Основа любого дата-центра — это инженерные системы, которые представляют собой сложное профессиональное оборудование, которое недоступно для покупки в локальную серверную. То, как будет работать ЦОД, зависит от правильной реализации инженерных систем. Всего можно выделить 5 главных инженерных систем дата-центров:

* **Электроснабжение.** Главный источник жизни ЦОДа. От того, насколько правильно и бесперебойно осуществляется электропитание дата-центра, зависит стабильность работы размещенного в нем оборудования. Поэтому ЦОД подключают к электросети по нескольким независимым «вводам», устанавливают системы бесперебойного питания, а также подключают дополнительный дизельный генератор на случай полного отключения.
* **Кондиционирование.** Так как перегрев оборудования недопустим, а любая вычислительная система потребляет много энергии и выделяет большое количество тепла, помещение машинного зала должно очень хорошо охлаждаться. Для охлаждения ЦОД используют профессиональные прецизионные кондиционеры, а также различные современные системы, такие как фрикулинг.
* **Безопасность.** Важно не только разместить оборудование заказчика в здании ЦОД, но и обеспечить его полную безопасность и конфиденциальность хранимых данных. Системы безопасности ЦОД включают систему контроля доступа, видеонаблюдение, пожарную сигнализацию, систему экстренного пожаротушения и другие. Важно превентивно устранять проблемы. Так, например, использование специальных датчиков раннего обнаружения пожара позволяют избежать масштабных катастроф. Также в ЦОД строго регламентируется физический доступ к размещенному оборудованию — за это отвечает собственная служба безопасности.
* **Передача данных.** Стабильный и бесперебойный процесс передачи данных важен для любого дата-центра. Для его обеспечения используют как выделенные каналы, так и общедоступные интернет-сети с широкой полосой пропускания. Каналы обязательно резервируются.
* **Диспетчеризация.** Обеспечение стабильной работы всего ЦОД невозможно без системы мониторинга и диспетчеризации. За всеми системами ведется круглосуточное наблюдение, а устранение обнаруженных проблем происходит по заранее разработанным алгоритмам. Это исключает ошибки и позволяет решать проблемы максимальной

Кроме правильной организации работы дата-центра необходимо организовать резервирование всех систем для повышения надежности. Все схемы резервирования обозначают символом N, происходящим от слова «need» (необходимость).

Любая система состоит из различного количества критичных компонентов, каждый из которых является необходимым для ее функционирования. Рассмотрим основные схемы резервирования:

* **N**. В этом варианте отсутствует дополнительное резервирование. Надежность системы напрямую зависит от качества реализации каждого структурного элемента. Соответственно, если один компонент перестает работать, то и вся система прекращает функционировать. Данная схема устаревшая и сегодня не используется.
* **N+1**. Подразумевает наличие одного запасного элемента, который не используется до возникновения проблемы в работе системы. Как только один из критических компонентов выйдет из строя — резервный его заменит, а на работу системы это никак не влияет. Единственный недостаток схемы: для проведения ремонтных работ систему придется полностью выключить.
* **2N**. Ее использование подразумевает наличие для каждой системы еще двух параллельно работающих элементов. В этом случае нагрузка будет равномерно распределяться между компонентами, и ни один элемент не будет перегружен. При таком варианте, даже если один элемент системы полностью выйдет из строя, другой все равно будет работать.
* **2N+1**. Схема идентична 2N, но строится с применением еще одного дополнительного элемента. Этот вариант дает возможность проводить ремонтные работы без остановки системы.
* **2(N+1).** Отличие от предыдущей схемы в том, что здесь дублируется даже дополнительный элемент.
* **3/2N**. Выгодная схема резервирования, так как нагружается на 2/3, а не на ½, что довольно эффективно. Производительность системы увеличивается, а ее амортизация уменьшается.

Для оценки эффективности ЦОД по размещению в нем вычислительного оборудования, которая учитывает надежность и уровень резервирования систем, разработана система сертификации Tier от организации Uptime Institute.

Уровни сертификации:

* **Tier 1**. Самый слабый уровень, он подразумевает базовую надежность с применением схемы N. Данный сертификат уже давно устарел и последний раз применялся 50 лет назад. В его требованиях даже наличие бесперебойного питания не является обязательным. При таком подходе уровень доступности ЦОД составляет 99,671%, что соответствует около 30 часам простоя в год.
* **Tier 2**. Можно получить со схемой резервирования N+1. В данном случае все равно остается необходимость останавливать работу системы во время проверок или ремонта, но уже присутствует довольно значительная степень резервирования. Это сертификат предъявляет небольшие требования к системе охлаждения и энергообеспечения, но наличие фальшпола уже обязательно. Время простоя в год — 22 часа.
* **Tier 3**. ЦОД на данном уровне не нуждается в остановке систем для ремонта или обслуживания, резервируются все необходимые компоненты, имеется два канала распределения электропитания, но постоянно используется лишь один. Время простоя в год — 1,6 часа.
* **Tier 4**. Самый высокий уровень надежности работы дата-центра. Используется последняя схема резервирования, соответственно каждая инженерная система имеет дубликат основного узла и резервного. Время простоя в год — 0,8 часа.

Практически все финансовые и трудовые затраты при организации функционирования дата-центра приходятся на обеспечение надежности, безопасности и отказоустойчивости технических площадок. И это неудивительно, ведь главная задача ЦОДа — предоставление возможности размещения вычислительных систем заказчика и обеспечения условий для их бесперебойной работы.

Многие дата-центры имеют свое собственное вычислительное оборудование, на базе которого они оказывают ряд облачных услуг. Для клиента такой ЦОД выступает в качестве хостинг-провайдера.

Дополнительные услуги, которые предоставляют дата-центры:

* **Аренда VPS (Virtual Private Server).** Клиентам ЦОД предоставляется виртуальный сервер, управлять которым можно при помощи панели управления. Пользователь сам управляет работой виртуальной машины, а также вносит различные изменения на уровне операционной системы.
* **Аренда сервера (Dedicated Server)**. Услуга, которая позволяет арендовать физический сервер целиком.
* **IaaS (Infrastructure as a Service).** Эту услугу предоставляют не все ЦОДы. Клиент получает полную виртуальную инфраструктуру, которая отличается надежностью и полным абстрагированием от физических ресурсов.

Посмотрев на этот список дополнительных услуг, можно подумать, что ЦОД — это универсальный поставщик решений для разных типов пользователей. В теории это верно, но на практике немного не так. Проще говоря, для предоставления услуги IaaS нужно вкладывать большие средства в парк оборудования и программного обеспечения. Также немаловажно иметь высококвалифицированный персонал, потому что такая услуга направлена на решение большого спектра задач клиентов и рядовой ИТ-специалист в одном лице с этим не справится.

Стоит отметить, что аренда VPS востребована небольшими организациями и частными лицами, соответственно, она способна заменить для них IaaS.

Так как самая главная статья расходов при эксплуатации ЦОД — это обслуживание его систем, то предоставление VPS на ограниченной аппаратной платформе целесообразно, а построение IaaS может оказаться слишком дорогой задачей.

Таким образом, становится понятно, что организация работы ЦОД подразумевает тонкую настройку множества систем, а обеспечение их непрерывной работы и безопасности — непростая задача даже для высокопрофессионального персонала.

Работа ЦОД в целом зависит от схем резервирования, которые должны быть обязательно сертифицированы. Выбирая поставщика облачных услуг, следует обратить внимание на то, в каком конкретно ЦОД размещено его оборудование, — так можно оценить уровень надежности. А проведение миграции и организацию управления виртуальной инфраструктурой следует доверить профессиональному сервис-провайдеру.

Контрольные вопросы

1.Что такое ЦОД?

**Лекция №16**

**Обзор компонент SystemCenter 2012 R2**

**Планирование и реализация стратегии виртуализации серверов**

**Рассматриваемые вопросы**

**1.Компонент SystemCenter 2012 R2**

**2.Стратегия виртуализации серверов**

Настройке сети в System Center 2012 R2 Virtual Machine Manager. Сеть в VMM можно условно поделить на три уровня:

**1. Физическая сеть (Phisical network)** — каждый хост виртуализации может быть подключен к одной или нескольким физическим сетям. Это могут быть сети, разделенные физически, с помощью VLAN или другой подобной технологии.  
**2. Логическая сеть (Logical network)**— логические сети в VMM строятся поверх физических сетей. Логические сети представляют из себя проекцию базовой физической инфраструктуры сети в виртуальную среду и позволяют моделировать сеть внутри VMM согласно потребностям, без необходимости разбираться в тонкостях сетевого окружения.  
**3. Сеть виртуальных машин (VM network)** — на базе логических сетей строятся сети ВМ, к которым и подключаются виртуальные машины, сервисы и т.п. Сети ВМ используют сетевую виртуализацию, что позволяет развернуть поверх каждой логической сети несколько независимых сетей ВМ, полностью изолированных как от логической сети так и друг от друга.

На каждом из уровней могут быть свои особенности, что с одной стороны дает большую гибкость при создании сетевой инфраструктуры, однако с другой усложняет сам процесс настройки. Описать все нюансы в рамках одной статьи не представляется возможным, поэтому я просто опишу один из стандартных вариантов настройки.

Немного об инфраструктуре, на базе которой будет производится настройка. В тестовой среде развернуты 4 сервера:

SRV1 — контроллер домена, DNS-сервер и шлюз по умолчанию.  
SRV2 — управляющий сервер VMM и библиотека.  
SRV3 и SRV4 — хосты Hyper-V.

Каждый сервер имеет два сетевых интерфейса.

**Виртуализация серверов** — это технология эмуляции аппаратного обеспечения с применением специального ПО — гипервизора, — при которой создаётся виртуальная машина (сервер), обладающая назначенными ей ресурсами и вычислительными мощностями. На каждую такую виртуальную машину можно устанавливать различные операционные системы (их принято называть гостевыми), на которые, в свою очередь, можно устанавливать необходимые службы, сервисы, приложения.

Технологии виртуализации серверов также применяются для создания отказоустойчивого кластера (объединение серверов). Это позволяет при выходе из строя одного или нескольких серверов перенести нагрузку на функционирующие без остановки работы служб и приложений.

Сегодня виртуализация не является чем-то необычным. Технология используется практически везде при построении ИТ-инфраструктуры как для небольших компаний, так и для крупных ЦОД (центр обработки данных).

### Решения для виртуализации серверов

Ключевым элементом в решениях для виртуализации является специальное программное обеспечение — **гипервизор**. Он отвечает за создание виртуальных машин, управление ими, распределение аппаратных ресурсов между ними, позволяет независимо друг от друга их включать, выключать и перезагружать.

На рынке существует множество решений для виртуализации серверов. Самые популярные из них при создании ИТ-инфраструктуры:

* Microsoft Hyper-V — входит в состав лицензий Microsoft Windows Server, бесплатно доступен как отдельный продукт Microsoft Hyper-V (без ограничений функциональности, но без графического интерфейса);
* VMware ESXi — входит в состав платных версий vSphere;
* KVM — гипервизор для Linux-среды, бесплатное решение на базе Open Source;
* Citrix Hypervisor (ранее XenServer) — доступен как отдельный платный продукт или в составе продуктов Virtual Apps и Virtual Apps&Desktops. Чаще используется в [VDI-инфраструктуре](https://www.azone-it.ru/virtualizaci-rabochih-mest-vdi).

В связи с реализацией стратегии импортозамещения, также набирают популярность российские решения на базе KVM:

* программный комплекс «Средства виртуализации «Брест»;
* система управления средой виртуализации ROSA Virtualization;
* система серверной виртуализации «Р-Виртуализация»;
* «Альт Сервер Виртуализации».

Выбор конкретного решения зависит от факторов:

* ИТ-инфраструктуры и её состава (для сценариев модернизации и [консолидации серверов](https://www.azone-it.ru/konsolidaciya-serverov));
* задач, которые требуется реализовать;
* компетенций и предпочтений технических специалистов;
* бюджета;
* наличия сертифицированных версий;
* нахождения в реестре российского программного обеспечения и т. д.

Контрольные вопросы:

1.Поясните что значит виртуализация сервера

**Лекция № 17**

Планирование развертывания диспетчера виртуальных машин (VMM). Планирование и реализация серверной виртуализации

Рассматриваемые вопросы

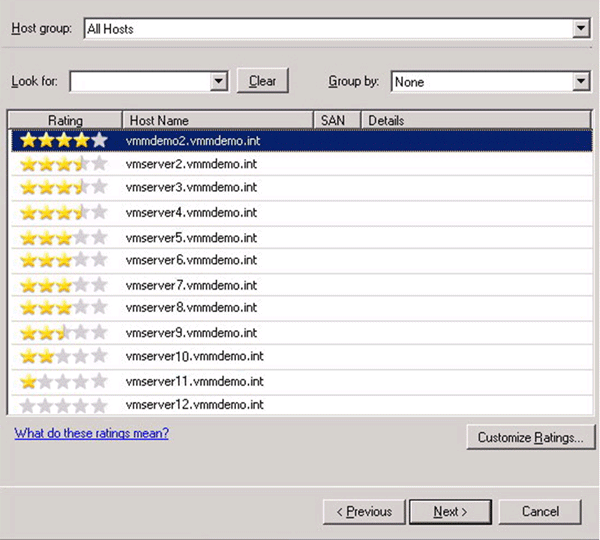
1.Диспетчер VMM

2. Серверная виртуализация

Обзор возможностей Virtual Machine Manager

Ключевое достоинство Virtual Machine Manager — тесная интеграция с другими решениями Microsoft для управления инфраструктурой Windows-серверов семейства System Center. SCVMM позволяет создать гибкую виртуальную инфраструктуру на основе платформы Virtual Server 2005 R2 и упростить развертывание виртуальных систем из центральной библиотеки шаблонов.

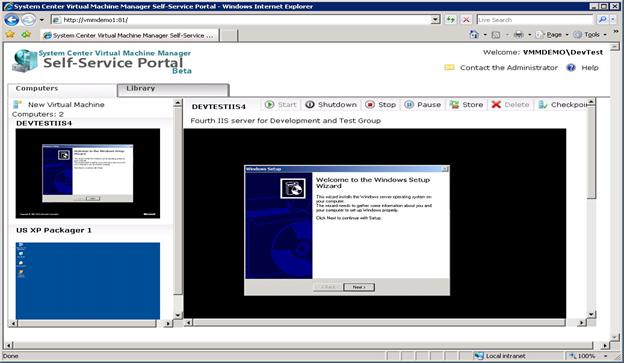
Virtual Machine Manager обладает возможностью интеллектуально размещать виртуальные серверы на физических компьютерах, используя данные об их рабочих нагрузках. Это позволяет системным администраторам управлять развертыванием виртуальных систем, основываясь на требованиях к их доступности, и создавать сбалансированную виртуальную инфраструктуру. Рейтинг каждого из физических серверов в отношении готовности к развертыванию на них виртуальных систем может быть представлен в виде условных очков, отображаемых звездочками.



SCVMM позволяет использовать командную оболочку PowerShell для написания сценариев автоматизации операций с виртуальными системами. Например, во время процедуры миграции с физического сервера на виртуальный можно получить скрипт PowerShell, просто нажав на кнопку «View Script». В дальнейшем его можно использования для написания сценария потоковой миграции.Централизованное управление и настройка ресурсов

Консоль администратора Virtual Machine Manager позволяет централизованно управлять всеми аспектами виртуальных систем, а также проводить «горячую» миграцию виртуальных машин с одного физического сервера на другой в случае возросшей нагрузки или необходимости остановки сервера на обслуживание.Простота развертывания

SCVMM имеет собственный портал самообслуживания, используя который пользователи, обладающие необходимыми правами, могут сами развернуть виртуальные машины с помощью мастера, не прибегая к услугам системных администраторов.



Virtual Machine Manager имеет отдельный компонент — централизованную библиотеку шаблонов, которая содержит в себе ISO-образы для установки гостевых систем, готовые к развертыванию виртуальные машины, а также различные сценарии настройки после установки и шаблоны. Библиотека позволяет избежать дублирования «строительных блоков» виртуальной инфраструктуры на различных компьютерах и организовать к ним простой доступ с возможностью поиска элементов.Централизованный мониторинг и отчетность.

SCVMM представляет собой многокомпонентное и гибкое решение для развертывания виртуальных инфраструктур различного масштаба. Продукт может применяться как в малых и средних предприятиях для управления несколькими серверами виртуализации, так и в крупных организациях с сотнями виртуальных серверов, где присутствуют другие решения на основе продуктов семейства System Center. Компоненты SCVMM могут быть разнесены по разным физическим компьютерам, управление и обслуживания каждого из которых может быть назначено отдельному человеку. На данный момент виртуальная инфраструктура на базе SCVMM не обладает такими широкими возможностями, как Virtual Infrastructure 3 компании VMware, однако с приходом технологии Hyper-V на базе Windows Server 2008 ситуация, возможно, изменится. Учитывая маркетинговые возможности Microsoft и сеть ее партнерств, а также степень интеграции Virtual Machine Manager с другими инфраструктурными решениями.

Компоненты продукта Virtual Machine Manager могут быть развернуты на одном или нескольких управляющих серверах, при этом системные требования зависят от числа управляемых серверов виртуализации. В случае если все компоненты SCVMM развертываются на одном физическом сервере, необходима следующая конфигурация:

Аппаратный компонент

От 5 до 10 управляемых серверов виртуализации

Процессор Pentium 4, 2 ГГц Dual-Core Pentium 4, 3,2 ГГц или выше

Объем оперативной памяти 2 ГБ 2 ГБ

Жесткий диск 80 ГБ 150 ГБ

От 11 до 20 управляемых серверов виртуализации

Процессор Pentium 4, 2,8 ГГц Dual-Core Pentium 4, 3,2 ГГц или выше

Объем оперативной памяти 2 ГБ 4 ГБ

Жесткий диск 150 ГБ 200 ГБ

Кроме того, при установке компонентов на один физический сервер необходимо соблюдение условий:

Операционная система Windows 2003 Server (Windows XP и Vista поддерживается только для некоторых компонентов SCVMM)

Windows Remote Management (WinRM)

Microsoft SQL Server 2005 (подойдет и бесплатный Express Edition)

Управляющая оболочка Windows PowerShell

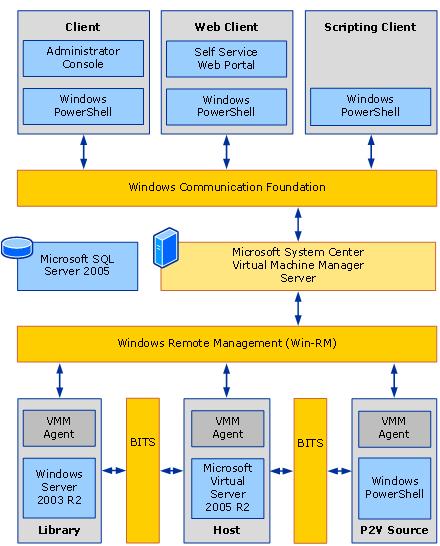
Службы Internet Information Services (IIS) 6.0

Microsoft .NET Framework 2.0 и 3.0

При разнесении сервера баз данных, управляющего сервера, консоли администратора, портала самообслуживания и библиотеки виртуальных шаблонов на разные физические серверы стоит придерживаться рекомендаций Microsoft для каждого из этих компонентов.

Для управления инфраструктурой до 150 физических серверов виртуализации, в качестве управляющего сервера вполне подойдет компьютер с частотой процессора 3 ГГц и четырьмя гигабайтами оперативной памяти (всего поддерживается не более четырехсот физических серверов). При этом стоит заранее спланировать большой объем дискового пространства для сервера баз данных и хранилища виртуальных шаблонов. Для портала самообслуживания и консоли администратора требования невысоки.

Компоненты Virtual Machine Manager могут быть установлены, как на одном физическом сервере, так и разнесены по нескольким. При этом осуществляется их тесное взаимодействие, как между собой, так и с другими элементами инфраструктуры System Center. Архитектура решения представлена ниже:



основным компонентам SCVMM относятся:Virtual Machine Manager Server (управляющий сервер)

Это основной управляющий элемент продукта, который должен быть установлен первым. Он осуществляет взаимодействие всех компонентов решения SCVMM. Manager Server реализует службу, которая исполняет управляющие команды, передает файлы и контролирует взаимодействие с серверами виртуализации, хранилищами виртуальных шаблонов и другими компонентами. На управляемых компьютерах запущены специальные агенты VMM, которые обмениваются информацией с Manager Server посредством механизма Windows Remote Management. Кроме того, Manager Server соединяется с базой данных SQL Server, которая хранит конфигурационную информацию. По умолчанию Manager Server также является библиотекой виртуальных шаблонов.Virtual Machine Host (сервер виртуализации)

Под этим компонентом понимается непосредственно управляемый сервер виртуализации, на котором установлена платформа Virtual Server 2005 R2 SP1. Хосты могут быть добавлены из консоли администратора. При их добавлении на этих серверах устанавливается сама платформа, а также агенты для взаимодействия с Manager Server.Library (хранилище).

После установки SCVMM можно приступать к определению подходящих на роль серверов виртуализации компьютеров и, сделав это, можно начинать процесс миграции с физических систем на виртуальные. Необходимо убедиться, что в брандмауэре открыты необходимые порты для взаимодействия различных компонентов Virtual Machine Manager, и они не конфликтуют с портами, используемыми другими приложениями.

При планировании серверов для библиотек шаблонов нужно размещать их так, чтобы файлы, хранимые на них, передавались на серверы виртуализации с как можно более высокой скоростью. Если используются сети SAN, необходимо, чтобы хосты, использующие библиотеку, размещались на том же устройстве, что и сама библиотека. При развертывании виртуальных машин на серверах виртуализации, надо учитывать типовые и пиковые нагрузки на виртуальные системы, уделяя, в первую очередь, внимание показателю используемой приложениями в гостевых системах оперативной памяти, поскольку ее нехватка наихудшим образом сказывается на быстродействии.

К сожалению на данный момент, платформа Virtual Server не позволяет виртуальным машинам представлять несколько виртуальных процессоров в виртуальных машинах (Virtual SMP), поэтому нужно учитывать этот факт при их развертывании. Для приложений, нуждающихся в высокой доступности, возможно, имеет смысл иметь несколько виртуальных сетевых интерфейсов в виртуальной машине на случай отказа одного из них.

Портал самообслуживания может являться отличным средством при разработке и тестировании приложений для делегирования полномочий развертывания тестовых сред различным участникам группы разработки. Компания Microsoft рекомендует использовать протокол SSL (Secure Socket Layer) для защиты VMRC-соединения (Virtual Machine Remote Control) пользователей с порталом самообслуживания.

**Лекция №18**

**Планирование и реализация сетевой инфраструктуры и систем хранения данных для виртуализации**

**Рассматриваемые вопросы:**

**1.Сетевая инфраструктура**

**2.Система хранения данных**

[Виртуализация хранения данных](https://www.stekspb.ru/autsorsing-it-infrastruktury/canned-solutions/private-cloud/) — это представление ресурсов хранения в абстрактном виде, как логические пространства хранения (тома) и без привязки к физическим накопителям. Технология обеспечивает удобный и прозрачный способ управления хранением, когда реальные устройства хранения, подключенные по различным протоколам, воспринимаются как единый пул.

Системы виртуализации хранения данных подразумевают разделение пула ресурсов на отдельные логические диски, которые можно добавлять по мере потребностей. ИТ-администраторы через центральную консоль размещают ресурсы хранения из общего пула на сервер приложений, и последний воспринимает виртуальные тома как реальные физические устройства, подключенные напрямую. Это упрощает администрирование ИТ-инфраструктуры и сетей хранения данных в частности. В рамках одной инфраструктуры технология может использоваться для разных задач: виртуализации серверов, приложений, рабочих столов, сетевых и других ресурсов.

Технически сеть хранения данных можно реализовать двумя способами: через SAN или NAS. В SAN (Storage Area Network) доступ к данным реализован на блочном уровне, в ее виртуализированной системе серверы обращаются не к виртуальным дискам, а к виртуальным томам, которые можно увеличивать незаметно для сервера. В NAS (Network Attached Storage) виртуализация реализована на уровне файлов, когда отдельные файлы, а не блоки, перемещаются между NAS-устройствами незаметно для пользователя, а те обращаются к устройствам по логическим адресам.

Сильные стороны виртуализацию и использует эту технологию для снижения издержек. Грамотно реализованное решение помогает компании ускорить окупаемость инвестиций и снизить стоимость владения ИТ-инфраструктуры сети хранения данных. Конечные пользователи тоже выигрывают: им не приходится беспокоиться о том, что новые файлы займут слишком много места или дисковое пространство закончится в неподходящий момент.

В основном сетевая инфраструктура состоит из различных программных приложений и аппаратных компонентов. Маршрутизация и переключения являются ключевыми функциями любой сети. Каждое задействованное устройство и серверы подключаются через свой сетевой кабель к коммутатору так, что в конце каждого устройства можно напрямую подключиться к любому другому. Основными компонентами сети являются сетевые кабели, с которыми связаны все серверы, компьютеры, принтеры, коммутаторы, маршрутизаторы, точки доступа и т. д.

**Лекция №19**

**Планирование и развертывание виртуальных машин**

Параметры виртуальных машин.

Рассматриваемые вопросы

1.Развертывание виртуальных машин

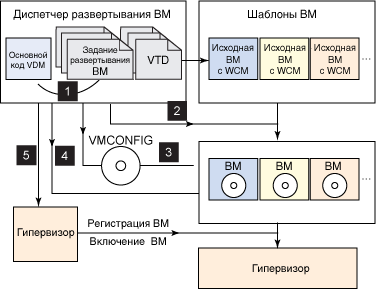
2.Параметры виртуальных машин

При создании и тестировании программ часто бывает необходимо создавать сразу несколько виртуальных машин. Нужно выбрать и скопировать шаблон виртуальной машины, изменить имя и параметры оборудования и устранить конфликт аппаратных адресов сетевых интерфейсов. Добавим сюда настройку сетевых параметров, имени хоста и параметров домена – и это быстро превратится в трудоемкую задачу

Рассматриваемое средство автоматического развертывания виртуальных машин состоит из двух основных частей: диспетчера развертывания виртуальных машин (Virtual Machine Deployment Manager, VDM) и диспетчера настройки виртуальных машин (Virtual Machine Configuration Manager, VCM).

Диспетчер развертывания виртуальных машин обрабатывает запросы пользователя по развертыванию ВМ, такие как клонирование образов ВМ, настройка параметров оборудования ВМ и регистрация ВМ в гипервизоре.

Диспетчер настройки виртуальных машин устанавливается на образе виртуальной машины, используемом в качестве шаблона ВМ, после загрузки системы он автоматически настраивает виртуальную машину. Архитектура и процесс автоматического развертывания ВМ показаны на рисунке



VDM состоит из трех частей:

* Основной код VDM, ядро VDM.
* Задания развертывания ВМ – файл описания отдельного задания развертывания ВМ, разновидность пользовательского файла конфигурации.
* Определения шаблона ВМ (VM Template Definitions, VTD) – файлы, содержащие информацию шаблонов ВМ, такую как расположение и описание шаблона ВМ. Шаблон ВМ представляет собой виртуальную машину, которая используется как источник для клонирования ВМ.

Основная часть процесса развертывания ВМ состоит из следующих этапов:

1. VDM считывает информацию из задания развертывания ВМ.
2. VDM ищет соответствующий шаблон ВМ в каталоге, содержащем файлы VTD, и клонирует шаблон ВМ в расположение, указанное в файле задания развертывания.
3. После клонирования исходной ВМ VDM собирает все данные конфигурации, упаковывает их в файл ISO и затем копирует его в каталог с копией ВМ.
4. VDM изменяет параметры оборудования клона ВМ на основе настроек, указанных в файле задания развертывания ВМ. Также создается устройство CD-ROM для монтирования файла ISO.
5. На последнем этапе развертывания запускаются утилиты гипервизора для регистрации ВМ и ее последующего запуска.

Пользователь может не указывать эти действия в файле задания развертывания ВМ. В качестве гипервизора может выступать VMware Server, Xen и т. п. В качестве примера реализации для подготовки этой статьи использовался VMware Server.

VCM устанавливается на ВМ, служащей шаблоном. После включения системы, он автоматически запускается и ищет CD с данными конфигурации, а затем запускает необходимые приложения, чтобы выполнить все предварительно настроенные действия.

Параметры виртуальной машины

Можно задать следующие параметры виртуальной машины.

Имя

Имя по умолчанию: Новая виртуальная машина

Введите имя для новой виртуальной машины.

Хранилище

Начальная настройка: хранилище сервера виртуализации по умолчанию, если новая машина создается на сервере виртуализации. В противном случае это папка документов текущего пользователя.

Это хранилище, где будет создана новая виртуальная машина. Возможность изменить хранилище на сервере виртуализации зависит от настроек и бренда продукта виртуализации. VMware ESX позволяет иметь несколько хранилищ. Сервер Microsoft Hyper-V позволяет создать новую виртуальную машину в любой локальной папке.

Память

Начальная настройка: если этого параметра нет в резервной копии, то это параметр по умолчанию сервера виртуализации.

Это объем памяти, выделяемой новой виртуальной машине. Диапазон изменения памяти зависит от оборудования хоста, операционной системы хоста и настроек продукта виртуализации. Например, виртуальным машинам может быть разрешено использовать не больше 30 % памяти.

Диски

Начальная настройка: количество и размер дисков исходной машины.

Количество дисков, как правило, равно таковому на исходной машине. Оно может быть другим, если в программу добавляются дополнительные диски, чтобы из-за ограничений, налагаемых продуктом виртуализации, соответствовать количеству томов на исходной машине. Виртуальные диски можно добавлять в конфигурацию машины или в некоторых случаях удалять предложенные диски.

При добавлении нового виртуального диска наряду с указанием интерфейса и производительности можно задать его формат.

Экономичный формат. Диск занимает такую же часть пространства памяти, что и данные, которые на нем хранятся. Это способствует экономии пространства памяти. Чтобы включить экономичный формат, выберите флажок Экономное распределение (для ESX) или Динамически расширяющийся диск (для Hyper-V).

Полный формат. Диск занимает все подготовленное пространство памяти. Это способствует повышению производительности виртуальной машины. Чтобы использовать полный формат, снимите флажок Экономное распределение (для ESX) или Динамически расширяющийся диск (для Hyper-V).

Если резервная копия создана для физической машины, настройкой по умолчанию является полный формат. При восстановлении из резервной копии виртуальной машины программное обеспечение пытается воспроизвести формат дисков исходной машины. Если это невозможно, используется полный формат.

Реализация машин Xen основана на Microsoft Virtual PC и наследует его ограничения: до 3 дисков IDE и 1 процессор. Использование дисков SCSI не поддерживается.

Процессоры

Начальная настройка: параметр сервера по умолчанию, если этого параметра нет в резервной копии или параметр из резервной копии не поддерживается сервером виртуализации.

Это количество процессоров новой виртуальной машины. В большинстве случаев этот параметр имеет значение 1. Положительный результат назначения машине нескольких процессоров не гарантируется. Количество виртуальных процессоров может зависеть от конфигурации ЦП хоста, продукта виртуализации и гостевой операционной системы. Обычно несколько процессоров становятся доступными на многопроцессорных хостах. При наличии ЦП многоядерного хоста или гиперпотоковой организации может стать возможным применение нескольких виртуальных процессоров на однопроцессорном хосте.

Контрольные вопросы

1.Дайте определение что такое виртуальная машина?

2.Назовите параметры виртуальной машины

**Лекция №20,21**

Подготовка к развертыванию виртуальных машин с использованием диспетчера виртуальных машин (VMM).

Развертывание виртуальных машин. Планирование и реализация реплики Hyper-V

**Планирование и реализация решения по администрированию виртуализации**

Рассматриваемые вопросы

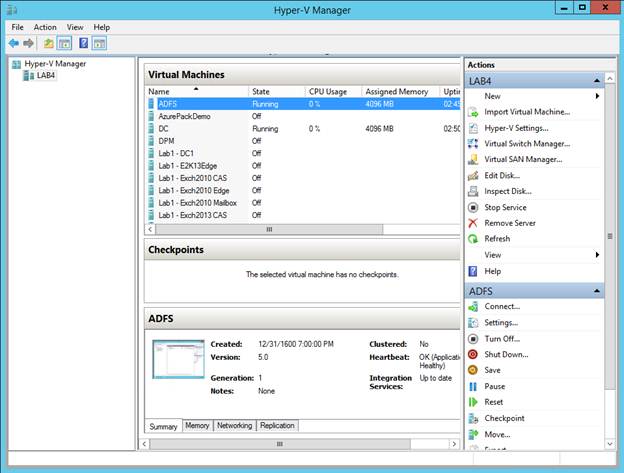
1.Диспетчер виртуальных машин

2.Реплика Hyper-V

Диспетчер Виртуальных Машин (Virtual Machine Manager, VMM) System Center 2012 R2, в случаях, когда используется отказоустойчивый кластер, репликация Hyper-V, несколько хостов Hyper-V, или несколько физических серверов. Диспетчер Виртуальных Машин System Center 2012 R2 (далее просто Диспетчер Виртуальных Машин) - это инструмент управления, который предназначен для того, чтобы сделать Hyper-V намного проще для управления этими серверами по мере того, как размер развёртывания Hyper-V увеличивается.

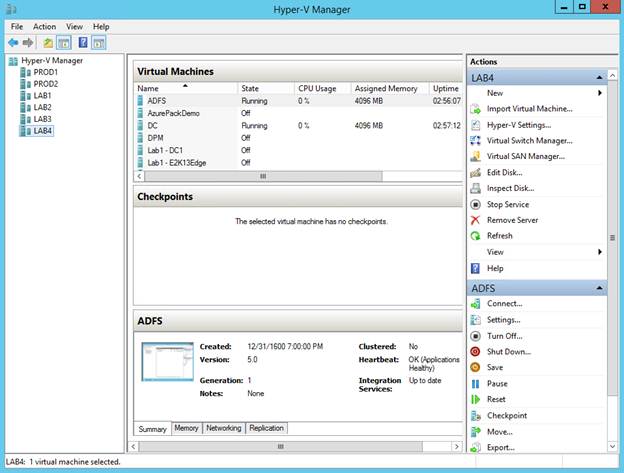
Диспетчер Виртуальных Машин также предоставляет ряд возможностей Hyper-V, к которым нельзя получить доступ через Диспетчер Hyper-V или через Диспетчер отказоустойчивости Кластеров.Сначала поговорим о масштабируемости, потому что Диспетчер Виртуальных Машин изначально был представлен как решение для масштабирования Hyper-V.

Чтобы по-настоящему оценить возможности, предоставляемые Диспетчером Виртуальных Машин, взглянем на ограничения, которые присутствуют в Диспетчере Hyper-V. На Рис.1 показан Диспетчер Hyper-V.

****

Как показано на рисунке выше, Диспетчер Hyper-V разделен на три вертикальных столбца. В столбце слева указан хост-сервер. В верхней части среднего столбца перечислены все виртуальные машины, которые запущены на хосте. Хотя такая схема кажется достаточно логичной, она несовершенна с точки зрения масштабируемости. Как уже объяснялось ранее, большинство организаций, использующих Hyper-V в производственной среде, имеют более одного сервера Hyper-V. Тем не менее Диспетчер Hyper-V отображает только локальный сервер и работающие на нём виртуальные машины.

Это не означает, что нет способа ввести в Диспетчер Hyper-V информацию о других хостах Hyper-V. Если желаете, чтобы Диспетчер Hyper-V был в курсе о дополнительных хостах Hyper-V, это можно сделать, нажав правой кнопкой мышки на контейнер Диспетчера Hyper-V (расположенном в верхней левой части консоли) и выбрав команду «Присоединиться к Серверу» из контекстного меню. Таким образом, можно предоставить Диспетчеру Hyper-V имя другого Сервера Hyper-V. Как указано на рисунке ниже, с помощью Диспетчера Hyper-V можно управлять несколькими серверами Hyper-V



Хотя в Диспетчере Hyper-V есть возможности управления несколькими серверами, имеются проблемы с использованием Диспетчера Hyper-V для управления крупномасштабными развёртываниями Hyper-V. Во-первых, подключение к различным хостам Hyper-V должно быть установлено вручную. Серверы Hyper-V, показанные на рисунке выше, можно подключить в течение нескольких минут. Даже если это так, представьте, сколько времени займёт процесс (и сколько места возможностей для ошибок или опечаток), если придётся вручную подключать к консоли несколько десятков серверов Hyper-V.

Более серьёзная проблема с этим подходом заключается в том, что он не решает проблему масштабируемости. Если посмотреть на рисунок выше, то заметите, что Диспетчер Hyper-V отображает виртуальные машины для текущего выбранного хоста. Итак, что произойдёт, если нужно найти конкретную виртуальную машину? Диспетчер Hyper-V не содержит строки поиска. Переход по памяти также не является вариантом, поскольку виртуальные машины Hyper-V могут динамически мигрировать с одного хост-сервера на другой. Таким образом, хост, на котором вчера была виртуальная машина, может быть не тем же хостом, где находится виртуальная машина сегодня.

Если имеется большое количество хост-серверов Hyper-V, и нужно найти определённую виртуальную машину, то есть три варианта. Первый вариант заключается в ручной прокрутке списка виртуальных машин, содержащихся на каждом отдельном хост-сервере. Излишне говорить, что это не очень удобно в больших средах, потому что это занимает много времени и подвержено ошибкам.

Второй вариант - использовать Windows PowerShell. Командлет Get-VM можно использовать для поиска виртуальной машины по имени. Хотя этот метод работает очень хорошо, многим администраторам не комфортно работать в PowerShell.

Третий вариант - использовать Диспетчер Виртуальных Машин. Диспетчер Виртуальных Машин может предоставить консолидированный вид виртуальных машин на всех хост-серверах. Можно даже использовать Диспетчер Виртуальных Машин для просмотра виртуальных машин, работающих в средах VMware.

Теперь после того, как немного поговорили о преимуществах Диспетчера Виртуальных Машин, пришло время начать изучение работы диспетчера виртуальных машин. В следующей части рассмотрим, как установить Диспетчер Виртуальных Машин, и начнём обзор интерфейса Диспетчера Виртуальных Машин.

Контрольные вопросы

1.Поясните что такое диспетчер виртуальных машин

**Лекция №22**

Планирование и реализация автоматизации с использованием System Center 2012 R2.

Рассматриваемые вопросы

1.Автоматизация с использованием System Center 2012 R2

Microsoft System Center 2012 представляет собой комплекс из восьми базовых программных модулей:

* System Center Operations Manager позволяет решать задачи, связанные с мониторингом всей ИТ-инфраструктуры (включая ЦОД, частное и общедоступное облако), и обеспечивать прогнозируемую производительность и доступность приложений;
* System Center Configuration Manager служит для развертывания и настройки ПО, организации и контроля работы пользователей с мобильными, физическими и виртуальными средами с различных клиентских устройств на любых платформах;
* System Center Data Protection Manager обеспечивает резервное копирование и восстановление данных на дисках и ленте для серверов SQL Server, Exchange Server, SharePoint, виртуальных и файловых серверов, а также поддерживает ПК с Windows;
* System Center 2012 Endpoint Protection Manager позволяет консолидировать средства защиты ПК и управления ими в единое решение;
* System Center Virtual Machine Manager предназначен для управления виртуальными машинами (их создания, миграции и удаления), а также для развертывания ИТ-сервисов в средах на базе различных гипервизоров, в том числе на платформах VMWare, Citrix;
* System Center Orchestrator дает возможность автоматизировать рутинные процессы и операции, связанные с управлением ИТ-инфраструктурой. Встроенные шаблоны рабочих процессов значительно упрощают эту задачу;
* System Center Application Controller — компонент, реализованный в виде веб-консоли, которая обеспечивает единообразный подход к управлению ресурсами частного и общедоступного облака и позволяет владельцам приложений или служб самостоятельно развертывать новые экземпляры требуемой службы или приложения;

Пакет System Center обладает ведущими функциями Windows Server и контроля над рабочими нагрузками. За работоспособность инфраструктуры (физической, виртуальной и облачной) отвечает известная консоль управления и мониторинга Operations Manager. Интегрированное средство определения сетевой топологии способствует выполнению мониторинга уровня работоспособности виртуальной сети и сетевых устройств. Возможность детального отслеживания потенциала среды частного облака реализуется за счет прозрачного взаимодействия компонентов. С помощью продуктивного управления дисковыми пространствами и файловым хранилищем Windows Server можно настраивать производительность хранилищ, обеспечивая достойный уровень надежности и эффективности для критических рабочих нагрузок. Существует возможность мониторинга ресурсов Microsoft Azure: облачной модели IaaS и большого количества компонентов Azure. Также, пакет Microsoft System Center предполагает расширение мониторинга до пространства VMware, благодаря управленческому пакету VEEAM Management Pack. За счет поддержки операционных систем HP-UX, IBM AIX, RHEL/SUSE Linux и Oracle Solaris, предоставляется доступ к проверенным сервисам кросс платформенного мониторинга.

**Лекция №23**

Планирование и реализация MicrosoftSystemCenterAdministration.

Планирование и реализация Self-Service с использованием System Center 2012 R2.

Рассматриваемые вопросы

1.Реализация Microsoft System Center Administration

2.Реализация Self-Service

Системы самообслуживания (Self-Service) - это решения, позволяющие клиенту найти ответ на свой вопрос (решение своей проблемы) без обращения в службу поддержки. Такие системы экономят массу времени и денег за счет снижения нагрузки на саппорт.

Как правило, Self-Service система представляет собой базу знаний (Help, FAQ) с категориями и поиском, доступную клиентам через интернет-браузер. База знаний может содержать вопросы-ответы, мастера поиска решения, статьи, документы, файлы для загрузки. Обычно, такие решения имеют систему авторизации и могут быть персонифицированы под каждого клиента (например, учитывать уровень его SLA контракта, или то, какие продукты данный клиент купил).

Важным параметром в подобных решениях является возможность легкого обновления базы знаний сотрудниками поддержки, т.к. любой продукт постоянно развивается и совершенствуется. Очень удобно, если в формировании базы знаний могут принимать участие и сами клиенты.

Пользователи с ролью Self-Service User имеют право подключаться к VMM из консоли или через веб-портал и создавать и управлять виртуальными машинами и сервисами в тех пределах, которые им отведены вышестоящими администраторами. Пользователи Self-Service User не имеют прав на создание каких либо ролей в VMM.

**Лекция №24**

**Планирование и реализация стратегии мониторинга серверов** Планирование мониторинга в Windows Server 2012 R2.

Рассматриваемые вопросы

1.Мониторинг серверов

2.Мониторинг в Windows Server 2012R

Основной задачей системы мониторинга является предоставление актуальной информации для анализа состояния ИТ-инфраструктуры и быстрого обнаружения возникшей неисправности и ее оперативное устранение. Системы мониторинга производительности позволяют ИТ-специалистам вовремя заметить снижение производительности и определить «узкие места» в ИТ-инфраструктуре. Постоянный мониторинг помогает избежать простоев в ее работе, поддерживать все ИТ-сервисы в рабочем состоянии и сохранять необходимый уровень их качества, а также спланировать её модернизацию.

Сама структура мониторинга значительно видоизменяется с течением времени. Например, одна из тонкостей возникла при появлении и большом распространении виртуализации: если ранее была необходимость отслеживать состояние только физических серверов, то теперь на каждом из них может быть ещё несколько виртуальных.

System Center Operations Manager – система сквозного мониторинга от Microsoft, в том числе активного слежения за состоянием сетей (наблюдение за любыми сетевыми устройствами, поддерживающими SNMP, вплоть до уровня портов, а также обнаружение виртуальных локальных сетей и коммутаторов в таких сетях). В последних версиях появилась возможность слежения не только за системами, под управлением операционных систем семейства Windows, но и за гетерогенными средами, включающими UNIX и Linux. System Center Operations Manager предназначен главным образом для организаций с числом машин более 500 и числом серверов более 30. Для меньших организаций существует продукт System Center Essentials, включающий в себя часть функционала продуктов System Center Operations Manager и System Center Configuration Manager, но предназначенный для малых и средних предприятий.

Одно из главных достоинств System Center Operations Manager – продвинутая визуализация всего огромного собранного набора данных, в основном в виде графиков и диаграмм, причём визуализация доступна не только в специальной консоли программы, но и через веб-интерфейс. Элементы представления же можно подвергать тонкой настройке, пример интерфейса на рисунке 1. Версия 2012 поддерживает расширенное наблюдение за смешанными средами, а именно за машинами под управлением Unix и Linux (так называемых «систем \*nix: агент \*nix поддерживает HP-UX 11i версии 2 или 3 на базе PA-RISC и IA64, Sun Solaris 9 на базе SPARC и 10 на базе SPARC и 32-разрядной платформы, Red Hat Enterprise Linux 4, 5 и 6 на 32- и 64-разрядных платформах, Novell SuSE Linux Enterprise Server 9 на 32-разрядной платформе, 10 SP1 и 11 на 32- и 64-разрядных платформах, а также IBM AIX 5.3, 6.1 и 7.1 на базе POWER. Для мониторинга используются 2 ключа: sudo (для конфигурирования стандартной учётной записи с нужным уровнем доступа) и SSH (для безопасного обслуживания агента).

Zabbix – свободно распространяемая система для комплексного мониторинга сетевого оборудования, серверов и сервисов. Состоит из четырёх частей: Сервер мониторинга (ядро) – выполняет периодический опрос и− получение данных, обрабатывает их, анализирует, также осуществляет запуск скриптов для рассылки оповещений. Может удаленно проверять сетевые сервисы, является хранилищем, в котором хранятся все конфигурационные, статистические и оперативные данные. Не может располагаться на сервере под управлением операционной системы семейства Windows, а также OpenBSD

Прокси - собирает данные о производительности и доступности от имени Zabbix сервера. Все собранные данные заносятся в буфер на локальном уровне и передаются Zabbix серверу, к которому принадлежит прокси- сервер. Zabbix прокси является идеальным решением для централизованного удаленного мониторинга мест, филиалов, сетей, не имеющих локальных администраторов. Он может быть также использован для распределения нагрузки одного Zabbix сервера. В этом случае, прокси только собирает данные, тем самым на сервер ложится меньшая нагрузка на ЦПУ и на ввод/вывод диска. Агент – специальный демон, который запускается на отслеживаемых− объектах и предоставляет данные серверу, осуществляя контроль локальных ресурсов и приложений (таких как жесткие диски, память, статистика процессора и т. д.) на сетевых системах, т.е. эти системы должны работать с запущенным Zabbix агентом ( однако мониторинг можно производить не только с помощью него, но и по SNMP версий 1, 2, 3, запуском внешних скриптов, выдающих данные, и несколько видов

предопределенных встроенных проверок, таких как ping, запрос по http, ssh, ftp и другим протоколам, а так же замер времени ответа этих сервисов. Zabbix агенты являются чрезвычайно эффективными из-за использования встроенных системных вызовов для сбора информации о статистике. Zabbix-агенты поддерживаются не только на \*nix операционных системах, но и на AIX и Windows.

Администраторам, работавшим над Linux, трудно перейти на Windows. тем не менее **Windows-сервер мониторинга** не менее важен, чем мониторинг Linux; благодаря постоянно расширяющейся гетерогенной ИТ-инфраструктуре. Наличие правильного инструмента мониторинга Windows может помочь администраторам решить проблемы, определить медленно работающие приложения и другие связанные проблемы. Ниже приведены несколько аспектов Windows [мониторинг серверов](https://www.motadata.com/ru/product/network-management-and-monitoring/server-monitoring/) инструмент, который поможет вам поддерживать Windows в рабочем состоянии.

1. Мониторинг основных компонентов
2. Прогнозирование и планирование
3. Обновления статуса для оборудования и программного обеспечения
4. Настраиваемые уведомления
5. Интеграция с приложениями 3rd Party
6. Управление Инвентаризацией Активов

### Мониторинг основных компонентов

Наиболее важным аспектом мониторинга Windows является обеспечение правильного мониторинга основных компонентов ресурсов Windows по различным ключевым показателям, таким как использование диска, памяти и ЦП. Он помогает анализировать потребление ресурсов, а также дает представление о тенденциях и росте использования, которые могут повлиять на общую производительность. Получив подробное представление о вашем сервере Windows, вы можете легко спрогнозировать и спланировать, как основные компоненты могут время от времени меняться

### Прогнозирование и планирование

Как указано выше, после получения подробной информации инструмент мониторинга помогает планировать и прогнозировать, когда ресурс сервера достигнет уровня предупреждения и критические пороговые значения для различных показателей будут нарушены. Он анализирует исторические данные, чтобы помочь вам с такими тенденциями, как пиковое время, время простоя, средняя емкость по времени и т. Д., Чтобы определить, когда ресурс может закончиться.

### Обновления статуса для аппаратного и программного обеспечения

Понимание аппаратного и программного обеспечения крайне важно для обеспечения высокой производительности и доступности приложений Windows. Мониторинг ключевых компонентов, таких как виртуальные машины, жесткие диски, процессоры и т. Д., Позволит вам получить общее представление об общем состоянии ваших серверов Windows. Обработка обновлений состояния программного и аппаратного обеспечения с должным вниманием имеет первостепенное значение, так что вы готовы действовать в случае сбоев системы.

### Настраиваемые оповещения

Когда возникают сложные ситуации - быстрое устранение неполадок, мониторинг и оповещение в реальном времени имеют большое значение для ускорения среднего времени для решения любой проблемы. Инструмент мониторинга, если его можно настраивать, позволяет конечным пользователям получать уведомления всякий раз, когда возникает какая-либо серьезная проблема или до того, как какое-либо обновление Windows может повлиять на производительность сервера. Имея возможность настраивать общие параметры системы на ходу, пользователи могут убедиться, что бизнес-процессы работают оптимально и бесперебойно, а уведомления предупреждают вас до того, как произойдут сбои, а не вызывают неожиданные сбои.

### Интеграция с приложениями 3rd Party

И последнее, но не менее важное: для вашего мониторинга Windows одинаково важно иметь возможность наблюдать как за приложениями Microsoft, так и за инструментами сторонних разработчиков 3rd. Обладая единым взглядом на постоянно растущую ИТ-среду, вы получаете желаемую свободу расширения с помощью новых технологий. Гибкость интеграции повышает значимость, а также играет важную роль в развитии вашей ИТ-инфраструктуры.

* **Приложения Microsoft**: Windows Server, Active Directory, Windows Hyper-V, SQL Server, IIS, Exchange Server, Azure, SharePoint, DHCP, DNS и другие
* монитор **3rd сторонние приложения** такие как Oracle, Java, Linux, UNIX, VMware, AIX, Tomcat, Apache, Citrix и другие

### Управление Инвентаризацией Активов

Мониторинг Windows также помогает вам управлять ИТ-активами Windows, автоматически обнаруживая информацию об оборудовании и программном обеспечении, такую ​​как драйверы, встроенное ПО, жесткие диски, виртуальные машины, логические тома, память, сетевые интерфейсы, процессоры, установленное программное обеспечение и т. Д. Инструмент позволяет контролировать состояние и наличие серверных аппаратных компонентов, таких как температура, батарея, процессор, частота вращения вентилятора и блок питания, а также получение предупреждений о потенциальных сбоях, которые могут повлиять на производительность.

Принимая во внимание преимущества, которые предлагает мониторинг Windows, существует необходимость в инструменте мониторинга Windows, таком как Motadata, который предлагает интегрированный [инструмент мониторинга сервера](https://www.motadata.com/ru/blog/server-monitoring-tools/) Он предоставляет подробные сведения обо всех критических параметрах производительности сервера, таких как емкость жесткого диска, загрузка ЦП, использование памяти и использование полосы пропускания, с помощью интуитивно понятной веб-консоли. Наш мониторинг производительности сервера позволяет сисадмину быть в курсе проблем простоя и производительности сервера. Это программное обеспечение для мониторинга серверов способно контролировать все типы серверов ИТ-инфраструктуры как в условиях консолидированной, так и в распределенной рабочей нагрузки.

**Основные преимущества инструмента мониторинга Windows Server**

* Увеличение доступности серверов, сервисов и приложений
* Быстрое обнаружение сбоев сети и сбоев протокола
* Быстрое обнаружение сбойных служб, процессов и пакетных заданий
* Быстрое обнаружение неисправного оборудования, которое может отрицательно повлиять на время простоя системы
* Предотвращение мошеннических процессов, которые потребляют избыточные ресурсы сервера

**Лекция №25**

Обзор SystemCenterOperationsManager.

Планирование и настройка компонент мониторинга. Настройка взаимодействия с VMM

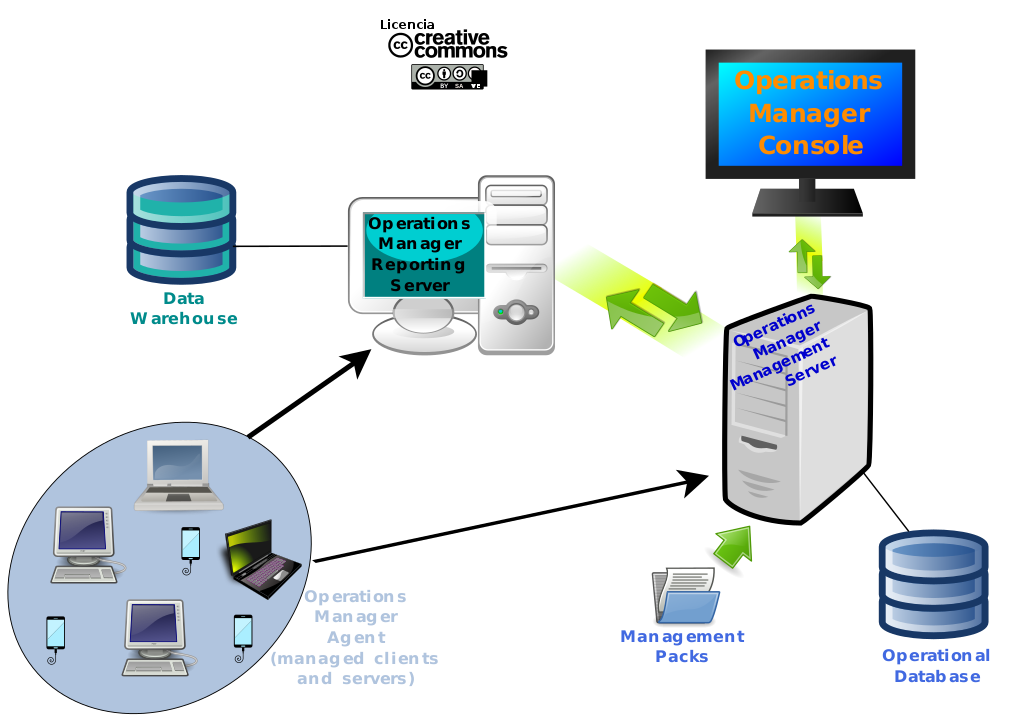
Рассматриваемые вопросы

1.System Center Operations Manager

System Center Operations Manager (SCOM) (ранее Microsoft Operations Manager, MOM) — программа компании Microsoft для управления и мониторинга ИТ-сервисов, приложений, серверов в гетерогенной среде Windows, UNIX и Linux. Продукт способен консолидировать информацию о функционировании различных компонентов ИТ-инфраструктуры, обеспечивая её обобщенное представление в единой консоли.

Существуют возможности для мониторинга различного системного и прикладного программного обеспечения, определения логики мониторинга самим администратором системы.

SCOM предназначен главным образом для организации с числом компьютеров более 500 и числом серверов более 30. Для меньших организаций существует продукт System Center Essentials, включающий в себя часть функциональности продуктов System Center Operations Manager и System Center Configuration Manager, но предназначенный для малых и средних предприятий.



System Center Operations Manager: Основные компоненты продукта.

**Лекция №26**

**Планирование и реализация NLB**

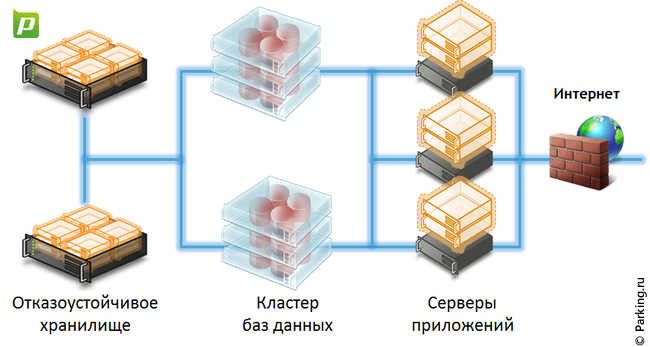
**Планирование и реализация решений высокой доступности на основе кластеров**

**Рассматриваемые вопросы**

**1.NLB**

**2.Решения высокой доступности на основе кластеров**

Pяд кластерныхрешений построенных на надежной дублированной инфраструктуре и имеющих в основе самые разные решения: от виртуальных машин до группы физических серверов. Отдельного внимания заслуживает предложение по ГЕО кластеризации в двух разных ЦОД, объединенных дублированными каналами связи.



#### Кластеры высокой доступности (High Availability cluster)

Создаются для обеспечения высокой доступности сервиса, предоставляемого кластером. Избыточное число узлов, входящих в кластер, гарантирует предоставление сервиса в случае отказа одного или нескольких серверов. Минимальное количество узлов — два, но может быть и больше.  
  
Обычно High Availability кластер строится для Microsoft SQL server'ов, который поддерживает базы данных интернет проектов. High Availability кластер возможно построить и для Exchange систем.  
  
Существует ещё одна разновидность High Availability SQL кластера — «зеркалирование БД» или database mirroring. Этот вид кластера не требует выделенного дискового хранилища, но для автоматического переключения в случае аварии нужен ещё один SQL сервер — следящий/witness. Такой кластер идеально подходит для WEB приложений и требует меньше затрат на создание.

#### Балансировка нагрузки (Network Load Balancing, NLB)

Принцип действия NLB-кластеров — распределение приходящих запросов на несколько физических или виртуальных узлов серверов. Первоначальная цель такого кластера — производительность, однако, они используются также для повышения надёжности, поскольку выход из строя одного узла приведет просто к равномерному увеличению загрузки остальных узлов. Совокупность узлов кластера часто называют кластерной фермой. Минимальное количество узлов в ферме — два. Максимальное — 32.  
  
При размещении высоконагруженных web-проектов в режиме NLB строится ферма web-серверов на IIS 7.х

#### Кластеры на виртуальных машинах

Наиболее доступным и масштабируемым решением является построение кластера на основе виртуальных машин на платформе Hyper-V.  
  
В качестве web-боксов NLB-кластера используются виртуальные машины с установленными на них Windows Web Server 2008 (IIS7.х, пользовательское приложение).  
  
В качестве кластера баз данных используется две виртуальные машины необходимой мощности на Windows Server 2008 Standard Edition и SQL Server 2008 Standard Edition.  
  
Отказоустойчивое единое хранилище данных на основе Storage System от NetApp или HP.  
  
Для обеспечения бОльшей надежности все узлы кластера располагаются на различных физических серверах\узлах кластера.  
  
Масштабируемость решения достигается путем увеличения мощности используемых виртуальных машин (вплоть до 100% мощности физического сервера), а также за счет добавления новых узлов в NLB-кластер.  
  
С использованием средств онлайновой миграции со временем возможен перенос узлов кластера на новые, более современные физические сервера без потери работоспособности и без простоя любого узла.  
  
Данный кластер является лучшим решением в соотношении цена/качество и рекомендуется как для критичных для бизнеса приложений, так и для относительно нагруженных web-проектов (~до 30000-50000 посетителей ежедневно).

#### Кластеры на физических серверах

Web-проекты с нагрузкой выше 50000 посетителей, проекты со специальными требования по безопасности требуют построения кластерных решений на выделенных серверах без потерь мощностей физических серверов на виртуализацию.  
  
Схема построения таких кластеров аналогична схеме построения кластеров на виртуальных машинах, только в качестве узлов используются выделенные физические серверы.