ТЕМА 3. ПЛАНИРОВАНИЕ И РАЗВЕРТЫВАНИЕ КОРПОРАТИВНОЙ ФИЗИЧЕСКОЙ ИНФРАСТРУКТУРЫ

В данной теме рассматриваются следующие вопросы:

- автоматизированная установка операционной системы Windows;
- наборы инструментов WADK и MDT;
- служба WDS;
- управление обновлениями операционной системы и приложений;
- служба WSUS;
- обзор технологий виртуализации;
- принципы построения высокодоступных и отказоустойчивых информационных систем;
- виртуализация Hyper-V;
- семейство продуктов System Center.

Лекции – 2 часа, лабораторные занятия – 2 часа, самостоятельная работа – 6 часов.

Минимальный набор знаний:

Программы для работы с WIM-файлами;

Назначение WinPE

Виды обновлений

Виды виртуализации

Типы виртуальных жестких дисков в Hyper-V

Понятие высокой доступности

Отказоустойчивые кластеры, виды кворума

Кластеры с балансировкой нагрузки

3.1. Автоматизированная установка операционной системы

3.1.1. Виды установки операционной системы

Когда требуется развернуть новые серверы или рабочие станции, то одним из главных вопросов является следующий: будет ли осуществляться сборка и развертывание этих систем вручную, или же процесс развертывания систем будет автоматизирован. Автоматизация развертывания систем не является задачей, которую можно выполнить в течение нескольких часов или дней, во всяком случае, не в первый раз. Наоборот, построение функциональной инфраструктуры развертывания операционных систем требует тщательного планирования, иногда — дорогих лицензий, и многих часов, дней или недель тестирования и настройки образов и механизмов автоматизации. Существует несколько разных вариантов развертывания сервера Windows и настольных операционных систем бизнес-класса. Это могут быть ручная установка, полностью автономные (не обслуживаемые) установки, автономные готовые или дополнительно настроенные установки, а также развертывания заготовленных и, возможно, специально настроенных образов операционной системы.

Ручная установка с использованием установочного носителя

Устанавливать систему вручную не очень сложно. Нужно воспользоваться установочным носителем и пройти все этапы установки, документируя по мере продвижения все настройки.

Этот способ иногда необходим, когда у администратора нет образа, подходящего для определенной аппаратной платформы, или когда регулярно развертывается только небольшое количество систем, а время, необходимое на создание автоматических установок или установок с использованием образов, не ограничено и не является ключевым фактором для организации.

Автономная (необслуживаемая) установка

Автономные установки могут быть полезными при развертывании большого количества настольных компьютеров и серверов, на которых установлено одинаковое оборудование.

Файл автономной установки представляет собой файл, содержащий ответы на все вопросы, задаваемые во время ручной установки. Конфигурационные файлы автономной установки обычно называют файлами ответов. Опции в некоторых файлах ответов автономной установки могут включать принятие лицензионного соглашения конечным пользователем, ввод лицензионного ключа, вариант форматирования жесткого диска, определение раздела или размера тома для операционной системы и многое другое. Теперь это называется файлом необслуживаемой установки (unattended installation file).

Сервер развертывания Windows выполняет некоторые из задач автономной установки, в основном задачу развертывания готового образа при присоединении к домену Active Directory. Если стандартная установка WDS по каким-то причинам неприемлема, можно создать автономные файлы для выполнения шагов установки: специальное разбиение жестких дисков на разделы, присоединение к домену, создание учетной записи локального администратора и ряд других. Создание и тестирование автономных файлов –

утомительное занятие, для которого необходим диспетчер образов систем Windows (Windows System Image Manager) из инструментального набора оценки и развертывания Windows (Windows Assessment and Deployment Kit) или же ручное редактирование XML-файлов.

Установка, сопровождаемая производителем

Некоторые производители поставляют носитель автономной установки, который сразу же после запуска предлагает администратору ответить на несколько вопросов, и оставшаяся часть установки происходит в автономном режиме. Этот распространенный сценарий встречается в секторе розничных продаж для домашних пользователей, а также для серверов и настольных компьютеров, поставляемых с установленными операционными системами.

Эти типы установок обычно включают лицензированное программное обеспечение от поставщика комплектного оборудования (Original Equipment Manufacturer — OEM). Здесь важно сказать следующее: если организация планирует выбрать вариант автономного развертывания серверов или настольных компьютеров с помощью систем развертывания или клонирования образов, то лицензию и носитель для операционной системы OEM использовать нельзя, поскольку это, как правило, противоречит лицензионному соглашению.

Серверные системы часто продаются с уже установленными операционными системами (OEM). Но многие серверы все-таки поставляются без операционных систем и требуют покупки или лицензирования установочного носителя. Многие производители предлагают установочные CD-диски, которые сначала выполняют опрос администратора, а затем по результатам этого опроса создают автономные файлы для установки серверной операционной системы Windows. В зависимости от ситуации и устанавливаемого ПО, это весьма удобный вариант, т.к. обычно он содержит все необходимые для оборудования драйверы и поддерживающее ПО для наблюдения за этим оборудованием.

Создание копий или образов систем

Создание копий или образов систем может быть полезно при развертывании нескольких идентичных настольных компьютеров и серверов. Вы создаете настольный компьютер или сервер, подготавливаете систему для клонирования или создания образа и копируете или захватываете образ системы с помощью средств сторонних разработчиков или средств развертывания от Microsoft, таких как WDS. Продукты Microsoft поддерживают клонирование и создание образов серверов и настольных компьютеров только в том случае, если для генерирования идентификаторов безопасности (Security Identifier — SID) нового компьютера используется утилита Sysprep.exe. Служба Windows Deployment Services может использоваться для развертывания установочных образов, а также специально настроенных или снятых установочных образов на серверах и настольных компьютерах, работающих под управлением Windows.

Microsoft и независимые поставщики программного обеспечения уже многие годы поддерживают создание образов и быстрое развертывание систем Windows. В настоящее время у Microsoft имеются три различных средства развертывания образов: служба развертывания Windows (Windows Deployment Services), диспетчер настроек системного центра (System Center Configuration Manager) и

инструментальный набор развертывания Microsoft (Microsoft Deployment Toolkit - MDT) 2012. В более ранних версиях Microsoft Windows Server также поставлялись средства развертывания как часть ОС и в виде отдельных пакетов компонентов.

3.1.2. Структура WIM-файла

WIM — это формат образа диска на основе файлов, который впервые был представлен в Windows Vista®. Файлы WIM представляют собой сжатые пакеты, содержащие несколько связанных файлов. Формат WIM-файла оптимизирован для максимального сжатия с использованием LZX или для быстрого сжатия с использованием XPRESS.

Структура файла WIM содержит до шести типов ресурсов: заголовок, файловый ресурс, ресурс метаданных, таблицу поиска, данные XML и таблицу целостности. На рис. 3.1 показан общий макет WIM-файла, который содержит два образа.

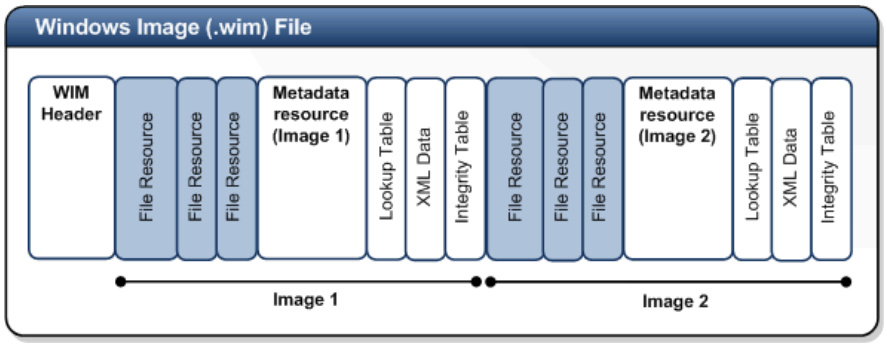

Рис. 3.1. Структура WIM-файла

Заголовок WIM. Определяет содержимое WIM-файла, включая расположение ключевых ресурсов (ресурс метаданных, таблицу поиска, данные XML) и различные атрибуты WIM-файла (версия, размер, тип сжатия).

Файловые ресурсы. Серия пакетов, содержащих данные, например, исходные файлы.

Ресурс метаданных. Содержит информацию о файлах, которые включены в образ, включая структуру каталогов и атрибуты файлов. Для каждого образа в WIM-файле есть один ресурс метаданных.

Lookup Table. Содержит расположение файлов ресурсов в WIM-файле.

XML Data. Содержит дополнительные данные об изображении.

Таблица целостности. Содержит информацию о хэш-безопасности, которая используется для проверки целостности изображения во время операции приложения.

Для работы с WIM-файлами используют программы ImageX и DISM из состава WADK. DISM также входит в состав Windows. Эти программы обладают сходной функциональностью, но запись параметров выполняется по-другому. Для иллюстрации различий приведены некоторые примеры.

Создание нового образа на основе жесткого диска с установленной операционной системой:

```
imagex /capture <другие параметры>
DISM /Capture-Image <другие параметры>
```

Применение WIM-файла к жесткому диску (то есть, копирование файлов из WIM-файла на жесткий диск):

```
imagex /apply <другие параметры>
DISM /Apply-Image <другие параметры>
```

Смонтировать (отобразить) WIM-файл на папку на диске и предоставить доступ к его содержимому посредством обычных файловых операций:

```
imagex /mount image_file image_number <другие параметры>
DISM /Mount-Image /ImageFile:<path_to_image_file> <другие параметры>
```

3.1.3. Использование файлов ответов

Во время стандартной установки Windows мастер установки задает оператору различные вопросы, например, параметры разметки жесткого диска, лицензионный ключ, имя пользователя и т. д. Такие параметры можно вручную указать в файле ответов, и он обеспечит автоматический ответ во время установки. Файл ответов — это текстовый файл в формате XML с именем Autounattend.xml.

Чтобы выбрать файл ответов во время установки, нужно загрузить среду предустановки Windows и выполнить команду setup.exe с параметром /unattend:filename. При отсутствии параметра /unattend программа установки будет искать файл с именем Autounattend.xml в корневых папках всех доступных дисков. Поэтому проще всего записать файл ответа на USB-устройство флэш-памяти, вставить его в компьютер, а затем загрузить этот компьютер с установочного диска Windows.

Так как файл ответов — это текстовый файл, его можно создать в любом текстовом редакторе, взяв за отправную точку образец в комплекте средств для развертывания и оценки Windows (Windows ADK) в папке C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Deployment Tools\Samples\Unattend.

Но намного удобнее использовать специальную программу — диспетчер установки Windows® (Windows SIM). Созданные вручную файлы ответов также необходимо проверять в диспетчере установки Windows.

Иногда можно использовать нескольких файлов ответов. Например, в ходе установки Windows можно использовать общий файл ответов, который содержит сведения о компании и поддержке. После завершения установки и при запуске средства Sysprep можно применить второй файл ответов для добавления дополнительных настроек.

3.1.4. Набор инструментальных средств Windows Assessment and Deployment Kit

Комплект средств для развертывания и оценки Windows (Windows ADK) содержит средства, необходимые для настройки образов Windows для широкомасштабного развертывания, а также для проверки качества и производительности системы, добавленных компонентов и приложений. Может быть бесплатно загружен с сайта Microsoft.

Инструменты Windows ADK можно разделить на две категории.

● Набор средств оценки Windows и набор средств оценки производительности Windows, используемые для оценки качества и производительности систем и компонентов.

● Средства развертывания, такие как WinPE, Sysprep и DISM, и другие средства, которые можно использовать для настройки и развертывания образов Windows 10.

Ниже перечислены инструменты, входящие в Windows 10 ADK:

Windows Configuration Designer

Windows Preinstallation Environment (WinPE)

Deployment Image Servicing and Management (DISM)

Windows System Image Manager (WSIM)

Windows Assessment Toolkit

Windows Performance Toolkit

User State Migration Toolkit (USMT)

Volume Activation Management Tool (VAMT)

User Experience Virtualization (UE-V)

Application Virtualization (App-V)

Кратко опишем некоторые инструменты.

Windows Preinstallation Environment (Windows PE). Минимальная операционная система, предназначенная для подготовки компьютера для установки и обслуживания Windows. Работает целиком в оперативной памяти, то есть не требует жесткий диск. Для предотвращения использования WinPE в производственной среде она автоматически перезагружается через 72 часа, при этом теряются все настройки. Также недоступны многие функции Windows.

User State Migration Tool (USMT) (Инструмент миграции состояния пользователей (USMT)). Инструмент USMT переносит данные пользовательских учетных записей и настройки приложений на целевую машину. Это экономит время администратора, но не воссоздает систему в первоначальном состоянии.

Deployment Tools (Инструменты развертывания). Инструменты развертывания требуются для выполнения автономной установки потому, что именно они выполняют такую автоматизированную установку. Фактически это подмножество инструментов для ADK. Оно содержит несколько поддерживающих программ, таких как инструмент обслуживания и управления образами (Deployment Image Servicing and Management — DISM), инструмент активации OEM (OEM Activation) и диспетчер образов систем Windows (Windows System Image Manager), а также другие средства.

3.1.5. Служба Windows Deployment Services

Windows Server 2012 WDS — это серверная роль, которая спроектирована для оказания помощи организациям, использующим доменную службу Active Directory при развертывании систем Windows. Система WDS обычно настраивается для обеспечения служб хранения и извлечения образов, необходимых для их развертывания, клиентских компонентов, таких как образы загрузки PXE, и управляющих компонентов, используемых для

конфигурирования параметров WDS, в том числе добавление образов на сервер WDS и создание мультивещательных передач.

Загрузочные образы

Загрузочный образ содержит клиент Windows Deployment Services и среду Windows PE (Windows Preinstallation Environment — предустановочная среда Windows), которая, по сути, является операционной системой в миниатюре, предназначенной для соединения системы с сервером WDS и предоставления средств для выбора и установки установочною образа WDS.

Загрузочный образ, имеющийся на установочном носителе Windows Server 2012, имеет имя boot.wim и может использоваться для загрузки систем, которые будут устанавливать образы Windows Vista SP1, Windows Server 2008 или более поздние серверные и настольные операционные системы x64. Загрузочный образ Windows Server 2012 может применяться также для установки образов с помощью мультивещательных передач. Если предполагается развертывать образы x86, то по опыту лучше загружать эти системы, используя совместимый загрузочный образ x86 Windows 8 или Windows 10. Это упростит проблему доставки драйверов и ручной их вставки в случае необходимости.

Установочные образы

Установочный образ на самом деле является установочным носителем Windows, который упакован в одном WIM-файле. В зависимости от носителя, используемого для предоставления WIM-файлов, он может содержать множество разных установочных образов.

Например, организации, получающие лицензионный носитель от Microsoft, могут получить DVD-диск Microsoft Windows Server 2012, который содержит вариант полной установки и образы Server Core для редакций Standard и Datacenter. На сервере WDS обычно требуется только один загрузочный образ на платформу x86 или x64, однако он может содержать множество разных установочных образов.

Образы обнаружения

Образ обнаружения создается из загрузочного образа и используется для запуска системы и загрузки среды Windows Preinstallation Environment (Windows PE), а также для нахождения сервера WDS и соединения с ним. Образ обнаружения обычно используется, если сеть или система не поддерживает загрузку PXE. Образы обнаружения могут экспортироваться в файлы ISO, затем записываться или сохраняться на переносимых носителях, таких как CD-диски, DVD-диски или карты памяти USB. В некоторых случаях, когда оборудование не является загрузочным и правильно подключено к серверу WSD, использующему загрузочный образ, образ обнаружения может быть протестирован в качестве альтернативы и развертыванию установочного образа, и захвату системы в образ.

Образы захвата

Образ захвата тоже создается из загрузочного образа, но вместо запуска установки, как у установочного образа, обеспечивает запуск утилиты захвата WDS. Утилита захвата WDS используется для связи с системой, готовой для

создания образа или клонирования, с использованием соответствующих инструментов подготовки системы, с системой WSD для создания нового установочного образа, который позднее можно развернуть на клиентах WDS. Прежде чем применять образ захвата, производится настройка системы с ОС посредством добавления приложений, специальных конфигураций и других изменений в системе, необходимых для определенной организации. Когда система будет готова к созданию образа, она подготавливается с помощью утилиты sysprep (от Microsoft). Эта утилита используется для очистки идентификатора безопасности (SID) компьютера и конфигураций операционной системы, являющихся специфическими для системы, на основе которой будет создан образ. Но зачастую перед запуском sysprep приходится выполнять дополнительные действия, которые обеспечат успешный захват, например, очистку ключей реестра для конкретных приложений, удаление пользовательских профилей и, возможно, удаление самих приложений. Чтобы быть уверенным в сторонних приложениях или даже разработанных Microsoft, просмотрите документацию производителя, обращая особое внимание на создание образов, клонирование и работу с утилитой sysprep.

3.1.6. Набор инструментальных средств Microsoft Deployment Toolkit

Microsoft Deployment Toolkit — единый набор средств и процессов для автоматизации развертывания серверных и настольных систем. В дополнение к уменьшению времени развертывания и стандартизации настольных и серверных образов, MDT упрощает работу со средствами безопасностью и текущими конфигурациями. MDT основывается на базовых средствах развертывания из комплекта средств для развертывания и оценки Windows (Windows ADK) с дополнительным руководством и функциями, которые уменьшают сложность задачи и время, необходимое для развертывания в корпоративной среде. MDT поддерживает развертывание Windows 10, а также Windows 7, Windows 8, Windows 8.1 и Windows Server 2012 R2. Средство также включает поддержку для создания автоматических (ZTI) установок с Microsoft System Center 2012 R2 Configuration Manager.

Набор инструментов Microsoft Deployment Toolkit (MDT) поддерживает три типа развертываний: Zero Touch Installation (ZTI), Lite Touch Installation (LTI) и User Driven Installation (UDI). ZTI — полностью автоматизированная схема развертывания, при которой установка не требует взаимодействия с пользователем. Для развертывания UDI требуется полное ручное вмешательство для ответа на каждое приглашение на установку, например, имя машины, пароль или язык. Для развертывания ZTI и UDI требуются инфраструктура Microsoft System Center. Для развертывания ZTI требуется постоянное сетевое подключение к точке распространения. Для развертывания LTI требуется ограниченное взаимодействие с пользователем. Для развертывания LTI требуется очень небольшая инфраструктура, поэтому его можно установить из общего сетевого ресурса или носителя с помощью USB флеш-накопителя или оптического диска.

3.1.7. Установка операционной системы с помощью System Center Configuration Manager

Развертывание операционной системы с помощью Configuration Manager является частью стандартной инфраструктуры распространения программного обеспечения. Однако имеются дополнительные компоненты. Например, в ходе развертывания операционной системы в Configuration Manager может использоваться роль точки миграции состояния, которая не используется при стандартном развертывании приложения в Configuration Manager.

Точка миграции состояния (SMP). Точка миграции состояния используется для сохранения данных миграции состояния пользователя в ходе сценариев замены компьютера.

Точка распространения (DP). Точка распространения используется для хранения всех пакетов в Configuration Manager, включая пакеты, связанные с развертыванием операционной системы.

Точка обновления программного обеспечения (SUP). Точку обновления программного обеспечения, которая обычно используется для развертывания обновлений на существующие компьютеры, также можно использовать для обновления операционной системы в рамках процесса развертывания. Также можно использовать автономное обслуживание для обновления образа непосредственно на сервере Configuration Manager.

Точка служб отчетов. Точку служб отчетов можно использовать для мониторинга процесса развертывания операционной системы.

Образы загрузки. Образы загрузки представляют собой образы среды предустановки Windows (Windows PE), которые Configuration Manager применяет для запуска развертывания.

Образы операционной системы. Пакет образа операционной системы содержит только один файл — пользовательский образ (.wim). Обычно это образ рабочего развертывания.

Установщики операционной системы. Установщики операционной системы были первоначально добавлены для создания эталонных образов с помощью Configuration Manager. Вместо этого рекомендуется использовать средство Lite Touch из MDT для создания своих эталонных образов. Дополнительные сведения о способе создания эталонного образа см. в разделе Создание эталонного образа Windows 10.

Драйверы. Как и средство Lite Touch из MDT, Configuration Manager также предоставляет репозиторий (каталог) управляемых драйверов устройств.

Последовательности задач. Вид и функции последовательности задач в Configuration Manager очень похожи на последовательности в средстве Lite Touch из MDT и используются для аналогичной цели. Однако в Configuration Manager последовательность задач поставляется клиентам в качестве политики через точку управления (MP). MDT предоставляет дополнительные шаблоны последовательности задач для Configuration Manager.

3.2. Автоматизация установки обновлений операционной системы и приложений

3.2.1. Виды обновлений

Управление обновлениями — это процесс управления развертыванием и обслуживанием промежуточных версий программного обеспечения в производственных средах. Это помогает вам поддерживать эффективность работы, преодолевать уязвимости безопасности и поддерживать стабильность вашей производственной среды. Если ваша организация не может определить и поддерживать известный уровень доверия в своих операционных системах и прикладном программном обеспечении, она может иметь ряд уязвимостей безопасности, которые, если они будут использованы, могут привести к потере доходов и интеллектуальной собственности. Минимизация этой угрозы требует наличия правильно настроенных систем, использования новейшего программного обеспечения и установки рекомендуемых обновлений программного обеспечения.

Существуют следующие типы обновлений.

Пакет обновления (Service Pack). Протестированный накопительный набор исправлений, обновлений для системы безопасности, критических обновлений и обновлений программного обеспечения. Пакеты обновления также могут содержать ограниченное количество изменений функций, выполненных по просьбам пользователей. Пакет обновления представляет новую базовую версию продукта.

Обновление для системы безопасности (Security Update). Общедоступное исправление для устранения уязвимости, связанной с безопасностью, в определенном продукте. Уязвимость, связанная с безопасностью, оценивается по степени серьезности, которая в бюллетене по безопасности (Майкрософт) может принимать следующие значения: критическая, важная, средняя или низкая.

Общее обновление. Общедоступное исправление для решения определенной важной проблемы, не связанной с безопасностью.

Исправление. Одиночный накопительный пакет, который состоит из одного или нескольких файлов, предназначенных для решения проблемы, возникшей в продукте. Исправление предназначено для определенной ситуации, возникшей у пользователя, и может не выйти за пределы организации пользователя.

3.2.2. Роль Windows Server Update Services

Службы обновления Windows Server (WSUS) позволяют администраторам информационных технологий развертывать последние обновления продуктов Microsoft. WSUS предоставляет полное управления распределением обновлений, выпущенных с помощью Центра обновления Майкрософт, на все компьютеры сети.

Сервер WSUS предоставляет функции, которые можно использовать для управления и распространения обновлений через консоль управления. Сервер WSUS также может быть источником обновлений для других серверов WSUS в

организации. Сервер WSUS, который действует как источник обновления, называется восходящим сервером. В реализации WSUS по крайней мере один сервер WSUS в вашей сети должен иметь возможность подключаться к Microsoft Update для получения информации об обновлении. Как администратор вы можете определить — на основе сетевой безопасности и конфигурации — сколько других серверов WSUS напрямую связано с Microsoft Update.

Сервер WSUS может быть интегрирован с System Center Configuration Manager для расширения возможностей управления обновлениями.

Более подробную информацию по управлению обновлениями можно найти на сайте Microsoft.

Управление обновлениями

https://technet.microsoft.com/ru-ru/bb245732

3.3. Использование виртуализации

Виртуализация сервера — это способность одной системы поддерживать несколько сеансов гостевой операционной системы, что позволяет эффективно задействовать вычислительные возможности очень мощного сервера. Всего лишь пару лет назад большинство серверов в центрах данных использовали процессор на 5-10 %, т.е. значительная часть емкости серверов в работе не участвовала. Объединяя возможности нескольких серверов, работающих под управлением операционной системы виртуального сервера-хоста, организации могут эффективнее расходовать вычислительную мощность сервера. И даже при виртуализации серверов организации достигают лишь 40-50% использования, т.е. больше половины серверных мощностей не используется.

Ключом к повышению использования до 70-80% или более является технология виртуализации, которая обеспечит повышенное резервирование, подхват функций, использование мощностей, мониторинг и автоматическое управление. Именно эти возможности имеются в Hyper-V в Windows Server 2012 и более поздних версиях, наряду с еще более улучшенными средствами мониторинга и управления из семейства продуктов System Center. Используя основные технологические усовершенствования в Windows Server 2012 Hyper-V. организации могут спокойно поднимать коэффициент использования серверов до более высоких отметок, заодно задействуя встроенное резервирование на основе подхвата функций и управления мощностью, для получения более эффективно управляемой виртуальной серверной среды.

3.3.1. Обзор технологий виртуализации

Серверная виртуализация

При виртуализации серверов вы можете создавать отдельные виртуальные машины и запускать их одновременно на одном сервере под управлением гипервизора Hyper-V. Эти виртуальные машины являются гостевыми, а компьютер, на котором запущен Hyper-V, — это сервер виртуализации или управляющая операционная система.

Гостевые виртуальные машины функционируют как обычные компьютеры. Когда пользователи могут подключиться к гостевой виртуальной машине удаленно с помощью удаленного рабочего стола (RDC) или удаленного сеанса Windows PowerShell®, вам нужно будет изучить свойства компьютера, на котором пользователь работает, чтобы определить, является ли это виртуальной машиной или традиционно развернутой физической машины. Виртуальные машины, размещенные на одном сервере виртуализации, независимы друг от друга. Вы можете одновременно запускать несколько виртуальных машин, которые используют разные операционные системы на сервере виртуализации, если на сервере виртуализации достаточно ресурсов.

Windows Azure — это облачная платформа, на которой вы можете приобрести вычислительные ресурсы для виртуальных машин, приложений или для таких служб, как базы данных SQL Server на SQL Azure ™. Одним из преимуществ использования Windows Azure является то, что вы платите только за используемые ресурсы, а не фиксированную ставку. Объем облачных ресурсов

эластичен, то есть он может быстро расти или сокращаться по мере необходимости.

Виртуализация рабочих столов

Вы можете использовать **Hyper-V в клиентской операционной системе**. Другими словами, вы можете установить роль Hyper-V на компьютерах под управлением некоторых версий клиентских операционных систем Windows 8, Windows 8.1 и Windows 10. Это позволяет запускать гостевые виртуальной машины на клиентских компьютерах. Hyper-V на клиентских операционных системах имеет дополнительное требование к процессору по сравнению с Hyper-V на серверных системах: компьютер должен иметь 64-хразрядный процессор, поддерживающий преобразование адресов второго уровня (SLAT) и не менее 4 гигабайтов (ГБ) оперативной памяти (ОЗУ).

В **Virtual Desktop Infrastructure (VDI)** клиентские операционные системы размещаются централизованно как виртуальные машины, а клиенты подключаются к этим виртуальным машинам с помощью клиентского программного обеспечения, такого как RDC. Вы можете настроить сервер для поддержки VDI, выбрав установку служб удаленных рабочих столов в Мастере добавления ролей и возможностей. Когда вы настраиваете сервер виртуализации для работы в качестве сервера VDI, вы можете установить роль узла виртуализации удаленных рабочих столов в дополнение к роли Hyper-V.

VDI может упростить управление клиентскими операционными системами:

- обеспечение регулярного резервного копирования для всех клиентских компьютеров, размещенных на одном сервере;
- хостинг виртуальных машин клиента на высокодоступном сервере виртуализации;
- обеспечение доступа пользователей к своей виртуальной машине с помощью других методов RDC при сбое клиентского компьютера.

Виртуализация представления

Эта технология также известна под названием служб терминалов (Terminal Services) или служб удаленного рабочего стола (Remote Desktop Services).

Виртуализация представления отличается от виртуализации настольных систем следующим образом:

- В виртуализации рабочих столов каждому пользователю назначается собственная виртуальная машина, на которой запущена клиентская операционная система. В виртуализации представления пользователи регистрируются и запускают отдельные сеансы на сервере или серверах. Например, пользователи Иван и Игорь могут быть подписаны одновременно на один и тот же сервер удаленных рабочих столов, но при этом работают в разных сеансах с использованием RDC.
- При использовании виртуализации настольных систем приложения работают на виртуальных машинах. С виртуализацией представления рабочий стол и приложения запускаются на сервере виртуализации.

Виртуализация приложений

При виртуализации приложений вы не устанавливаете приложения на клиентских компьютерах постоянно. Вместо этого, когда пользователи хотят использовать приложения, приложения развертываются с сервера на компьютер клиента. В виртуализации приложений Microsoft (App-V) используется клиент Microsoft Application Virtualization Desktop Client, который установлен на клиенте. App-V доступен как часть пакета оптимизации Microsoft Desktop Optimization Pack и не является встроенной ролью или компонентом Windows Server 2012.

Существует три основных преимущества App-V:

- **Изоляция приложений**. App-V изолирует приложение от операционной системы и запускает его в отдельной виртуальной среде. Это означает, что вы можете запускать приложения, которые могут быть несовместимы при совместном использовании на одном компьютере. Например, вы можете использовать App-V для одновременного развертывания и запуска различных версий Microsoft Office Word.
- **Потоковое приложение**. При запуске приложения только те части приложения, которые используются, передаются на клиентский компьютер. Это ускоряет развертывание приложений, поскольку только часть приложения должна передаваться по сети на клиентский компьютер.
- **Портативность приложений**. При развертывании App-V с Microsoft System Center 2012 Configuration Manager пользователи могут использовать одни и те же приложения на нескольких клиентских компьютерах, не требуя традиционной установки на этих клиентских компьютерах. Например, пользователь может зарегистрироваться на чужом компьютере и использовать приложение. Так как это приложение не установлено локально, то, когда пользователь выйдет, приложение больше не будет доступно для других пользователей на этом компьютере.

Виртуализация пользовательского опыта

Так же, как App-V позволяет пользователям получать доступ к своим приложениям с разных клиентских компьютеров, Microsoft User Experience Virtualization (UE-V) позволяет пользователям иметь одинаковые параметры операционной системы и приложений на нескольких устройствах под управлением Windows 7, Windows 8 и Windows 10. Например, пользователь настраивает параметр для приложения, поставляемого через App-V на одном компьютере, настраивая пользовательскую вкладку на ленте в продукте Microsoft Office. Этот параметр доступен автоматически, когда это приложение доставляется через App-V на другой компьютер.

3.3.2. Основные функции Hyper-V

Hyper-V — это роль виртуализации оборудования, доступная в Windows Server 2012. Аппаратная виртуализация обеспечивает уровень гипервизора, который имеет прямой доступ к аппаратным средствам хост-сервера. Операционная система хоста и все виртуальные машины, которые работают на хосте, получают доступ к оборудованию через гипервизор.

Вы можете развернуть Hyper-V на компьютер под управлением Windows Server 2012 с помощью мастера добавления ролей и компонентов, и вы можете настроить Windows Server 2012 как сервер виртуализации с помощью роли Hyper-V. Затем Windows Server 2012 может принимать гостей виртуальной машины, работающих под управлением поддерживаемых операционных систем. Вы можете управлять виртуальными машинами локально через Windows PowerShell, или вы можете управлять ими удаленно через консоль Hyper-V Manager.

Вы можете установить роль Hyper-V в варианте установки Server Core для Windows Server 2012. Также существует бесплатная версия Microsoft Hyper-V Server 2012, которая включает только компоненты, необходимые для размещения виртуальных машин.

Сервер, на котором вы планируете установить роль Hyper-V, должен отвечать следующим требованиям к оборудованию:

- Сервер должен иметь платформу x64, которая поддерживает аппаратную виртуализацию и бит предотвращения выполнения данных (Data Execution Prevention, DEP).
- Сервер должен иметь достаточную мощность процессора для соответствия требованиям гостевых виртуальных машин.

Технология Hyper-V в Windows Server 2012 поддерживает 64 виртуальных процессора и 1 Тбайт ОЗУ на каждую виртуальную машину, содержит встроенную кластеризацию с переключением функций между хостами и может выполнять переключение функций между сайтами очень эффективным образом. Версия Hyper-V в Windows Server 2016 поддерживает также гостевую виртуализацию.

Продукт Hyper-V в Windows Server 2012 также существенно повысил степень доступности хостов и гостевых сеансов Hyper-V по всем направлениям: от прозрачного применения исправлений и обновлений хостов и гостевых сеансов до подхвата (failover) функций между серверами и между сайтами. Конкретнее, интегрированные технологии в Hyper-V по обеспечению высокой доступности включают следующие моменты.

- **Подхват живого переноса (без SAN).** Живой перенос (live migration) представляет собой возможность подхвата гостевого сеанса с одного сервера-хоста Hyper-V на другой, при котором конечные пользователи, подключившиеся к гостевым сеансам, не теряют связи с приложениями. Технология живого переноса появилась еще в Windows Server 2008 R2, но там она требовала наличия SAN как общедоступного хранилища для подхвата гостевых сеансов. Это делало живой перенос дорогостоящим занятием и весьма негибким для небольших предприятий или сайтов больших организаций. После появления Hyper-V в Windows Server 2012 живой перенос гостевых сеансов можно выполнить с помощью обычного файлового сервера Windows Server 2012 в качестве общедоступного хранилища для подхвата кластера.
- **Нулевое время простоя при исправлении или обновлении.** Еще одной трудностью в виртуализации серверов является зависимость от одного сервера-хоста, который управляет несколькими (иногда более десятка) живыми гостевыми сеансами. Если к операционной системе хоста необходимо применить

исправление или обновление, потребуется остановить все виртуальные гостевые сеансы или провести живой перенос

гостевых сеансов на другие серверы. В Windows Server 2012 появилось средство кластерного обновления (Cluster Aware Updates - CAU), которое автоматически обновляет узел кластера (например, узел кластера Hyper-V) без прерывания работы конечных пользователей. Для этого при выполнении исправления выполняется автоматический подхват узла кластера другим узлом.

• **Интегрированная межсайтовая репликация.** Хотя подхват гостевых сеансов в Hyper·V поддерживался еще в версии Windows Server 2008, возможность подхвата гостевых сеансов между сайтами была больше номинальной. В Windows Server 2012 Hyper-V появилась технология под названием Hyper-V Replica (Реплика Hyper-V), которая реплицирует данные виртуального гостевого сеанса между сайтами, чтобы в случае отказа сайта можно было перевести в оперативный режим другой сайт с реплицированными копиями систем гостевого сеанса.

• **Встроенное объединение NIC.** Объединение NIC (NIC teaming) представляет собой возможность работы нескольких сетевых адаптеров в системе сервера-хоста с разделением нагрузки сетевых коммуникаций. Эта возможность не нова, т.к. поставщики оборудования вроде Hewlett-Packard, Dell и IBM предоставляли драйверы для поддержки объединений NIC. Однако в Windows Server 2012 эта технология встроена в операционную систему. Теперь можно сконфигурировать агрегирование сетевых адаптеров (NIC) или разделение NIC на хосте Hyper-V, чтобы обеспечить производительность и резервирование, а сервер-хост Hyper-V может подхватывать функции другого сервера-хоста, и при этом Windows Server 2012 Hyper-V распознает сетевые возможности для поддержки подхвата. Уже не нужны обращения к поставщикам драйверов, поскольку все необходимые функции встроены в Windows Server 2012.

Основой для консолидации виртуальных гостевых сеансов на ограниченном количестве физических серверов-хостов является возможность более легкого управления и поддержки гостевых сеансов. Без управляемости серверы начнут "неконтролируемо размножаться", и постепенно в организации возникнет ситуация, когда серверов гораздо больше, чем нужно, нет легкого способа управления или администрирования, а на управление гостевыми сеансами уходит больше времени, чем на обычные физические серверы.

Поэтому настолько важна возможность более легкого управления и сопровождения систем (физических и виртуальных). Ниже перечислены основные усовершенствования в этой области.

• **Консоль диспетчера серверов.** Диспетчер серверов (Server Manager) Windows Server 2012 представляет собой централизованную консоль управления серверами, которая позволяет администраторам наглядно видеть, группировать и администрировать системы - как физические, так и виртуальные. Все это позволяет легко конфигурировать и обновлять одновременно сразу несколько систем. В отличие от других технологий виртуальных серверов, которые ориентированы просто на возможность создания все большего количества

виртуальных гостевых сеансов, Windows Server 2012 с Hyper-V предоставляет не только лучший способ запуска гостевых сеансов, но и управления ими.

• **Мобильность IP-адресов.** Во время перехвата функций одним центром данных с другого одной из самых больших сложностей является необходимость изменять IP-адреса в соответствии с подсетью и конфигурацией сетевых ресурсов после завершения подхвата. Windows Server 2012 позволяет сделать IP-адреса, в том числе и адреса, сгенерированные DHCP, переносимыми между сайтами. Во время подхвата таблицы адресов автоматически обновляются, и все сгенерированные IP-адреса остаются доступными в резервированном центре данных для немедленного продолжения работы и без необходимости переадресации систем в работающем центре данных с привлечением IT-персонала.

• **Шифрование BitLocker на хостах и гостевых серверах.** Поскольку виртуальные гостевые сеансы встречаются практически в любом месте вычислительных сетей предприятия, даже в небольтих и удаленных центрах, необходимость защиты хостов и гостевых сеансов становится критичной для безопасности предприятия. ОС Windows Server 2012 поддерживает шифрование BitLocker как на хостах, так и в гостевых сеансах, с возможностью шифрования локальных дисковых хранилищ, шифрования дисков в отказоустойчивых кластерах и шифрования общедоступных томов кластеров. Это помогает повысить защиту хостов и гостей Hyper-V.

3.3.3. Виртуальные жесткие диски

Виртуальные жесткие диски (virtual hard disk — VHD) используются виртуальными машинами для эмуляции дисков Windows. Виртуальные жесткие диски могут бьгть созданы в существующей системе Windows Server 2012 посредством консоли управления Hyper-V или же созданы непосредственно с помощью консоли Disk Management (Управление дисками).

В основном диски VHD создаются на хост-системе Windows в виде файла с расширением .vhd на существующем томе Windows. Диски VHD могут быть созданы с фиксированным размером либо динамически расширяемыми. VHD фиксированного размера в 10 Гбайт будет эквивалентен файлу в 10 Гбайт на томе хоста Windows. Файлы VHD могут легко перемещаться между серверами и между виртуальными машинами, а также довольно легко расширяться, при условии, что в этот момент VHD не используется и есть достаточно свободного пространства на томе хоста. Файлы VHD могут присоединяться непосредственно к хосту Windows Server 2012 с помощью консоли Disk Management, в отличие от предыдущих выпусков, где требовались сценарии для монтирования файла. Эта дополнительная функциональность является усовершенствованием интегрированной функциональности резервного копирования VSS Hyper-V, входящей в Windows Server Backup и доступной для независимых поставщиков средств резервного копирования.

Виртуальные жесткие диски формата VHDX в Windows Server 2012

В Windows Server 2012 появился новый формат виртуальных жестких дисков — VHDX. Старый формат VHD имеет ограничение 2 Тбайт, а новые файлы формата

VHDX могут иметь размер до 64 Тбайт, и они лучше защищены от порчи данных с помощью журнала изменения данных, который ведется в самом файле.

Диск фиксированного объема

Диски VHD можно создавать фиксированного объема или с динамическим расширением. VHD-диск фиксированного объема 10 Гбайт эквивалентен файлу в 10 Гбайт на томе хоста Windows. При использовании нового формата VHDX реальный размер фиксированного диска может быть даже меньше, хотя и ненамного. Виртуальные диски фиксированного объема следует использовать в первую очередь для повышения производительности виртуальных гостевых сеансов и систем хост-партнер в производственных развертываниях серверов. Основное преимущество фиксированных дисков в отношении производительности в том, что реальный файл не становится со временем фрагментированным, если диск совместно использует память того же самого тома хоста-партнера.

Динамически расширяемые диски

Динамически расширяемые виртуальные диски настраиваются на максимальный объем, но занимают в системе хоста лишь конкретно необходимое место. Например, если динамически расширяемый виртуальный диск на 25 Гбайт создан на хосте и добавлен в виртуальную гостевую систему Hyper-V, то гостевая система увидит доступных 25 Гбайт дисковой памяти. Однако файл для этого диска в хостовой системе будет иметь лишь размер, необходимый для размещения данных. Такие диски удобнее всего для тестовых машин и машин, которым не требуется максимальная производительность. Впрочем, в последних реализациях Hyper-V использование динамически расширяемых виртуальных дисков практически не влияет на производительность.

Разностные диски

В гостевых системах Hyper-V можно создавать диски с родительско-дочерним отношением. Родительский диск создается с базовой конфигурацией, а после этого для него могут создаваться один или несколько дочерних дисков, связанных с ним. Разностные диски (differencing disk) используются для изоляции изменений в гостевой системе: изменения хранятся на таком диске, в то время как родительский диск остается неизменным. Разностные диски можно также использовать для создания снимков гостевых систем Hyper-V.

3.4. Принципы построения высокодоступных и отказоустойчивых информационных систем

3.4.1. Понятие высокой доступности

Высокая доступность (англ. high availability) — характеристика технической системы, разработанной для предотвращения незапланированного обслуживания путём уменьшения или управления сбоями и минимизацией времени плановых простоев.

Высокую доступность можно определить как свойство системы быть защищённой и легко восстанавливаемой от небольших простоев в короткое время и автоматизированными средствами. При таком определении рассматриваются три фактора: категоризация возможных проблем (сбоев), категоризация требований к системе в отношении продолжительности перерывов в работе, технологические решения для автоматической защиты и восстановления после сбоев.

При определении высокой доступности между заказчиком и поставщиком услуги оговаривается максимально допустимое время простоя компьютерной системы, так как от желаемого уровня доступности зависит стоимость реализации и эксплуатации системы. Для этого составляется и подписывается соглашение об уровне предоставления услуги — SLA.

Соглашение об уровне предоставления услуги (англ. Service Level Agreement, SLA) — термин методологии ITIL, обозначающий формальный договор между заказчиком (и в рекомендациях ITIL заказчик и потребитель — разные понятия) услуги и её поставщиком, содержащий описание услуги, права и обязанности сторон и, самое главное, согласованный уровень качества предоставления данной услуги.

SLA используется внутри организации для регулирования взаимоотношений между подразделениями, а также является основным инструментом непрерывной оценки и управления качеством предоставления услуг аутсорсинга специализированной организацией — аутсорсером.

Как правило термин SLA используется применительно к ИТ и телекоммуникационным услугам. В таком соглашении может содержаться детальное описание предоставляемого сервиса, в том числе перечень параметров качества, методов и средств их контроля, времени отклика поставщика на запрос от потребителя, а также штрафные санкции за нарушение этого соглашения. Для того, чтобы соблюсти SLA, поставщик услуг в свою очередь заключает операционное соглашение об уровне услуг (OLA, operational-level agreement) с другими внутренними подразделениями, от которых зависит качество предоставления услуг.

Параметры качества услуги, указанные в SLA, должны быть измеримыми, то есть представимыми в виде числовых метрик. Например, для услуги доступа в Интернет это может быть максимальное время недоступности, максимальное суммарное время недоступности за период (например, за месяц). Скорость доступа при этом является плохим параметром, поскольку зависит не только от оператора, но и от других операторов, от загруженности сервера сайта и т. п., на что, как правило, поставщик повлиять не может.

Часто в SLA определяется период, за который поставщик услуги предоставляет заказчику отчёт об измеренных параметрах качества.

Количественное определение доступности

Процентный метод

Для вычисления достигнутого уровня доступности необходимо знать время простоя (П) и время обещанной доступности (Д), в случае высокой доступности в это время не включается суммарное время запланированных простоев. Тогда уровень доступности можно получить по формуле[6]:

```
доступность = (Д — П) / Д × 100 %
```

Например, простой системы постоянной доступности в течение 45 минут в январе говорит об уровне доступности 99,9 % («три девятки»).

Доступность можно выразить в виде средних величин[7]:

```
средняя доступность = MTTF / (MTTF + MTTR) × 100 %,
```

где MTTF (англ. mean time to failure) — средняя наработка до отказа, MTTR (англ. mean time to repair) — среднее время до восстановления работоспособности.

Время восстановления после сбоя зависит от многих факторов, таких как сложность системы (чем сложнее система, тем дольше её перезапуск), серьёзность проблемы, доступность обслуживающего персонала, запасного оборудования, недостаточного резервного копирования и т. п. Следует также отметить, что доступность системы измеряется с точки зрения пользователя, а не фиксации факта работы основных узлов.

Наработка на отказ

Другой метрикой доступности, применяемой в отношении больших сетей и составляющих их устройств, является метод, в котором считается число отказов на миллион (DPM, англ. defects per million) часов работы. Этот метод точнее, чем процентный, позволяет принимать во внимание сбои в работе части сети. В этом случае можно измерять часы безотказной работы сети в целом, суммарное время работы всех устройств или даже суммарное время работы пользователей.

3.4.2. Отказоустойчивые кластеры

В Windows Server 2012 предлагаются две технологии кластеризации, которые доступны во всех редакциях. **Кластеризация** — это группирование независимых серверных узлов, позволяющее получать доступ к этим серверам и просматривать их в сети так, будто бы они являются единой системой. Когда служба и/или приложение запускается из кластера, запросы подключающегося к нему пользователя могут обрабатываться как только одним конкретным узлом, так и несколькими разными узлами кластера. В случае данных, доступных только для чтения, клиент может делать запрос к какому-то одному серверу в кластере, а его следующий запрос - направляться уже к другому серверу, причем так, что клиент об этом может даже и не догадываться. Кроме того, если один из узлов в кластере с несколькими узлами выйдет из строя, остальные узлы будут продолжать обслуживать клиентские запросы, и в зависимости от кластеризированной службы или приложении клиент может даже не заметить прерывания в обслуживании.

Первой технологией кластеризации, которая поставляется с Windows Server 2012, являются **отказоустойчивые кластеры**. Отказоустойчивая кластеризация (Failover Clustering) обеспечивает устойчивость к отказам на уровне системы с помощью процесса, называемого подхватом функций. Когда какая-нибудь система или узел в кластере выходит из строя или перестает отвечать на запросы клиентов, кластеризированные службы или приложения, которые функционировали на этом конкретном узле, переводятся в автономный режим и перемещаются на другой узел, где снова делаются функциональными и полностью доступными. Службы могут переводиться в автономный режим потому, что некоторые из них способны использовать современные возможности подхвата кластерных функций, которые распределяют память и клиентские сеансы между узлами, для прозрачного перемещения службы с узла на узел кластера. Правда, в большинстве развертываний клиенты могут заметить небольшую паузу в обслуживании, или им даже потребуется переподключение к службе после завершения подхвата. В большинстве реализаций отказоустойчивые кластеры требуют доступа к общему хранилищу данных и больше всего подходят (но не ограничиваются) для развертывания перечисленных ниже ролей.

• **Файловые серверы.** Файловые службы, развернутые в отказоустойчивых кластерах, предоставляют почти все функциональные возможности, которые может предоставлять автономная система Windows Server 2012, но только при развертывании в виде кластеризированных файловых служб они позволяют создавать единый репозиторий хранилищ данных и делать так, чтобы клиенты могли получать к нему доступ через назначенный и доступный в текущий момент узел без репликации данных файлов.

• **Серверы печати.** Службы печати, развертываемые в отказоустойчивых кластерах, обладают одним главным преимуществом по сравнению с автономным сервером печати: в случае выхода активного сервера печати из строя каждый из общих принтеров делается доступным для клиентов с тем же именем сервера печати. Хотя развертывание и замена принтеров для компьютеров и пользователей легко осуществляется с помощью групповых политик, последствия выхода из строя автономных серверов печати могут оказаться огромными.

• **Серверы баз данных.** При развертывании в крупных организациях критических приложений, требующих наличия сервера баз данных, предпочтительным методом является развертывание служб баз данных в отказоустойчивых кластерах. Во многих случаях установка и конфигурирование производственного сервера баз данных может занимать несколько часов, а сами базы данных могут иметь значительные размеры, так что развертывание серверов баз данных на автономных системах и их воссоздание в случае отказа одного сервера может потребовать нескольких часов, а то и дней. Это еще одна причина создания база данных на отказоустойчивых кластерах.

• **Централизованные производственные системы обмена сообщениями.** По многим таким же причинами, что перечислялись выше для служб баз данных, службы обмена сообщениями стали играть во многих организациях критически важную роль и потому тоже больше всего подходят для

развертывания в отказоустойчивых кластерах. Последние версии Microsoft Exchange хоть и опираются в своей работе на отказоустойчивые кластерные службы, но использует собственные механизмы высокой доступности.

• **Виртуальные машины Hyper-V.** По мере движения многих организаций в сторону консолидации серверов и превращения физических серверов в виртуальные, обеспечение средств поддержки высокой доступности и надежности становится еще более важным, когда на единственном физическом хосте Hyper-V выполняется несколько критических виртуальных машин. Windows Server 2012 Hyper-V и отказоустойчивые кластеры содержат несколько новых возможностей, которые делают Hyper-V еще более устойчивой к единичным системным ошибкам.

Ниже перечислены некоторые основные термины, ассоциируемые с технологиями кластеризации Windows Server 2012.

• **Кластер (cluster).** Кластер — это группа независимых серверов (узлов), позволяющая получать доступ к входящим в нее серверам и представлять их в сети так, будто бы они являются единой системой.

• **Узел (node).** Узел — это отдельный сервер, который является членом кластера.

• **Кластерный ресурс (cluster resource).** Кластерный ресурс — это служба, приложение, IP-адрес, диск или сетевое имя, которое определяется и управляется с помощью кластера. Внутри самого кластера кластерные ресурсы объединяются и управляются вместе за счет использования групп кластерных ресурсов, которые теперь называются группами ролей.

• **Группа ролей (role group).** Кластерные ресурсы, содержащиеся внутри кластера в виде логического набора, теперь называются группами ролей, хотя часто употребляется и название "кластер группы служб и приложений". Эти группы представляют собой своего рода единицы подхвата функций в кластере. В случае выхода одного кластерного ресурса из строя и невозможности осуществить его автоматический перезапуск, группа ролей, частью которой является данный ресурс, будет переведена в автономный режим, перемещена на другой узел в кластере, а затем снова возвращена в оперативный режим.

• **Точка клиентского доступа (Client Access Point).** Точка клиентского доступа – это термин, который применяется в отказоустойчивых кластерах Windows Server 2012 и подразумевает под собой комбинацию, состоящую из сетевого имени и ассоциируемого с ним IP-адреса. По умолчанию при добавлении новой группы ролей точка клиентского доступа создается с именем и адресом IPv4. Стандарт IPv6 тоже поддерживается в отказоустойчивых кластерах, но требует либо добавления ресурса IPv6 в какую-то существующую группу, либо создания отдельной общей группы ролей и добавления всех необходимых ресурсов и их зависимостей в нее.

• **Виртуальный сервер кластера (virtual cluster server).** Виртуальным сервером кластера называется такая группа ролей, в которой содержится ресурс точки клиентского доступа, ресурс диска и хотя бы еще один дополнительный ресурс роли. Доступ к ресурсам виртуального сервера кластера осуществляется либо с помощью имени DNS, либо с помощью имени NetBIOS со ссылкой на адрес

1Pv4 или IPvб. Имя и IP-адрес остаются одинаковыми, независимо от того, на каком именно узле кластера функционирует виртуальный сервер.

• **Активный узел (active node).** Активным узлом называется такой узел в кластере, на котором в текущий момент функционирует хотя бы одна группа ролей. Группа ролей может быть активной только на одном узле в каждый момент времени и потому все остальные узлы, на которых она также может находиться, считаются по отношению конкретно к ней пассивными.

• **Пассивный узел (passive node).** Пассивным узлом в кластере называется тот узел, на котором в текущий момент не функционируют никакие группы ролей.

• **Кластер типа "активный-пассивный".** Кластер типа "активный-пассивный" — это такой кластер, в котором имеется хотя быть один узел с функционирующей группой ролей, и несколько дополнительных узлов, которые также могут обслуживать эту группу, но пока что находятся в состоянии ожидания. Такая конфигурация является типичной в случаях, когда в отказоустойчивом кластере развертывается только одна единственная группа ролей.

• **Кластер типа "активный-активный".** Кластер типа "активный-активный" — это такой кластер, в котором на каждом узле активно обслуживается или функционирует хотя бы одна группа ролей. Такая конфигурация является типичной в случаях, когда в одном отказоустойчивом кластере развертывается множество групп ролей для обеспечения максимального использования серверных или системных ресурсов. Ее недостаток состоит в том, что в случае выхода одной активной системы из строя оставшейся системе или системам нужно обслуживать все группы и предоставлять доступ к службам ролей в кластере всем необходимым клиентам.

• **Сигнал активности кластера (cluster heartbeat).** Сигнал активности кластера — это термин, который применяется для описания сообщений, пересылаемых между отдельными узлами кластера и используемых для определения их состояния. Обмен сигналами активности может осуществляться как по отдельной сети, так по той же самой, что и обмен данными с клиентами. Из-за такого взаимодействия между узлами администраторы, отвечающие за создание сетей и программное обеспечение для их мониторинга, должны обязательно заранее предупреждаться о количестве подобных сетевых сообщений между узлами кластера. Объем трафика, генерируемый во время обмена сигналами об активности, большим не является, исходя из размера передаваемых данных, но анализ частоты его пересылки может потребовать включения мониторинга уведомлений.

• **Кворум кластера (cluster quorum).** Кворум кластера отвечает за отличительные конфигурационные данные кластера и текущее состояние каждого узла, каждой группы ролей, каждого ресурса и сети в кластере. Более того, при считывании данных кворума каждый узел определяет на основании извлекаемой информации то, должен ли он остаться доступным, завершить работу кластера или активизировать конкретные группы ролей на локальном узле. Чтобы стало еще понятнее, следует отметить, что существуют четыре разных модели кворума. Тип кворума, применяемый в кластере, определяет и

тип самого кластера. Например, кластер, в котором используется модель кворума Node and Disk Majority (Большинство узлов и дисков) может называться кластером с большинством узлов и дисков.

- **Кластерный диск-свидетель (cluster witness disk)** или **общий файловый ресурс (file share)**. Кластерный диск-свидетель или общий файловый ресурс-свидетель применяются для хранения информации о конфигурации кластера и оказания помощи с определением состояния кластера в случае невозможности установки связи с каким-то или со всеми узлами кластера.

3.4.3. Кластеры с балансировкой нагрузки

Вторая предлагаемая в Windows Server 2012 технология кластеризации называется технологией **балансировки сетевой нагрузки** (Network Load Balancing — NLB). Эта технология больше всего подходит для обеспечения отказоустойчивости для клиентских веб-приложений и веб-сайтов, серверных систем Remote Desktop Services Session Host, серверов VPN и прокси-серверов. Она обеспечивает отказоустойчивость за счет того, что вынуждает каждый сервер в кластере индивидуально запускать сетевые службы и приложения и тем самым исключает вероятность появления одиночных точек отказа. В зависимости от конкретных потребностей развертываемой в кластере NLB службы или приложения, для указания того, как клиенты будут подключаться к вспомогательным узлам кластера NLB, могут настраиваться различные параметры конфигурации и сходства. Например, в случае доступного только для чтения веб-сайта запросы клиентов могут направляться любому из узлов кластера NLB, из-за чего, следовательно, даже во время одного посещения этого веб-сайта клиент сможет подключаться к разным узлам кластера NLB. Другим примерам может служить защита веб-сайта с помощью шифрования SSL (Secure Sockets Layer — протокол защищенных сокетов): клиентский сеанс должен быть инициирован и обслужен одним узлом кластера, т.к. конкретный сеанс может содержать данные именно этого сеанса.

3.5. Семейство продуктов System Center

Семейство продуктов Microsoft System Center предоставляет новый подход к гибридному облаку. Современная платформа продуктов и услуг помогает организациям преобразовывать свою текущую инфраструктуру в высоко-эластичную, масштабируемую и надежную облачную инфраструктуру, позволяет быстро и гибко создавать и управлять современными приложениями на всех платформах и устройствах. Microsoft однозначно предоставляет последователь-ный и полный набор облачных возможностей для корпоративных частных, гибридных и общедоступных облаков, таких как Windows Server 2016 и System Center 2016, Windows Azure или общедоступные облачные предложения от поставщиков услуг, использующих Microsoft Azure Stack.

Microsoft System Center 2016 обеспечивает единое управление ресурсами в корпоративном центре обработки данных и у облачных провайдеров, в том числе в Windows Azure. Он включает в себя критические аспекты управления инфраструктурой и DevOps для предоставления ресурсов, настройки, мониторинга, автоматизации, управления услугами, защиты конечных точек, а также резервного копирования и восстановления. Благодаря постоянному и унифицированному управлению System Center 2016 помогает сделать ваш центр обработки данных современным.

System Center 2016, расширенный с помощью Microsoft Operations Management Suite (OMS), раскрывает новые возможности управления, чтобы обеспечить возможность управления гибридами в любом центре данных или облаке. System Center позволяет ИТ-команде управлять практически любой инфраструктурной платформой, в том числе локальными облаками, облачными Web-сервисами Azure и Amazon Web Services (AWS), а также поддерживает работу на Windows Server, Linux, VMware или OpenStack.

В состав пакета входят следующие продукты:

- System Center Configuration Manager
- System Center Operation Manager
- System Center Virtual Machine Manager
- System Center Data Protection Manager
- System Center Orchestrator
- System Center Service Manager
- System Center Application Controller
- System Center Endpoint Protector