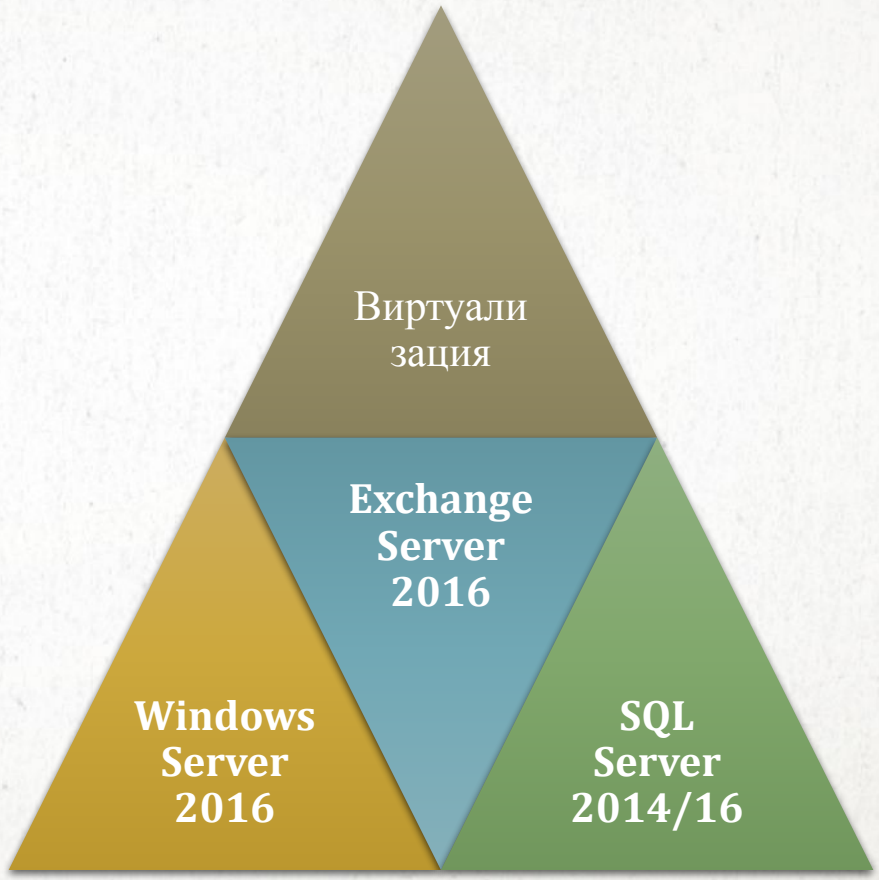
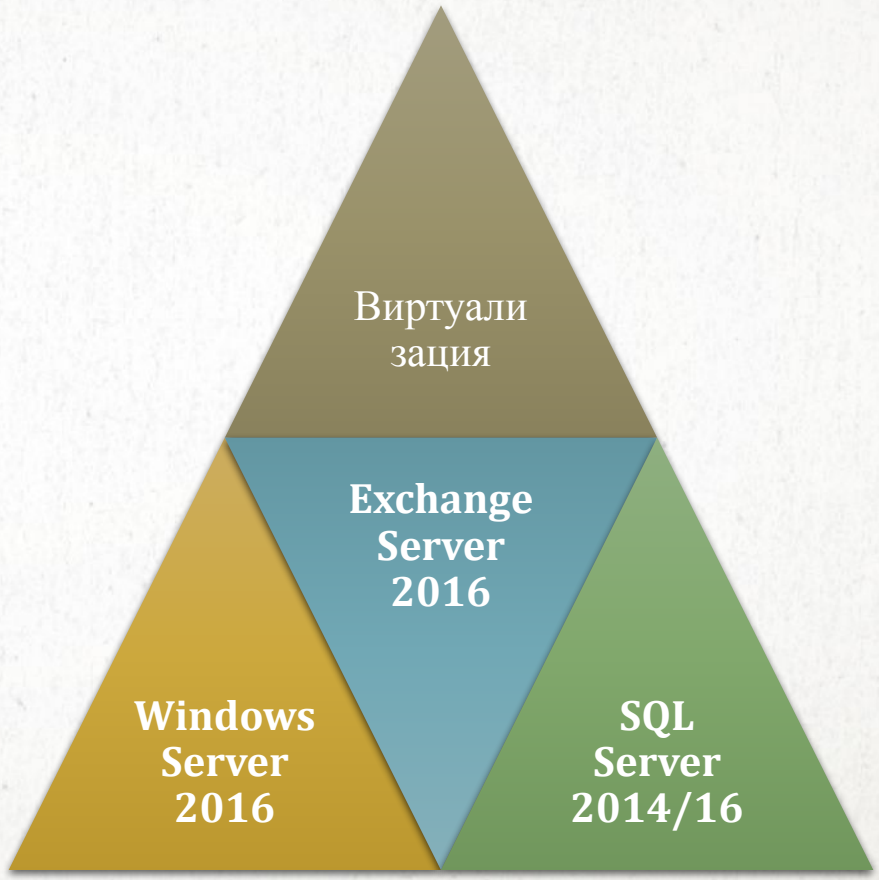
АРХИТЕКТУРНЫЙ ДИЗАЙН

IT ИНФРАСТРУКТУРЫ КОМПАНИИ

- **Windows Server 2016**
  - Стирая границы между облачной и локальной IT-инфраструктурой
  - Контейнеры – «карманные линкоры» виртуализации
  - Управляемая безопасная сеть, доступная везде
  - Хранилища – упрощение и доступность
- **SQL Server**
  - In-Memory OLTP
  - Усовершенствования в AlwaysOn
  - Расширение буферного пула
  - Обновляемые колоночные индексы



- **Exchange Server 2016**
  - Архитектура
  - Установка
  - Хранилище
  - Высокая доступность
  - Управление
  - Дополнительные функции
- **Виртуализация**



- Примерно каждые 7-8 лет Microsoft выпускает принципиально новую версию Windows Server.
- Новую – с точки зрения задач и подходов, которые будет решать данный сервер.
- *Меняются реалии бизнеса, меняется структура сервисов, которые должны предоставляться для бизнеса – и меняются концепции, которые заложены в Windows Server.*

Windows Server 2016

Стирая границы между облачной и локальной IT-инфраструктурой

- Так было при переходе от Windows NT Server и поколению Windows Server 2000/2003 – *от базовых служб инфраструктуры к полному стеку сетевых служб, служб управления рабочими местами и аутентификацией.*
- Так было далее при переходе от Windows Server 2003 к Windows Server 2008/2012 – *концепция виртуализации и платформа для построения виртуализированных центров обработки данных (ЦОД).*

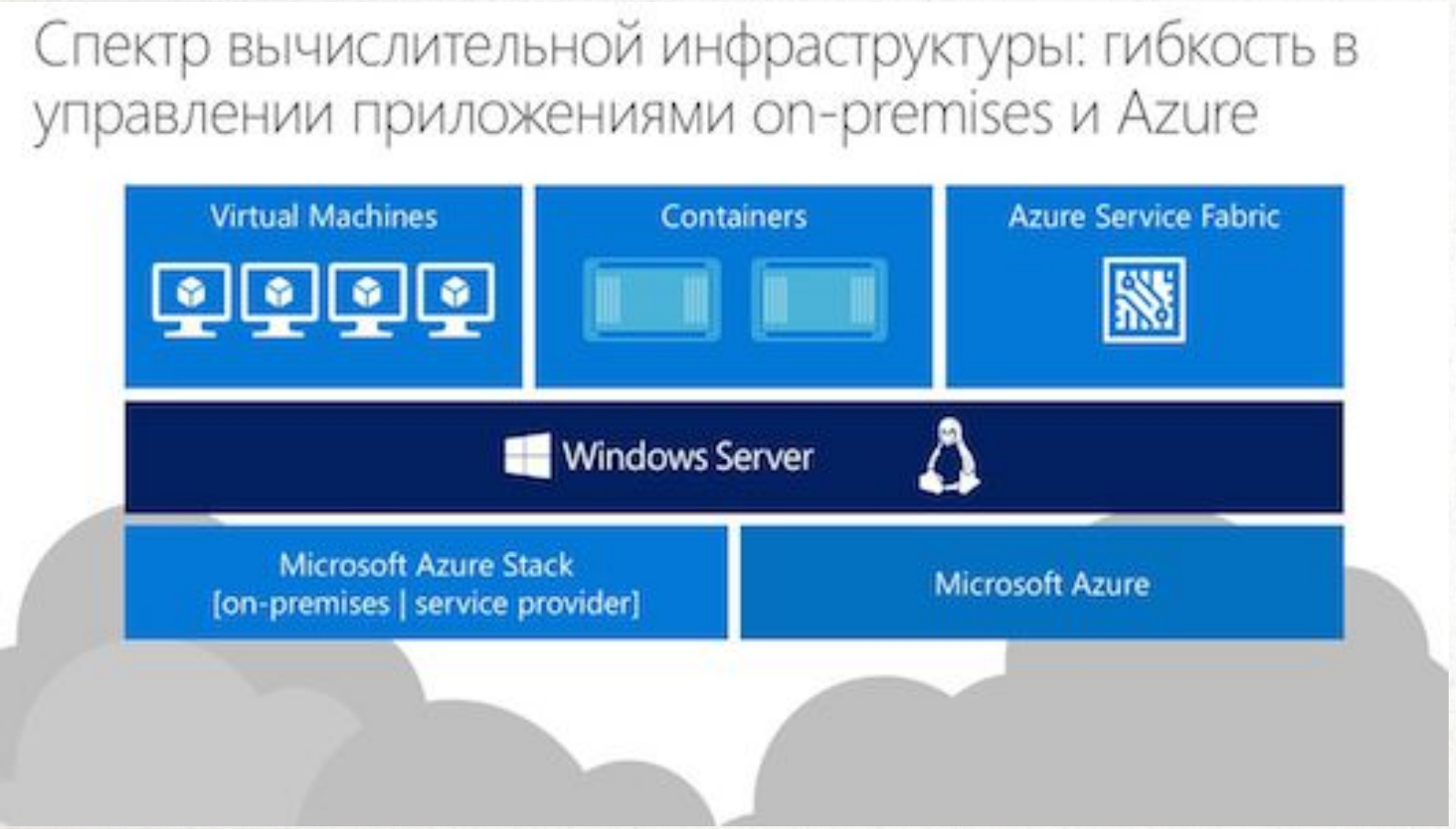
Windows Server 2016

стирая границы между облачной и локальной IT-инфраструктурой

- Windows Server 2016 представляет собой **измененное видение Microsoft на утилизацию ресурсов приложениями, облачные технологии и их взаимодействие с локальной ИТ-инфраструктурой.**
- **При таком подходе в организациях будут стираться границы между облачной и локальной ИТ-инфраструктурой**, а перенос бизнес приложение или использование ими ресурсов облака или локальных ресурсов – не будет требовать переработки кода, переконфигурирования или дополнительной настройки ИТ-инфраструктуры.

Windows Server 2016

стирая границы между облачной и локальной IT-инфраструктурой



Windows Server 2016

стирая границы между облачной и локальной IT-инфраструктурой

- **Более высокая плотность запуска** изолированных друг от друга приложений на одной аппаратной платформе, нежели использование «настоящей» виртуализации, когда в каждой виртуальной машине стартует ядро ОС, которое должно обеспечить работу приложения.

- **Скорость развертывания даже сложных приложений.** На физический или виртуальный родительский хост с развернутой службой контейнеров достаточно просто скопировать образ контейнера с файлами требуемого приложения и всеми «довесками» в виде ветвей реестра и служб. И все – родительский хост не требует дополнительной настройки, все библиотеки, параметры, файлы – уже в образе контейнера. Контейнер просто запускается администратором и приложение в контейнере начинает предоставлять требуемые услуги в организации (или клиентам).

Windows Server 2016

Контейнеры – «карманные линкоры» виртуализации

- **Совместимость со средой, предыдущими версиями приложения и т.п.** Поскольку контейнер и представляет из себя «все в одном флаконе» и работает изолированно – то работоспособность нового контейнера зависит только от правильности предварительной сборки его образа и никак не связана с тем, что уже «живет» на родительском хосте – будь это трижды несовместимые приложения или библиотеки – они либо в других контейнерах и вообще не видятся «нашим» приложением, либо они на сервере, но их файлы и настройки подменяются теми библиотеками и службами, что идут вместе с контейнером.

- **Мгновенная бесшовная переносимость** приложений из локальной среды исполнения в облачную среду Microsoft Azure и обратно.

- **Пример использования** -- быстро заменить рабочую («продакшен») версию приложения на новую и, при возникновении проблем – быстро вернуться к предыдущей, когда на хосте, где размещается приложение, могут быть другие, несовместимые приложения или предыдущие несовместимые версии библиотек, требующиеся для работы.

Windows Server 2016

Контейнеры – «карманные линкоры» виртуализации

- **Windows Server 2016 предоставляет все необходимые инструменты по управлению работой контейнеров,** созданию и добавлению новых образов в репозитарий, делегированию прав на управление контейнеры. Базовым средством управления контейнерами в Windows Server 2016 является командная строка PowerShell, в которой реализован соответствующий модуль.

- **Для управления контейнерами в Windows Server 2016 реализовано docker-совместимое API**, что позволяет использовать наработки на docker для запуска и управления контейнерами в среде Windows. При этом контейнеры и репозитарии PowerShell и Docker существуют отдельно и независимо друг от друга.

- **Служба «контейнеризации» может быть запущена как на физическом сервере, так и внутри виртуальной машины** под управлением Windows Server 2016, которая выполняется на родительском хосте также под управлением Windows Server 2016 (обязательное условие, поскольку требуется работа вложенной/наследуемой виртуализации).

Windows Server 2016

Контейнеры – «карманные линкоры» виртуализации

- **Концепция виртуальной сети расширена** и теперь она применяется не только к трафику виртуальных машин, а к любому трафику. Также поддерживается не только протокол инкапсуляции NVGRE, но и VXLAN. Центром управления сети стал виртуальный программируемый коммутатор, через который проходят все пакеты, будь то ОС физического сервера и его приложения или пакеты виртуальных машин и контейнеров на данном хосте.

- **Window Server 2016 получает централизованные политики виртуальных сетей** (с использованием открытого протокола управления Open vSwitch Database Management Protocol), которые позволяют администраторам описывать границы тех или иных виртуальных сетей, к которым могут принадлежать разные виртуальные машины и приложения на данном сервере, политики ограничения доступа на уровне виртуального коммутатора, политики пересылки трафика и политики балансировки нагрузки.

Windows Server 2016

Управляемая безопасная сеть, доступная везде

- **Пример использования --** решение извечную проблему безопасности, когда администраторы приложений пренебрегают базовыми требованиями сетевой безопасности, например, полностью отключая или не настраивая должным образом межсетевые экраны в тех виртуальных машинах/контейнерах, в которых работают их приложения.

- Политики виртуальных сетей **обеспечивают инструменты настройки правил сетевого доступа на каждом виртуальном коммутаторе**, гранулярно применяя их к отдельным сетям, виртуальным машинам/контейнерам или сетевым интерфейсам, которые подключены к данному коммутатору.

- Политики позволяют администраторам инфраструктуры **принудительно ограничивать сетевой доступ к тому или иному экземпляру приложения/виртуальной машины**, даже если собственный администратор не озаботился настройкой безопасности..

Windows Server 2016

Управляемая безопасная сеть, доступная везде

- Пересылка сетевого трафика на требуемый узел перед доставкой получателю.

- **Пример использования --** сервер антивирусной защиты, который «просеивает» все, что поступает извне (или средства журналирования/кеширования определенных протоколов), даже если в конкретной виртуальной сети не предусмотрено подобной службы.

- **Построение решений Software Load Balancing (SLB),** когда балансировка сетевой нагрузки и запросов для того или иного приложения/группы виртуальных машин выполняется также на уровне виртуальных коммутаторов, а не службами балансировки нагрузки, которые необходимо установить и настроить в каждом экземпляре приложения/виртуальной машины. Таким образом и особенно с учетом гибкости развертывания приложений в контейнерах, скорость наращивания производительности приложений, которые могут масштабироваться путем балансировки нагрузки – существенно возрастает.

Windows Server 2016

Управляемая безопасная сеть, доступная везде

- **Storage Replica** – позволяет планировать отказоустойчивые инфраструктуры, реплицируя средствами Windows Server 2016 (без специальных требований к аппаратной репликации со дисковых подсистем) данные между дисками отдельных серверов, общими дисками разных кластеров и, что самое главное, реплицируя общие диски одного кластера на георасределенные хранилища

- Первые два сценария позволяют компаниям обеспечить доступность данных при выходе из строя или переносе служб с одного сервера/кластера на другой, а последний сценарий позволяет создавать георасределенные кластеры с высокодоступными приложениями на них.

Windows Server 2016

Хранилища – упрощение и доступность

- Storage Space Direct-- позволяет формировать кластеры хранения, даже не имея общих аппаратных дисковых массивов, а используя в качестве общего массива дисков локальные диски каждого из серверов-участников кластера.

- позволяет полностью отказаться от ресурсозатратных аппаратных решений типа сетей хранения данных, используя в качестве аппаратного обеспечения кластеров-хранилищ только стандартные серверы с подключенными к ним на прямую дисками и такие же стандартные сети передачи данных Ethernet.

- позволяет быстро наращивать ка объемы дискового массива путем добавления локальных дисков в серверы, так и производительность кластера-хранилища, добавляя новые серверы-узлы (и при этом наращивая и доступный объем за счет их локальных дисков) без больших капитальных затрат в сети хранения данных.

Windows Server 2016

Хранилища – упрощение и доступность

ПЕРВАЯ ДЕСЯТКА НОВШЕСТВ В SQL SERVER 2014

IN-MEMORY OLTP

- В SQL Server 2014 стала возможной оптимизация выбранных таблиц и хранимых процедур для загрузки в память. Технология In-Memory OLTP, которая создавалась с расчетом на высокий параллелизм операций, использует новый механизм оптимистического параллельного управления для устранения задержек из-за блокировок. По заявлению Microsoft, это позволяет получить ***20-кратное повышение производительности*** по сравнению с SQL Server 2012.

Усовершенствования в AlwaysOn

- Усилена интеграция технологии AlwaysOn за счет ***увеличения максимального числа вторичных реплик с четырех до восьми***. Доступные для чтения вторичные реплики теперь можно использовать для задач чтения, даже если первичная реплика недоступна. Новый мастер создания реплик позволяет создавать асинхронные вторичные реплики в Windows Azure.

ПЕРВАЯ ДЕСЯТКА НОВШЕСТВ В SQL SERVER 2014

Расширение буферного пула

- SQL Server 2014 предусматривает интеграцию твердотельных дисков (SSD), что позволяет расширять буферный пул с использованием быстрой энергонезависимой памяти (NvRAM). Этот новый компонент делает возможным применение твердотельных накопителей для расширения буферного пула в системах, где память задействуется по максимуму. **Расширение буферного пула позволяет повысить производительность OLTP-приложений, для которых характерна высокая интенсивность чтения.**

Обновляемые колоночные индексы

- Впервые появившиеся в SQL Server 2012 колоночные индексы ***позволили заметно ускорить выполнение запросов к хранилищам данных.*** В некоторых случаях удается добиться **десятикратного повышения производительности.** Однако в SQL Server 2012 колоночные индексы используются в режиме «только чтение». В SQL Server 2014 это ограничение снято, благодаря появлению обновляемых колоночных индексов. В SQL Server 2014 колоночный индекс должен использовать все колонки в таблице, и его нельзя комбинировать с другими индексами.

ПЕРВАЯ ДЕСЯТКА НОВШЕСТВ В SQL SERVER 2014

Управление вводом/выводом хранилища

- Регулятор ресурсов ограничивает потребление ресурсов процессора и памяти для данной рабочей нагрузки. В SQL Server 2014 возможности регулятора ресурсов расширены и позволяют управлять потреблением ресурсов ввода-вывода хранилища. ***Теперь регулятор ресурсов может ограничивать физические ресурсы ввода-вывода, выделяемые для потоков пользовательского уровня в данном пуле ресурсов.***

Power View для многомерных моделей

- С появлением SQL Server 2014 технологию Power View, ранее работавшую только с табличными данными, ***можно использовать с многомерными моделями (кубами OLAP).*** Power View теперь позволяет создавать различные типы визуализации данных, включая таблицы, матрицы, пузырьковые диаграммы и географические карты. Многомерные модели Power View также поддерживают запросы с использованием выражений анализа данных Data Analysis Expression (DAX).

ПЕРВАЯ ДЕСЯТКА НОВШЕСТВ В SQL SERVER 2014

Power BI для интеграции с Office 365

- Power BI для Office 365 – «облачная» служба бизнес-аналитики (BI), обеспечивающая интеграцию данных и возможности визуализации. Power BI для Office 365 включает технологии Power Query (прежнее название – Data Explorer), Power Map (прежнее название – GeoFlow), Power Pivot и Power View.

SQL Server Data Tools для бизнес-аналитики

- Новая технология SQL Server Data Tools для BI (SSDT-BI) используется для создания моделей SQL Server Analysis Services (SSAS), отчетов SSRS и пакетов SSIS. SSAS и SSRS поддерживаются как для SQL Server 2014, так и для более ранних версий, но создание и развертывание проектов служб Integration Service (SSIS) доступно только для SQL Server 2014.

ПЕРВАЯ ДЕСЯТКА НОВШЕСТВ В SQL SERVER 2014

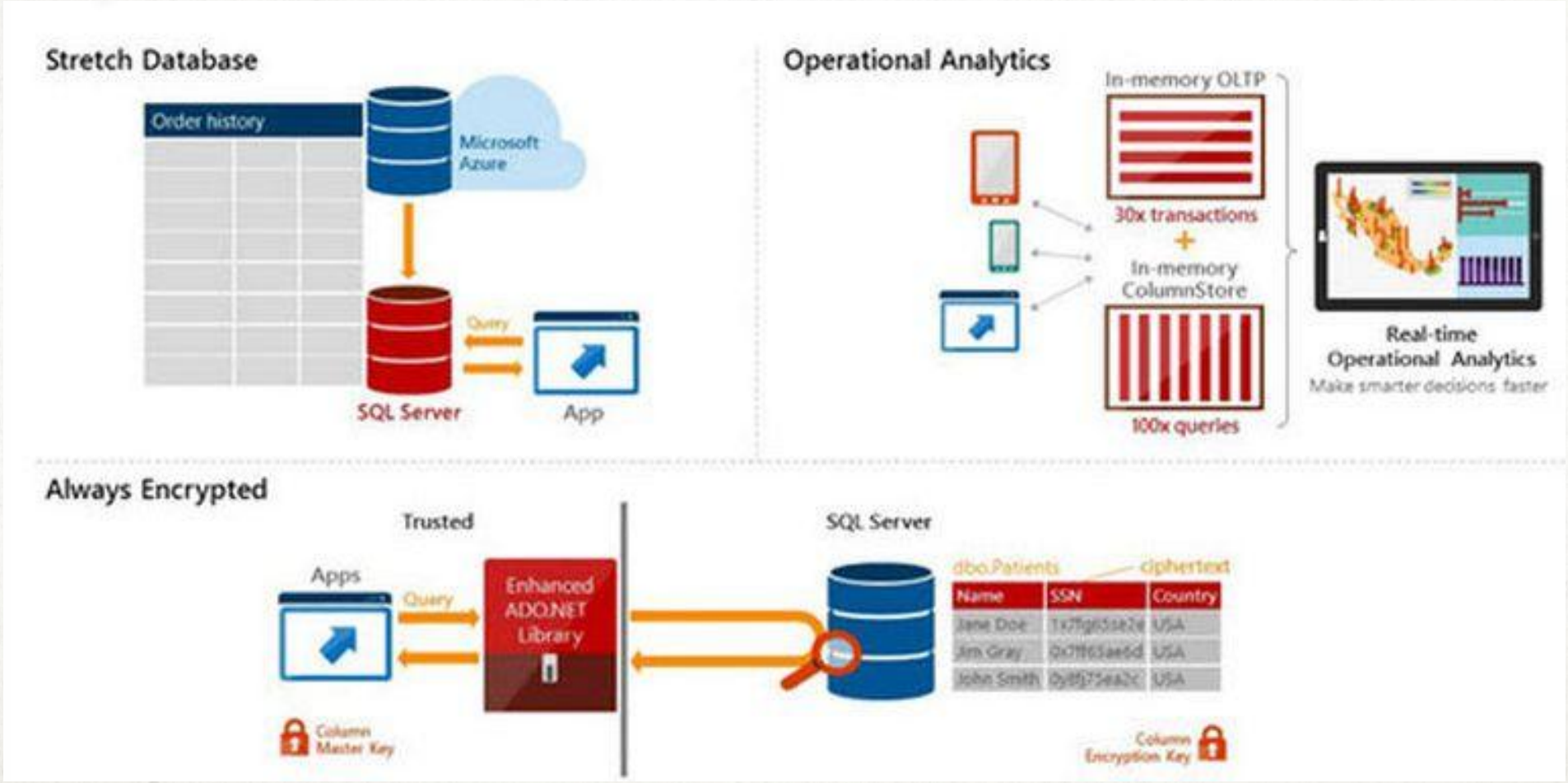
Шифрование резервных копий

- Долгожданным нововведением в SQL Server 2014 является возможность шифрования резервных копий баз данных для защиты хранящихся данных. SQL Server 2014 поддерживает несколько алгоритмов шифрования, включая Advanced Encryption Standard (AES) 128, AES 192, AES 256 и Triple DES. Шифрование резервных копий SQL Server 2014 требует использования сертификата или асимметричного ключа.

Управляемое резервное копирование SQL Server в Windows Azure

- Реализованная в SQL Server 2014 функция резервного копирования предусматривает интеграцию с Windows Azure. Локальный сервер SQL Server 2014 и экземпляры виртуальных машин в Windows Azure поддерживают резервное копирование в хранилище Windows Azure, хотя меня не радует перспектива зависеть от подключения к интернету для выполнения восстановления из резервных копий. Возможность резервного копирования в Windows Azure также встроена в SQL Server Management Studio (SSMS).

SQL SERVER 2016: ЧТО НОВОГО?



SQL SERVER 2016: ЧТО НОВОГО?

- **Always Encrypted** — новая функция, разработанная подразделением Microsoft Research и предназначенная для криптозащиты данных «в покое и движении»;
- **Stretch Database** — новая технология, позволяющая динамически расширить область размещения «теплых» и «холодных» транзакционных данных в Microsoft Azure;
- **Новая встроенная аналитика**, (http://www.osp.ru/win2000/2015/10/13047183/) интегрируемая с ПО на базе языка R.
- **Усовершенствования в технологиях in-memory-СУБД Hekaton**, встроенной Microsoft в SQL Server для аналитики в реальном времени;
- **Polybase** — движок для более простого управления реляционными и нереляционными данными, до сих пор бывший частью SQL Server Parallel Data Warehouse Appliance;

SQL SERVER 2016: ЧТО НОВОГО?

- **Безопасность строкового уровня** — функция, позволяющая контролировать доступ к данным на основе прав пользователя без модификации приложений;
- **Поддержка временных баз данных** для отслеживания изменений данных во времени;
- **Query Data Store** — «самописец» для администраторов баз данных, работает как рекордер информации для базы данных, обеспечивая полную историю исполнения запросов, так что DBA может отслеживать ресурсоёмкие запросы и оптимизировать их.
- **Улучшенное гибридное резервирование в Azure** и ускоренное восстановление в SQL Server на виртуальных машинах Azure.
- **Поддержка Native JSON** – позволяет просто парсить и сохранять JSON и экспортные данные в JSON.

SQL SERVER 2016: ЧТО НОВОГО?

- **AlwaysOn Enhancements** – возможность достигнуть более высоких уровней доступности данных и производительности на второстепенных устройствах с поддержкой до 3 синхронных копий, DTS и циклической балансировкой нагрузки.
- **Row Level Security** – даёт пользователям возможность управлять доступом к данным на базе характеристик пользователя. Система безопасности имплементирована непосредственно в БД, благодаря чему не требуется модификаций приложения.
- **Dynamic Data Masking** — поддержка обфускации данных в реальном времени таким образом, что пользователи, запрашивающие данные, не смогут получить доступ к неавторизованной информации. Это позволяет защитить важные данные, даже когда они не были зашифрованы;

EXCHANGE Server 2016

Архитектура

- Рекомендуемая архитектура:
  - DAG, растянутый на 2 датацентра
  - 4 копии почтовых баз: 3 обычных копии и 1 lagged копия (с задержкой 7 дней)
  - FileShareWitness размещен в Azure или третьем датацентре
  - Один сетевой адаптер для клиентского и репликационного трафика
  - Использование двухсокетного сервера с 20-24 ядрами и до 196Gb оперативной памяти
  - Использование JBOD дисков с большим объемом
  - Размещение нескольких почтовых баз на одном LUN
  - Использование функции Autoreseed с дисками под замену
  - Использование ReFS файловой системы для дисков с почтовыми базами
  - Использование BitLocker для дисков с почтовыми базами
  - Наличие фермы Office WebApp Server в каждом датацентре

- Роли CAS и Mailbox теперь объединены в одну
- Роль Edge будет доступна позднее.
- MAPI/CDO более не поддерживается
- MAPI/HTTP протокол по умолчанию для подключения Outlook. Управление MAPI/HTTP будет осуществляться на уровне почтового ящика
- Office WebApp Server необходим для просмотра или редактирования документов в OWA 2016
- Для масштабируемости необходимо использовать дополнительные сервера, нежели увеличение ресурсов существующих
- Не рекомендуется DAG, растянутый более чем на 2 датацентра
- Использование общедоступного (внешнего) и приватного (внутреннего) имени для Outlook Anywhere, чтобы обеспечить внутренним клиентам Kerberos аутентификацию
- Exchange 2016 для claim-based аутентификации требует ADFS 2016

EXCHANGE Server 2016

Архитектура

- Клиентский трафик может проксироваться в следующих направлениях: Exchange 2016 –> Exchange 2013 и Exchange 2013 –> Exchange 2016. Это означает, что теперь нет необходимости сначала обновлять сервера в сайте с Интернет доступом
- Путь обновления с Exchange 2010 до Exchange 2016 аналогичен обновлению Exchange 2010 до Exchange 2013
- Exchange 2016 может сосуществовать с Exchange 2010 SP3 RU11+ или с Exchange 2013 CU10+
- Exchange 2016 может использовать тот же аккаунт ASA для керберос аутентификации, что и Exchange 2013
- Сосуществование с Exchange 2007 – не поддерживается. Для обновления с Exchange 2007 придется использовать следующий путь: Exchange 2007 –> Exchange 2010 (2013) –> Exchange 2016

EXCHANGE Server 2016

Установка

- Exchange 2016 поддерживает установку на Windows Server 2012 R2 и Windows Server 2016
- Exchange 2016 требует, как минимум Windows Server 2008 R2 FFL и DFL (и соответственно, как минимум контроллеры с Windows Server 2008 R2)
- Exchange 2016 поддерживает следующих клиентов:
  - Outlook 2010 SP2 с апрельским обновлением от 2015 года (KB2956191 и KB2965295)
  - Outlook 2013 SP1 с декабрьским обновлением от 2014 года (KB3020812)
  - Outlook 2016

EXCHANGE Server 2016

Установка

EXCHANGE Server 2016

Хранилище

- Exchange 2016 требует на 22% IOPS меньше в сравнении с Exchange 2013 RTM
- Служба поиска будет индексировать пассивную копии вместо копирования индексов с активной копии
- Replay Lag Manager будет включен по умолчанию
- В Exchange 2016 функция Autoreseed сможет восстанавливать одну из почтовых баз, размещенных на одном LUN
- Exchange 2016 будет более внимательно следить за производительностью дисков

- DAG в Exchange 2016 по умолчанию будет устанавливаться без CNO
- Пассивная копия почтовой базы в Exchange 2016 будет активироваться на 33% быстрее (6-7 секунд)
- Сервера Exchange 2016 могут находиться в одном пуле с Exchange 2013 на балансировщике

EXCHANGE Server 2016

Высокая доступность

- Exchange 2016 может управлять объектами Exchange 2013 и наоборот. Для управления объектами Exchange 2010 рекомендуется использовать Exchange 2010
- Вернется утилита Exchange Server User Monitor
- В Exchange 2016 появятся политики с ограничением на перемещение ящиков в рабочее время
- В Exchange 2016 будет возможно включить режим In-Place Hold для общих папок
- Outlook 2016 и Exchange 2016 будут использовать поиск на стороне сервера, обеспечивая одинаковый результат в Outlook, OWA, ActiveSync

EXCHANGE Server 2016

Управление

Дополнительные функции

- В Exchange 2007 мы уменьшили количество обращений к диску ((Input/Output Operations per Second, IOPS) более чем на 70% по сравнению с Exchange 2003.
- В Exchange 2010 мы уменьшили количество дисковых операций ввода-вывода еще более чем на 70% по сравнению с Exchange 2007. Это означает, что Exchange 2010 генерирует примерно 10% от операций ввода-вывода эквивалентно нагруженной системы Exchange 2003.
- Это открывает нам совершенно новый набор возможностей для использования очень больших, очень медленных, очень дешевых дисков, таких как 2-терабайтных дисков SATA 7200 об/мин или дисков SAS.

EXCHANGE Server 2016

Дизайн хранилища

ДИЗАЙН ХРАНИЛИЩА

- Множество дизайнов поддерживаются. Есть три измерения в дизайне:
- SAN □□ DAS
  - SAN не быстрее DAS
  - Уменьшение сложности
  - Не нужны дорогие избыточные компоненты SAN
- FC □ SAS □ SATA
  - Быстрые диски не нужны. Нужны большие
  - В Ex2013 требования к IOPS снижены на 93% по сравнению с Ex2003 и на 79% по сравнению с Ex2007
  - Типичная база Ex2013 требует ~10 IOPS
    7200 rpm LFF (3.5”) SATA даёт ~60 IOPS
    15K rpm SFF (2.5”) SAS/FC даёт ~250 IOPS
  - Быстрые, маленькие и дорогие диски не нужны
- RAID □□ JBOD
  - Избыточность дисков не нужна:
    избыточность данных перенесена на уровень приложения
  - Серверы Ex2013 это такой программный RAID
  - RAID поддерживается, но зачем?